IDPro Body of Knowledge Table of Contents
Working DRAFT

April 20, 2020

Contents

Chapter 1

Introduction

1.1 Introduction to Identity – Part 1: Admin-time – *article in progress*

Abstract: This article introduces the concepts of digital identity and identity and access management (IAM). It also discusses the constituents that identity professionals serve, compares and contrasts business-to-employee (B2E) and business-to-consumer (B2C) identity use cases, and considers IAM technologies from the perspective of administrative, or admin-time, technologies.

Sections in this article include:

- Introduction: How to Approach Identity and IAM.
- Constituencies - who is it that we serve?
- Business-to-Employee (B2E): Making Employees Productive.
- Business-to-Business (B2B): Connecting to Partners.
- Business-to-Consumer (B2C): Digitally Engage.
- Technologies Involved - Admin-time vs. Run-time.
- Admin-time Technologies.
- Sources of “Truth”.
- Identity Governance and Administration.
- Identity Analytics.
- Privileged Account Management.
- Identity Proofing.

1.2 Introduction to Identity – Part 2: Run-time – *article in progress*

1.3 Introduction to Identity – Part 3: Use Cases – *article in progress*

1.4 Ethics – *article in progress*

1.5 Information Security

1.6 Trust in the IAM Context

1.7 Privacy

1.8 Identification and authentication

1.8.1 Context and Identity

1.8.2 Levels of Assurance

1.9 Bias in Identity Systems

Chapter 2

Digital Identity

2.1 Definition of Digital Identity

Abstract: Despite the difficulty of creating a universal definition of identity, we create a working definition of a more limited concept of digital identity. In this section, we focus on human persons and touch only slightly on non-personal identities such as corporations and devices. Starting with the concept that digital identity is a unique identifier together with relevant attributes required to enable the identifier to be used in the context of a digital transaction, this article elaborates and articulates interesting details, such as the level of certainty about and provenance of attribute values.

2.1.1 Reputation

2.2 Digital Identifiers *– article in progress*

Abstract: What is in a name? It turns out that there are concerns that are explored here. These include the domain in which it can be considered unique when it can be reused, whether it should be considered secret, and whether it should be memorable. Additional system-level considerations are raised such as permanent system identifiers. Given that users may forget or lose their identifiers, the article also discusses the need to allow for the safe recovery of the same. Identifiers for devices are covered more fully in the non-human entity section.

2.3 Digital Identity Lifecycle

Abstract: In addition to the steps typically associated with other digital records, such as create, update and delete, this article describes several other activities also asso-

ciated with digital identities. For instance, there are activities that may gather or dispose of additional attribute information either based on claims made by a person or based on information from 3rd parties. This article provides a list of activities that may occur between the creation of the digital identity and its disposal.

2.4 Proofing, Binding or Registration

Abstract: In many contexts, it is important to relate a human to a digital account. Typically it matters in commercial and institutional environments. This activity has been described as proofing or vetting, implying certainty about the mapping. But there is a gradient of need - in some cases, it is very important such as in the fields of medicine or finance, whereas in other cases much less care is needed to achieve the needed level of assurance. This article discusses the drivers and the palette of tactics that can be used to balance the desired level of certainty to the mapping and the desired level of friction to be experienced by the user.

2.4.1 Verification/Validation

2.5 Credentials

Abstract: When the registration process contains more than a little friction, many systems provide a way to avoid that friction during logins, a process that happens many more times than registration does. In the simplest scenario, this is done by issuing a user ID and a password, in other words, a credential. This section describes the varieties of credentials that are in common use. It also describes methods for establishing credentials (how to convey them safely) and some recovery mechanisms when they are lost or compromised. Because credentials can be stolen, this article touches on the approach that some implementations have taken which look to device identities to reduce risk.

Chapter 3

Access Control

3.1 Introduction to Access Control – *article in progress*

Abstract: As the name implies Identity and Access Management (IAM) is split into two functions: managing identity information and performing access control. Arguably, if there was no access control requirement there would be no need for identity management; it is therefore the focus for IAM professionals.

At its core access control is ensuring users are authenticated to access protected resources. This is accomplished by managing user entitlements and satisfying the requirements of relying applications so that users can only access the systems and information they are entitled to access.

This article looks at the history of access management, the expected current functionality and the trends to be expected.

3.1.1 Authentication

3.1.2 Dynamic Authentication (risk-based)

3.1.3 Multi-Factor Authentication

3.1.4 Single Sign-on Within a Domain

3.1.5 Centralised Authentication Service

3.1.6 Federated Authentication (between domains)

3.1.7 Device Identity for Corroboration

3.1.8 Fast Identity Online (FIDO) and its cousins

3.1.9 Session Management

3.2 Authorization

3.2.1 Resources to Protect

3.2.2 Authorisation

3.2.2.1 ACL's

3.2.2.2 RBAC

3.2.2.3 ABAC / Dynamic Access Management

Policy Management solutions

3.2.3 Privileged Access Management

3.2.3.1 Alignment to Risk Management

3.2.3.2 System Accounts

Chapter 4

Laws, Regulations, and Standards

Abstract: This chapter provides information about the externally defined environment in which Identity and Access management professionals operate. The laws are documents that define duties and consequences in legal jurisdictions, such as countries. Regulations are more specific and detailed requirements. Standards may also be mandatory; government entities often require compliance with standards produced by certain standards bodies. We also include *de facto* standards and recommended practices here.

4.1 Framework to Understand Legal Environment – *article in progress*

Abstract: Identity systems and its participants are governed by a myriad and complex set of laws, regulations, and contractual requirements, and the obligations they impose are not always clear. This article focuses on the legal environment that governs identity systems. The emphasis is on United States, but references are made to other countries' laws and efforts to coordinate rules underway in the UN Commission on International Trade Law (UNCITRAL) regarding identity management legislation.

4.2 Approach to Compliance for the Identity Practitioner

Abstract:

The overview, above, provides a broad perspective on what the practitioner might encounter. This article provides a companion piece that is less theoretical and more practical and concise. This does not provide legal advice; for that one must consult a legal professional. Instead we chart paths that the reader might take in sample

situations to prepare for legal review. The goal is to ensure the identity system, as built and operated, will be in robust compliance with law. This takes the form of three illustrative use-cases where the identity system supports various combinations of jurisdictions, participants and federation:

a) Single jurisdiction, supporting customer access, including out-bound federation for certain aspects of the customer journey;

b) A system that relies entirely on external "identity providers", with operations in several jurisdictions;

c) A multi-jurisdiction employee/contractor-focused system, which wishes to use biometric techniques for authentication.

The general approach is to use the jurisdictions, participants, federations and technologies under consideration in order to locate aspects of the law that must be considered.

4.3 Highlights of Selected Laws

Abstract: This section is organized by jurisdiction. It is intended to provide at a minimum a reference to known laws and regulations in jurisdictions likely to be encountered by our membership. At present this includes Europe, United States, and Canada will likely also include Australia in the short term.

4.3.1 Europe

4.3.1.1 Introduction to GDPR – *article in progress*

Abstract: This article provides a basic understanding of how the *General Data Protection Regulation (GDPR)* applies when processing 'any information relating to an identified or identifiable natural person'.

4.3.1.2 IAM Implications of GDPR – *article in progress*

Abstract: This article provides information to the IAM practitioner about how to achieve compliance with the European data protection and privacy rules for European and multi-national firms

4.3.2 United States

Abstract: This article explains how identity and access management supports the requirements of prominent U.S. laws.

4.3.2.1 Sarbanes-Oxley Section 404

4.3.2.2 Health Insurance Portability and Accountability Act (HIPAA)

4.3.2.3 Health Information Technology for Economic and Clinical Health Act (HITECH)

4.3.2.4 Family Educational Rights and Privacy Act of 1974 (FERPA)

4.3.2.5 Children's Online Privacy Protection Act (COPPA)

4.3.2.6 Fair and Accurate Credit Transaction Act (FACTA)

4.3.3 Canada

Abstract: This article explains how identity and access management support the requirements of prominent Canadian laws.

4.3.3.1 Personal Information Protection and Electronic Documents Act (PIPED Act, or PIPEDA)

4.4 Regulations

Abstract: This article explains how identity and access management supports the requirements of prominent regulations.

4.5 Standards

Abstract: There are many standards. Standards may be mandatory such as when government entities require compliance with standards produced by certain standards bodies. We also include *de facto* standards and recommended practices here. This is a curated set of standards that have been deemed to be useful to identity professionals. They are organized topically, not by their source. Standards that span more than one topic are possible. In this case cross references may be used.

4.5.1 Architecture

Abstract: This article surveys the known standards concerning architecture for identity systems.

4.5.1.1 ISO/IEC 24760-2:2015 Information technology -- Security techniques -- A framework for identity management -- Part 2: Reference architecture and requirements – *article in progress*

4.5.2 Assurance

Abstract: This article surveys the known standards concerning risk and assurance for identity systems.

4.5.2.1 *Directive on Identity Management - Appendix A: Standard on Identity and Credential Assurance*

[Canada] Government of Canada July 2019 `https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32612`

4.5.2.2 *Digital Identity Guidelines*

[SP 800-63-3] NIST Special Publication 800-63-3 June 2017 https://doi.org/10.6028/NIST.SP.800-63-3

4.5.2.3 *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*

[SP-800-37] NIST Special Publication 800-37r1 June 2014 https://doi.org/10.6028/NIST.SP.800-37r1

4.5.3 Authentication

Abstract: This article surveys the known standards concerning methods of authenticating principals.

4.5.3.1 *Digital Identity Guidelines: Authentication and Lifecycle Management*

[SP 800-63B] NIST Special Publication 800-63C December 2017 https://doi.org/10.6028/NIST.SP.800-63b

4.5.3.2 *Introduction to Public Key Technology and the Federal PKI Infrastructure*

[SP 800-32] NIST Special Publication 800-32 February 2001. https://tsapps.nist.gov/publication/get_p

4.5.3.3 *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map*

[IETF RFC 4510] RFC 4510 June 2006 https://tools.ietf.org/html/rfc4510

4.5.3.4 *OpenID Connect Core 1.0 incorporating errata set 1*

[OIDC] Sakimura, N., Bradley, B., Jones, M., de Medeiros, B., and C. Mortimore November 2014 https://openid.net/specs/openid-connect-core-1_0.html.

4.5.3.5 *Personal Identity Verification (PIV) of Federal Employees and Contractors*

[FIPS 201-2] NIST FIPS Publication 201-2 September 2013 https://doi.org/10.6028/NIST.FIPS.201-2

4.5.3.6 *Biometric Data Specification for Personal Identity Verification*

[SP 800-76-2] NIST Special Publication 800-76-2 July 2013 https://doi.org/10.6028/NIST.SP.800-76-2

4.5.4 Authorization

Abstract: This article surveys the known standards concerning methods of access control. These standards involve protecting resources. This is sometimes called authorization.

4.5.4.1 *The OAuth 2.0 Authorization Framework*

[IETF RFC 6749] RFC 6749 October 2012 https://tools.ietf.org/html/rfc6749

4.5.4.2 *User-Managed Access (UMA) Profile of OAuth 2.0*

Abstract: The weaknesses of many notice-and-consent paradigms of data privacy are clear. This article notes the social, legal and regulatory drivers and examines some approaches to satisfy them.

[KI UMA] Kantara Initiative UMA Recommendation December 2015 https://docs.kantarainitiative.uma-core.html

4.5.5 Federation

Abstract: This article surveys the known standards concerning methods of allowing authentication from one domain to be honored in another.

4.5.5.1 *OpenID Connect Core 1.0 incorporating errata set 1*

[OIDC] Sakimura, N., Bradley, B., Jones, M., de Medeiros, B., and C. Mortimore November 2014 https://openid.net/specs/openid-connect-core-1_0.html.

4.5.5.2 *Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) V2.0*

[OASIS SAML 2] SAML 2.0 March 2005 http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf

4.5.5.3 *Digital Identity Guidelines: Federation and Assertions*

[SP 800-63C] NIST Special Publication 800-63C December 2017 https://doi.org/10.6028/NIST.SP.800-63c

4.5.6 Lifecycle

Abstract: This article surveys the known standards concerning the creation and registration of identities and subsequent changes to the characteristics of those identities and the eventual removal of the same.

4.5.6.1 *Standard on Identity and Credential Assurance*

[Canada] Government of Canada July 2019 https://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=32612

4.5.6.2 *Digital Identity Guidelines: Enrollment and Identity Proofing Requirements*

[SP 800-63A] NIST Special Publication 800-63A December 2017 https://doi.org/10.6028/NIST.SP.800-63a

4.5.6.3 *Digital Identity Guidelines: Authentication and Lifecycle Management*

[SP 800-63B] NIST Special Publication 800-63C December 2017 https://doi.org/10.6028/NIST.SP.800-63b

4.5.6.4 *System for Cross-domain Identity Management: Protocol*

[IETF RFC 7644] RFC 7644 September 2015 https://tools.ietf.org/html/rfc7644

4.5.6.5 *System for Cross-domain Identity Management: Core Schema*

[IETF RFC 7643] RFC 7643 September 2015 https://tools.ietf.org/html/rfc7643

4.5.7 Operations

Abstract: This article surveys the known standards concerning the operation of identity systems.

4.5.7.1 *Information technology -- Security techniques -- A framework for identity management -- Part 3: Practice – article in progress*

[ISO 24760-3] ISO/IEC 24760-3:2016 2016 https://webstore.ansi.org/Standards/ISO/ISOIEC2476020

4.5.8 Terminology

Abstract: This article surveys the known standards for the purpose of collating and contrasting terminology defined.

4.5.8.1 *Digital Identity Guidelines*

[SP 800-63-3] NIST Special Publication 800-63-3 June 2017 https://doi.org/10.6028/NIST.SP.800-63-3

4.5.8.2 *An Ontology of Identity Credentials Part I: Background and Formulation*

[SP 800-103] NIST Special Publication 800-103 (Draft) October 2006. https://tsapps.nist.gov/publicati

4.5.8.3 *Security and Privacy -- A Framework For Identity Management -- Part 1: Terminology And Concepts – article in progress*

[ISO 24760-1] ISO/IEC 24760-1:2019 IT 2019 https://webstore.ansi.org/Standards/ISO/ISOIEC247602

4.5.8.4 ISO/IEC 24760-1:2019 IT Security and Privacy -- A Framework For Identity Management -- Part 1: Terminology And Concepts

4.6 Emerging Societal Norms

4.6.1 Managing Consent – *article in progress*

Chapter 5

Workforce IAM / Internal IAM

5.1 IAM Processes

5.1.1 Joiner-Mover-Leaver

5.1.2 HR Ownership

5.1.3 Provisioning (On-boarding and Off-boarding)

5.1.4 Role Management

5.1.5 Re-certification

5.2 Compliance

5.3 Analytics and Intelligence

5.4 Handling Business Partners' People

Chapter 6

Consumer/Citizen IAM

6.1 CIAM vs Workforce IAM

This introductory article reviews the main key differences between IAM in the consumer world versus IAM in the enterprise. Some of these differences include: focusing on the consumer experience and consumer needs as opposed to the needs of the enterprise and offering a different balance between what a consumer expects in terms of usability and security versus enterprise requirements.

6.2 Consumer Journey

Consumers are the focus of the CIAM program. There are several areas that need to be considered that could help you implement a successful CIAM program, including the registration process for consumers, determining and implementing assurance requirements, and the handling of user consent. This section focuses on these areas, offering specific examples and guidance for the IAM practitioner in the consumer-focused industry.

6.2.1 Registration of consumers

This article discusses consumer registration in a product or service. Registration is one of the early experiences in your product. Too much friction in this step would result in consumers going away. In general, it's the idea of asking for as little as possible on first contact (email-only or email+password registration) and then using various profile enrichment strategies later on, e.g., MFA, shipping address, phone number, etc.

6.2.2 Authentication assurance (meeting LoA requirements)

Most activities in CIAM do not require a great level of assurance to be able to do an operation, for example, updating a birthday or a display name. This article explores the concept of levels of assurance (LoA) as it applies to CIAM, including a review of activities that might require a high authentication level of assurance as those are sensitive activities such as the purchase of regulated goods, or access to health-related records. In this case, another authentication process might be rolled out, e.g., prompt another layer of authentication to make sure the consumer is the right people perform the activities.

6.2.3 Data usage consent

The consumer should know how his/her data is being used by the company to give a better experience to the consumer. That's why it's important to ask the consumer's consent to make sure they are all aware of their data usage and store the consent to help with a dispute in case it happens. This article references "Managing Consent" by Eve Maler and Graham Williamson, currently in the BoK queue and focuses on additional considerations specific to CIAM.

6.2.4 Social sign-in and sign-up

Social sign-up offers a consumer a way to sign-up to a CIAM system that takes advantage of existing accounts owned by the user. CIAM-focused companies can effectively outsource some of the user support (such as password management) to these social media systems and instead focus on what information is required for personalization. This article explores how social media logins can complement a CIAM infrastructure and offers suggestions on how to offer the maximum benefit to the consumer. This article ties closely to the Data Usage Content article.

6.3 Unified consumer view

This article describes the opportunities and challenges involved with supporting a unified view of the consumers of a product or service to a company in order to support targeted marketing, content, or product recommendations. In order to have a unified consumer view, the CIAM system could provide flexible attributes so the application is able to add its own unique fields and help shape the consumer profile. Done appropriately, this service can be of value to both the company and the consumer.

6.4 Industry Considerations

6.4.1 Public sector vs private sector

The article explains the unique use cases and challenges in the public sector and private sector that should be considered by the IAM practitioners. The article also provides the best practices and tips to deal with the use cases and challenges. Almost every service requires a different identification method in public sectors. Each governmental agency has unique requirements for authentication. As an example registering with your General Practitioners (GP) in the UK requires a National Health Service number, while HMRC directs users to its Government Gateway scheme to sign up and pay self-assessment taxes. This net result is citizens need to have a variety of different identification methods to complete straight forward tasks. The section article explains tips and best practices for navigating this issue.

6.4.1.1 Strong identity proofing

Identity proofing is essential to enable the digital government. But the extensive amount of data to prove the citizen identity has become one of the challenges. The section explains the tips on navigating some of the issues to create a strong yet consumer-friendly identity proofing.

6.4.2 Financial services

The section explains the unique use cases and challenges in the financial industry that should be considered by IAM practitioners. The section also provides the best practices and tips to deal with the use cases and challenges.

6.4.2.1 Integration with the legacy system

This should be considered given that most of the banks or financial services have had their own system for a long time ago. Things like how to let existing customers apply for new services easily should be considered.

6.4.2.2 High Level of Assurance on sensitive activities

Most of the activities in the financial services industry involve action toward and accessing sensitive information, such as purchase goods, funds transfer, etc. Due to this, there must be a high LoA to make sure the right person performs the right activities. This article explores ways of having a higher level of assurance and protects

consumers from fraud, e.g., perform step-up authentication, contextual authorization, pin validation, card validation, etc.

6.4.2.3 The identities delegation

An example is a child managing a bank account on behalf of an elderly parent. There are several challenges to deal with the use case. Some of them are to deal with the power of attorney, and audit to make sure the child doing things based on court authorization on behalf of the parent and not just sharing the parent's password with the child. The article explores the best practices to deal with the use case as it is becoming more common use cases across several sectors, such as financial and healthcare services.

6.4.2.4 Financial regulations compliance and guidance from the government organizations

There are specific regulations and organizational guidance in the financial industry that help security and convenience to the consumer, for example, Payment Service Directives 2 (PSD2), Open Banking, Financial Ask Task Force organization. The article explains about those and provides tips on how to comply with the regulation or follow the organizational guidance.

6.4.3 Healthcare

The section explains the unique use cases and challenges in the financial industry that should be considered by IAM practitioners. The section also provides the best practices and tips to deal with those use cases and challenges.

6.4.3.1 High Level of Assurance on sensitive data (LoA)

Most data in the healthcare industry are sensitive data, e.g., a patient's profile, disease history, medical records, etc., and so a high level of assurance is required for making sure only the right person accesses the right data. There are several exceptions though. For example, a homeless man who doesn't have a fixed address and no form of authentication wants to access his data. The person deserves to access his data but he can't prove himself. The section explains ways and best practices for achieving the high LoA, e.g., step-authentication and to deal with the unique use case such as the homeless man case, e.g., implements "known to the practitioners" or in other words the ability of a practitioner (doctor) to vouch for the patient's identity

6.4.3.2 Identities delegation

An example is the parent and child relationship where the parent has access to their child's medical records (provided consent was given). There are several challenges to deal with the use case. Some of them are to deal with the power of attorney and audit. The article explores the best practices to deal with the use case as it is becoming more common use cases across several sectors, such as financial and healthcare services.

6.4.3.3 Healthcare regulations compliance

The section explains the regulations in the healthcare industry such as the Health Insurance Portability and Accountability Act (HIPAA) and the tips to comply with those.

6.4.4 Game

6.4.5 The section explains unique use cases and challenges faced in the gaming industry that should be considered for IAM practitioners. The section also explains the tips and best practices to deal with those use cases and challenges.

6.4.5.1 Local game privacy compliance

The section explains the regulations in the game industry that should be considered while building CIAM such as General Data Protection Regulation (GDPR) for EU players, and Shutdown Law for Korean players and the tips to comply with those.

6.4.5.2 Scalability and availability

There are around 1.2 billion players in the world. Knowing this, the scalability and the high availability are important factors for having a successful CIAM. The article explains the tips and best practices to handle the load and keep the game services online at all times.

6.4.5.3 Gaming and authentication

Most mobile games do not require authentication at the start so the player could start playing immediately thus increasing the player engagement. This could be achieved by creating an anonymous account at the start of the game. The article explores the tips to deal with this "expectation", anonymous account implementation, and account upgrade implementation to help players secure their account.

6.5 Privacy and Compliance

Privacy and compliance capabilities are foundational and the CIAM program should focus on protecting the individual. CIAM teams must adhere to an increasing number of consumer protection laws and regulations. For example the EU General Data Protection Regulation (GDPR) and California Consumer Privacy Act (CCPA). Multinational companies should worry about the privacy compliance of each and every country they do business with. This article builds on other areas of the BoK that consider specific regulations like GDPR and discusses the specific considerations of privacy and compliance in a consumer-focused environment.

6.6 Security

Good security must underpin all CIAM initiatives as this is the key to protect consumer data and to maintain their trust in our system. It is important to remember user experience should be considered as well while creating a good security model. The following sections explain some key methods for achieving good security.

6.6.1 Adaptive authentication

It is an authentication action that takes account of other dynamic-runtime environment data or context-based attributes, e.g., device location, time to login, etc., in addition to credentials such as username and password to authenticate users. The authentication is also known as risk-based or contextual authentication.

6.6.2 Multi-Factor Authentication (MFA)

This refers to the use of more than one credential in the authentication of the user. Generally, the use of multiple factors results in a higher LoA for the user's authentication. Two-factor (2FA) is the simplest example of MFA where two different credentials are used. MFA provides a variety of factors to choose from, ranging from asking a security question to capturing and confirming biometric data to using physical authentication keys, codes or One-Time Passwords (OTPs) over SMS/email or Time-based One-time Password (TOTP) (Google Authenticator).

Chapter 7

Non-Human Entity

7.1 Operational Technology (OT)

7.2 Service Accounts

7.3 IoT Devices

7.3.1 IoT Sectors

7.3.1.1 Home Automation

7.3.1.2 Personal (wearables)

7.3.1.3 Implants

7.3.1.4 Plant Automation

7.3.1.5 Vehicle

7.3.1.6 Smart Cities

7.3.1.7 Agriculture

7.3.1.8 Building/Industrial

7.3.1.9 Utilities

7.4 RPA / robotics

7.5 Security requirements

Chapter 8

IAM Architecture and Solutions

8.1 IAM Architecture Overview – *article in progress*

8.2 Architecture Patterns – *article in progress*

8.3 Technical Architecture – *article in progress*

8.4 Identity Governance – *article in progress*

8.4.1 Elements of IGA Systems – *article in progress*

8.5 Key Definitions and Terms – *article in progress*

8.6 Business System

8.6.1 Business Processes

8.6.1.1 Recertification of accounts

8.7 Recommended Practices

8.7.1 Design for security

Chapter 9

Operational Considerations

9.1 Account recovery

9.2 Call centers

9.3 Engagement of user for their own security

9.4 Security events and operations

Chapter 10

Project Management

Many Identity and Access Management (IAM) projects proceed without a project manager. In these cases the IT group in charge of identity management are left to deploy the required solution in the absence of any overarching management. While this is sometimes seen as the most expedient way to get a system installed or updated, it is short-sighted and likely to cost the organisation more money in the longer term. An IAM solution touches so many systems within an organisation and is dependent on the current and planned condition of so many applications that to deploy a solution without properly considering the impact, managing the required resources and keeping management advised of progress, will result in a substandard deployment.

Here we look at two ways to manage a project – "Classic", sometimes called Waterfall, and "Agile, a way to manage projects that accommodates changes that inevitably arise during the course of a project.

Reference is made to the Project Management Institute (PMI) Framework. This document in no way seeks to replicate the PMI's methodology or replace the project management training that the PMI provides. The reader is referred to the PMI Body of Knowledge for further information.

10.1 Project Management Institute Framework and Project Management Office Issues *– article in progress*

10.2 New Implementation Projects

10.3 Migration Projects

Chapter 11

IAM Knowledge Sharing

11.1 Independent Organizations – *articles in progress*

11.2 Standards Bodies

11.3 Analyst Organizations

11.4 Conferences

Chapter 12

Advanced Topics – Parking Lot

12.1 Digital Legacy - handling deceased persons’ digital ID (Advanced Topic)

12.2 Self-Sovereign Identity

12.2.1 Blockchain ID