**SOFTWARE TRAINING**

**IDENTITY AND ACCESS MANAGEMENT**

**Submitted in partial fulfilment of the**

**Requirements for the Software Training of**

**Degree of B.Tech in Computer Science and Engineering**



**As Part of Course Work of**

**B.Tech. in Computer Science and Engineering**

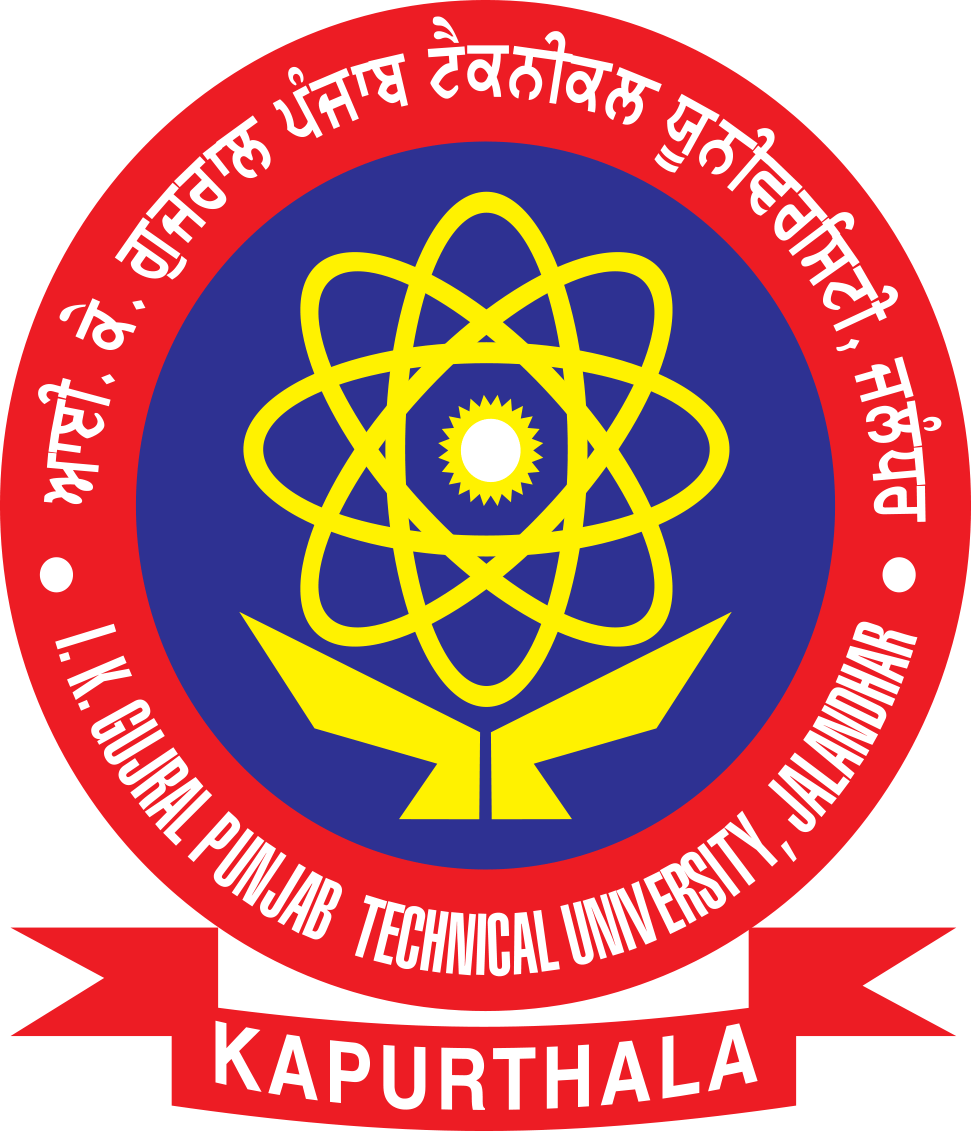
**Submitted to: Submitted By:-**

CSE Department Name:Arjun Suri

Branch: CSE

Semester: 8th

Univ Roll No: 1535426



**Affiliated to I.K Gujral Punjab Technical University, Jalandhar**

**(Batch: 2015-2019)**

**CGC TECHNICAL CAMPUS, FACULTY OF ENGINEERING,**

**JHANJERI, MOHALI**

### CERTIFICATE

This is to certify that Mr. Arjun Suri has completed the 4 Months Industrial Training during the period from January to April in our Industry as a Partial Fulfillment of Degree of Bachelor of Technology in Computer science & Engineering. He was trained in the field of Identity and Access Management.

**Signature of Training Manager**

**ACKNOWLEDGEMENT**

I would like to place on record my deep sense of gratitude to Er. **Biswajeet Mohanty, (Advisory Manager)** for his generous guidance, help, useful suggestions and continuous encouragement.

I am extremely thanks to **Dr. Rajneesh Talwar**, Principal CGC Technical Campus, Jhanjeri, Mohlai (Punjab) and Management for providing encouragement and allowing me to work in Deloitte USI Bangalore & supporting and guiding me regarding the same.

I am extremely thankful to **Dr. Raman Chadha,** HOD, Computer Science & Engineering, CGC Technical Campus, Jhanjeri, Mohali(Punjab) for valuable suggestions and motivation.

I am also thankful to all my Teachers who have taught me throughout my Degree and the Training & placement officers of CGC Technical Campus, Faculty of Engineering, Jhanjeri, Mohali(Punjab), for providing the opportunity to get the knowledge.

**Signature of Student**

**ABSTRACT**

Identity and access management (IAM) is a framework for business processes that facilitates the management of electronic or digital identities. The framework includes the organizational policies for managing digital identity as well as the technologies needed to support identity management.

With IAM technologies, IT managers can control user [access](https://whatis.techtarget.com/definition/access) to critical information within their organizations. Identity and access management products offer [role-based access control](https://searchsecurity.techtarget.com/definition/role-based-access-control-RBAC), which lets system administrators regulate access to systems or networks based on the roles of individual users within the enterprise. Systems used for identity and access management include [single sign-on](https://searchsecurity.techtarget.com/definition/single-sign-on) systems, [multifactor authentication](https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA) and access management. These technologies also provide the ability to securely store identity and profile data as well as [data governance](https://searchdatamanagement.techtarget.com/definition/data-governance) functions to ensure that only data that is necessary and relevant is shared.

The tool used to implement IAM solution is “Sailpoint”.

**ABOUT DELOITTE**



Deloitte is one of the "[Big Four](https://en.wikipedia.org/wiki/Big_Four_(audit_firms))" accounting organizations and the largest [professional services network](https://en.wikipedia.org/wiki/Professional_services_networks) in the world by revenue and number of professionals.

Deloitte provides [audit](https://en.wikipedia.org/wiki/Audit), [tax](https://en.wikipedia.org/wiki/Tax), [consulting](https://en.wikipedia.org/wiki/Consultant), [enterprise risk](https://en.wikipedia.org/wiki/Enterprise_risk_management) and [financial advisory](https://en.wikipedia.org/wiki/Corporate_services) services with more than 263,900 professionals globally. In [FY](https://en.wikipedia.org/wiki/Fiscal_year) 2017, the network earned a record $38.8 billion USD in aggregate revenues. As of 2016, Deloitte is the 6th-largest [privately owned organization](https://en.wikipedia.org/wiki/Private_company) in the United States.

As per reports in 2012, Deloitte had the largest number of clients amongst [FTSE 250](https://en.wikipedia.org/wiki/FTSE_250) companies in the UKand in 2015, Deloitte currently has the highest market share in auditing among the top 500 companies in India. Deloitte has been ranked number one by market share in consulting by [Gartner](https://en.wikipedia.org/wiki/Gartner), and for the fourth consecutive year, Kennedy Consulting Research and Advisory ranks Deloitte number one in both global consulting and [management consulting](https://en.wikipedia.org/wiki/Management_consulting) based on aggregate revenue.

**TABLE OF CONTENTS**

**Chapter No. Page No.**

1. **Acknowledgement**....……...........…………..…………………................................. ii
2. **Abstract**...............…………………...........…………..…………………................... iii
3. **About The Company**........................................................................................... iv
4. **Introduction to Identity and Access Management** .......................................................**1**

1.1 Access Management................................................................................................1

1.2 Why Access Management?.......................................................................................1

1.3 Identity Lifecycle Management.................................................................................2

1.4 Multifactor Authentication.......................................................................................4

1.5 Privileged Access Management................................................................................6

1.6 Benefits of Identity and Access Management..............................................................7

1.7 Executive Summary of the Project............................................................................8

1.8 Objectives of the Project..........................................................................................9

1. **System Requirement Specification**..............................................................................10

2.1 Product Definition..................................................................................................10

2.2 Functions to be provided.........................................................................................10

2.3 Hardware and Software Requirements.......................................................................10

2.4 System Requirement Specification..........................................................................10

1. **Architecture**..............................................................................................................14
2. **Project Methodology...**..............................................................................................18

4.1 Test Plan..............................................................................................................18

1. **Screenshots**...............................................................................................................22
2. **Conclusion and Future Scope**....................................................................................26
3. **Reference**..................................................................................................................27

**LIST OF FIGURES**

1. Access Management.................................................................................................... 2
2. Identity Lifecycle Management.................................................................................... 4
3. Multifactor Authentication.......................................................................................... 5
4. Architecture of Sailpoint Identity IQ........................................................................... 14
5. Sailpoint Integration Architecture............................................................................... 15
6. IAM Solution Overview............................................................................................. 15
7. User Creation and provisioning solution diagram......................................................... 16
8. Role Based Access Control Solution diagram............................................................... 16
9. User Identity Maintenance and Audit diagram.............................................................. 17
10. User Termination Solution Overview........................................................................... 17

**IDENTITY AND ACCESS MANAGEMENT**

**INTRODUCTION**

**1.1 ACCESS MANAGEMENT**

Access is defined as the means or opportunity to approach or enter a place/application

Access management is the process of granting authorised users the right to use a service, while preventing access to non-authorised users. Access management can also be referred to as rights management or identity management. It is a task of identifying, tracking, controlling and managing authorized or specified users' access to a system, application or any IT instance. It is a broad concept that encompasses all policies, processes, methodologies and tools to maintain access privileges within an IT environment. Access management is primarily an information security, IT and data governance process used in granting access to valid users and prohibiting invalid users. Typically, AM is used in conjunction with identity access management (IAM). Identity management creates, provisions and controls different users, roles, groups and polices, whereas AM ensures that these roles and policies are followed. An AM-based application/system stores the different user roles and their profiles, and process user access requests based on the data/profile/roles.

Systems used for identity and access management include single sign-on systems, [multifactor authentication](https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA) and access management. These technologies also provide the ability to securely store identity and profile data as well as [data governance](https://searchdatamanagement.techtarget.com/definition/data-governance) functions to ensure that only data that is necessary and relevant is shared.

These products can be deployed on premises, provided by a third party vendor via a cloud-based subscription model or deployed in a hybrid cloud. Identity access management systems should include all the necessary controls and tools to capture and record user login information, manage the enterprise database of user identities and manage the assignment and removal of access privileges.

**1.2 WHY ACESS MANAGEMENT?**

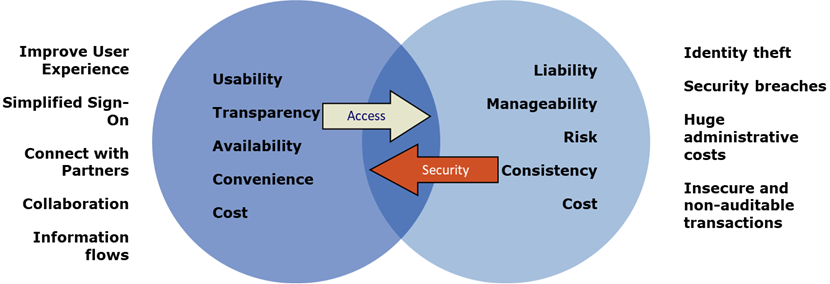
Effective IAM solutions help enterprises facilitate secure, efficient access to technology resources across these diverse systems, while delivering a number of important benefits:

**Improved data security:** Consolidating authentication and authorization functionality on a single platform provides IT professionals with a consistent method for managing user access. When a user leaves an organization, IT administrators may revoke their access in the centralized IAM solution with the confidence that this revocation will immediately take effect across all of the technology platforms integrated with that IAM platform.

**Reduced security costs:** Using a single IAM platform to manage all user access allows administrators to perform their work more efficiently. A security team may have some additional upfront work integrating new systems into an IAM platform but may then dedicate time to the management of that platform, saving time and money.

**More effective access to resources:** When users receive access through a centralized platform, they benefit from the use of single sign-on (SSO) technology that limits the number of interactions they have with security systems and increases the likelihood that their legitimate attempts to access resources will succeed.

These three benefits combine to demonstrate the importance of centralized identity and access management to the modern enterprise.



**Fig.1 : Access Management**

**1.3 IDENTITY LIFECYCLE MANAGEMENT**

Identity Lifecycle Management is a process where a user creation, managing , coordinating and restricting the identification, access and governance of identities to different tools / applications is performed using the different technologies.

 ILM encompasses the entire span of an employee's need to access critical business data, apps and tools in order to effectively perform their tasks and accomplish business objectives. It entails ensuring employees have access at various times and locations while logging, monitoring and restricting access when necessary to increase security and protect the enterprise's mission-critical data.

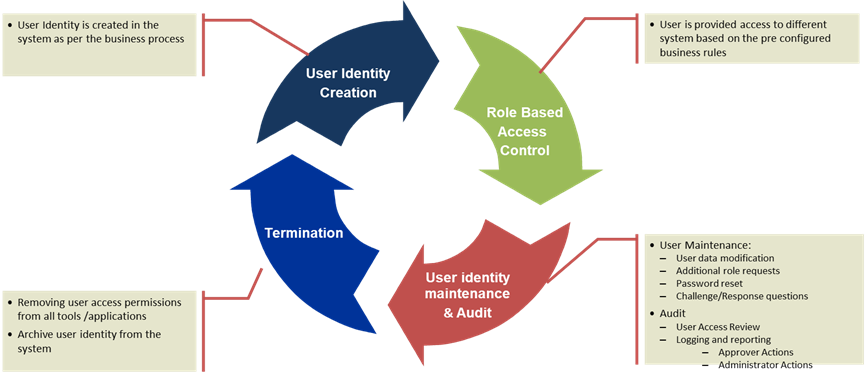
Identity Lifecycle Management also addresses the need for deprovisioning, or removing, access when an employee leaves the company or changes roles within the company.

Identity Management basically consists of below activities :

* **User Creation & Provisioning to target systems :-** User Identity is created in the system as per the business process
* **Role Based Access Control :-** Role-based access control (RBAC) is a method of regulating access to computer or network resources based on the roles of individual users within an enterprise. In this context, access is the ability of an individual user to perform a specific task, such as view, create, or modify a file. Roles are defined according to job competency, authority, and responsibility within the enterprise.

When properly implemented, RBAC enables users to carry out a wide range of authorized tasks by dynamically regulating their actions according to flexible functions, relationships, and constraints. This is in contrast to conventional methods of access control, which grant or revoke user access on a rigid, object-by-object basis. In RBAC, roles can be easily created, changed, or discontinued as the needs of the enterprise evolve, without having to individually update the privileges for every user.

* **User Identity Maintenance & Audit :-** Mover Life Cycle is called when a user is moving form Contractor to Permanent position. After approval, unwanted access is removed and new access is granted based on new position.
* **Termination :**- Termination/Leaver Life Cycle Event is triggered based on HR Termination date. Access to Managed Resources has be removed. Identity status is marked as “Terminated” .



**Fig.2 : Identity Lifecycle Management**

**1.4 MULTIFACTOR AUTHENTICATION**

One of the largest problems with traditional user ID and password login is the need to maintain a password database. Whether encrypted or not, if the database is captured it provides an attacker with a source to verify his guesses at speeds limited only by his hardware resources. Given enough time, a captured password database will fall.

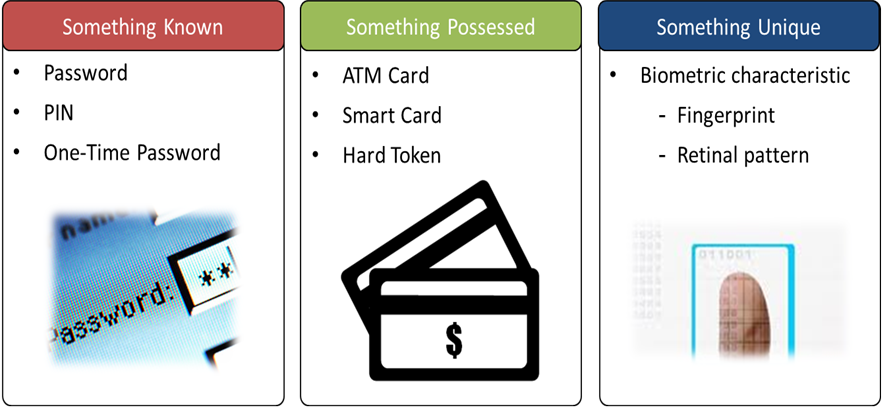
As processing speeds of CPUs have increased, brute force attacks have become a real threat. Further developments like GPGPU password cracking and rainbow tables have provided similar advantages for attackers. GPGPU cracking, for example, can produce more than 500,000,000 passwords per second, even on lower end gaming hardware. Depending on the particular software, rainbow tables can be used to crack 14-character alphanumeric passwords in about 160 seconds. Now purpose-built FPGA cards, like those used by security agencies, offer ten times that performance at a minuscule fraction of GPU power draw. A password database alone doesn't stand a chance against such methods when it is a real target of interest.

In the past, MFA systems typically relied upon two-factor authentication. Increasingly, vendors are using the label "multifactor" to describe any authentication scheme that requires more than one identity credential.

Multifactor authentication combines two or more independent credentials: what the user knows (password), what the user has (security token) and what the user is (biometric verification). The goal of MFA is to create a layered defence and make it more difficult for an unauthorized person to access a target such as a physical location, computing device, network or database. If one factor is compromised or broken, the attacker still has at least one more barrier to breach before successfully breaking into the target.

Typical MFA scenarios include:

* Swiping a card and entering a PIN.
* Logging into a website and being requested to enter an additional one-time password (OTP) that the website's authentication server sends to the requester's phone or email address.
* Downloading a VPN client with a valid digital certificate and logging into the VPN before being granted access to a network.
* Swiping a card, scanning a fingerprint and answering a security question.
* Attaching a USB hardware token to a desktop that generates a one-time pass code and using the one-time pass code to log into a VPN client.

****

**Fig.3 : Multifactor authentication**

**1.5 PRIVELEGED ACCESS MANAGEMEMT**

Privileged Access Management (PAM) is a solution that helps organizations restrict privileged access within an existing Active Directory environment.

Privileged Access Management accomplishes two goals:

* Re-establish control over a compromised Active Directory environment by maintaining a separate bastion environment that is known to be unaffected by malicious attacks.
* Isolate the use of privileged accounts to reduce the risk of those credentials being stolen.

PAM makes it harder for attackers to penetrate a network and obtain privileged account access. PAM adds protection to privileged groups that control access across a range of domain-joined computers and applications on those computers. It also adds more monitoring, more visibility, and more fine-grained controls. This allows organizations to see who their privileged administrators are and what are they doing. PAM gives organizations more insight into how administrative accounts are used in the environment.

PAM setup and operation has four steps.

1. **Prepare**: Identify which groups in your existing forest have significant privileges. Recreate these groups without members in the bastion forest.
2. **Protect**: Set up lifecycle and authentication protection, such as Multi-Factor Authentication (MFA), for when users request just-in-time administration. MFA helps prevent programmatic attacks from malicious software or following credential theft.
3. **Operate**: After authentication requirements are met and a request is approved, a user account gets added temporarily to a privileged group in the bastion forest. For a pre-set amount of time, the administrator has all privileges and access permissions that are assigned to that group. After that time, the account is removed from the group.
4. **Monitor**: PAM adds auditing, alerts, and reports of privileged access requests. You can review the history of privileged access, and see who performed an activity. You can decide whether the activity is valid or not and easily identify unauthorized activity, such as an attempt to add a user directly to a privileged group in the original forest. This step is important not only to identify malicious software but also for tracking "inside" attackers.

**1.6 BENEFITS OF IDENTITY AND ACCESS MANAGEMENT**

IAM technologies can be used to initiate, capture, record and manage user identities and their related access permissions in an automated manner. This ensures that access privileges are granted according to one interpretation of policy and all individuals and services are properly authenticated, authorized and audited.

Because companies that properly manage identities have greater control of user access, they're able to reduce the risks of internal and external [data breaches](https://searchsecurity.techtarget.com/definition/data-breach).

Automating IAM systems allows businesses to operate more efficiently by reducing the effort, time and money that would be required to manage access to their networks manually or via individual access controls that aren't connected to centralized management systems.

Using a common platform for identity and access management enables the same security policies to be applied across all the different devices and operating platforms used by the enterprise. In terms of security, use of an IAM framework can make it easier to enforce policies around user [authentication](https://searchsecurity.techtarget.com/definition/authentication), validation and privileges and address issues regarding privilege creep.

By implementing identity access management tools and following related best practices, a company can gain a competitive edge.

For example, IAM technologies allow the business to give users outside the organization, e.g., customers, partners, contractors and suppliers, access to its network across mobile applications, on-premises apps and [software-as-a-service](https://searchcloudcomputing.techtarget.com/definition/Software-as-a-Service) apps without compromising security. This enables better collaboration, enhanced productivity, increased efficiency and reduced operating costs.

Poorly controlled identity access management processes may lead to regulatory noncompliance because if the organization is audited, management will not be able to prove that company data is not at risk for being misused.

IAM systems help companies better comply with government regulations by allowing them to show that corporate information isn't being misused. With identity and access management tools, companies can also demonstrate that any data needed for auditing can be made available on-demand.

* 1. **Executive Summary of the Project:**

Identity and access management (IAM) is a framework for business processes that facilitates the management of electronic or digital identities. The framework includes the organizational policies for managing digital identity as well as the technologies needed to support identity management.

With IAM technologies, IT managers can control user [access](https://whatis.techtarget.com/definition/access) to critical information within their organizations. Identity and access management products offer [role-based access control](https://searchsecurity.techtarget.com/definition/role-based-access-control-RBAC), which lets system administrators regulate access to systems or networks based on the roles of individual users within the enterprise.In this context, access is the ability of an individual user to perform a specific task, such as view, create or modify a file. Roles are defined according to job competency, authority and responsibility within the enterprise.

Systems used for identity and access management include [single sign-on](https://searchsecurity.techtarget.com/definition/single-sign-on) systems, [multifactor authentication](https://searchsecurity.techtarget.com/definition/multifactor-authentication-MFA) and access management. These technologies also provide the ability to securely store identity and profile data as well as [data governance](https://searchdatamanagement.techtarget.com/definition/data-governance) functions to ensure that only data that is necessary and relevant is shared.

Identity access management systems include all the necessary controls and tools to capture and record user login information, manage the enterprise database of user identities and manage the assignment and removal of access privileges. That means that systems used for IAM provide a centralized directory service with oversight as well as visibility into all aspects of the company user base.

IAM systems are used to provide flexibility to establish groups with specific privileges for specific roles so that access rights based on employee job functions can be uniformly assigned. The system also provides request and approval processes for modifying privileges because employees with the same title and job location may need customized, or slightly different, access.

**1.8 Objectives of the Project:**

* To initiate, capture, record and manage user identities and their related access permissions in an automated manner.
* To ensure that access privileges are granted according to one interpretation of policy and all individuals and services are properly authenticated, authorized and audited.
* To have greater control of user access, hence being able to reduce the risks of internal and external [data breaches](https://searchsecurity.techtarget.com/definition/data-breach) in an organisation.
* IAM systems allows businesses to operate more efficiently by reducing the effort, time and money that would be required to manage access to their networks manually or via individual access controls that aren't connected to centralized management systems.
* Using a common platform for identity and access management enables the same security policies to be applied across all the different devices and operating platforms used by the enterprise.
* IAM systems help companies better comply with government regulations by allowing them to show that corporate information isn't being misused.
* With identity and access management tools, companies can also demonstrate that any data needed for auditing can be made available on-demand.

**Proposed System:**

The IAM tool enables initiating, storing and managing user identities and access permissions. IAM ensures that users are who they say they are (authentication) and that they can access the applications and resources they have permission to use (authorization). First aggregation occurs from an authoritative source (trusted source) to the IAM space wherein the identities are created. Then comes the part where roles specific to the identities have to be managed and thereafter access to an application and its resources are provided based on the roles allocated to the identity.

**2. SYSTEM REQUIREMENT SPECIFICATION**

**2.1 Product Definition:**

SailPoint’s IdentityIQ is an IAM tool that can be used to create identities and is a complete governance-based IAM solution that provides fast, convenient access that keeps business users productive, and access controls that keep the business safe. IdentityIQ integrates compliance management and provisioning in a unified solution that leverages a common identity governance framework.Sailpoint concentrates on governance which includes provisioning, password management, reporting, certification, audit, self service and role mining and is delivering user friendly, feature rich and offering robust tool called IdentityIQ.

**2.2 Functions to be provided:**

* IdentityIQ mitigates risk of inappropriate access by centralizing visibility to users and their access across cloud and on-premises applications and data.
* It boosts productivity while reducing costs by empowering users to request/approve access and manage passwords from any device.
* It improves audit performance by automating compliance controls and audit reporting.
* Certifications can be done in order to check whether the right person has the right access to the right resource at the right time.

**2.3 Hardware and Software Requirements:**

* **Hardware Requirements:**
* Hardware: Enterprise Server
* Speed: ~3.0 GHz
* RAM: >16 GB
* **Software Requirements:**
* Operating System (client preferred)
* MYSQL Server
* IdentityIQ Database

**2.4 System Requirement Specification:**

A System Requirements Specification (SRS) (also known as a Software Requirements Specification) is a document or set of documentation that describes the features and behaviour of a system or software application. It includes a variety of elements (see below) that attempts to define the intended functionality required by the customer to satisfy their different users. In addition to specifying how the system should behave, the specification also defines at a high-level the main business processes that will be supported, what simplifying assumptions have been made and what key performance parameters will need to be met by the system.

**Main Elements**

Depending on the methodology employed (agile vs waterfall) the level of formality and detail in the SRS will vary, but in general, an SRS should include a description of the functional requirements, system requirements, technical requirements, constraints, assumptions and acceptance criteria. Each of these is described in more detail below:

* **Business Drivers** - This section describes the reasons why the customer is looking to build the system. The rationale for the new system is important as it will guide the decisions made by the business analysts, system architects and developers. Another compelling reason for documenting the business rationale behind the system is that the customer may change personnel during the project. Documentation which clearly identifies the business reasons for the system will help sustain support for a project if the original sponsor moves on. The drivers may include both problems (reasons why the current systems/processes are not sufficient) and opportunities (new business models that the system will make available). Usually a combination of problems and opportunities are needed to provide motivation for a new system.
* **Business Model** - This section describes the underlying business model of the customer that the system will need to support. This includes such items as the organizational context, current-state and future-state diagrams, business context, key business functions and process flow diagrams. This section is usually created during the functional analysis phase.
* **Functional and System Requirements** - This section usually consists of a hierarchical organization of requirements, with the business/functional requirements at the highestlevel and the detailed system requirements listed as their child items. Generally the requirements are written as statements such as "System needs the ability to do x" with supporting detail and information included as necessary.
* **Business and System Use Cases** - This section usually consists of a UML use case diagramthat illustrates the main external entities that will be interacting with the system together with the different use cases (objectives) that they will need to carry out. For each use-case there will be formal definition of the steps that need to be carried out to perform the business objective, together with any necessary pre-conditions and postconditions. The business use cases are usually derived from the functional requirements and the system use cases are usually derived from the system requirements.
* **Technical Requirements** - This section is used to list any of the "non-functional" requirements that essentially embody the technical environment that the product needs to operate in, and include the technical constraints that it needs to operate under. These technical requirements are critical in determining how the higher-level functional requirements will get decomposed into the more specific system requirements.
* **System Qualities** -This section is used to describe the "non-functional" requirements that define the "quality" of the system. These items are often known as the "-ilities" because most of them end in "ility". They included such items as: reliability, availability, serviceability, security, scalability, maintainability.
* **Constraints and Assumptions** -This section will outline any design constraints that have been imposed on the design of the system by the customer, thereby removing certain options from being considered by the developers. Also this section will contain any assumptions that have been made by the requirements engineering team when gathering and analyzing the requirements. If any of the assumptions are found to be false, the system requirements specification would need to be re-evaluated to make sure that the documented requirements are still valid.
* **Acceptance Criteria** -This section will describe the criteria by which the customer will "sign-off" on the final system. Depending on the methodology, this may happen at the end of the testing and quality assurance phase, or in an agile methodology, at the end of each iteration. The criteria will usually refer to the need to complete all user acceptance tests and the rectification of all defects/bugs that meet a pre-determined priority or severity threshold.

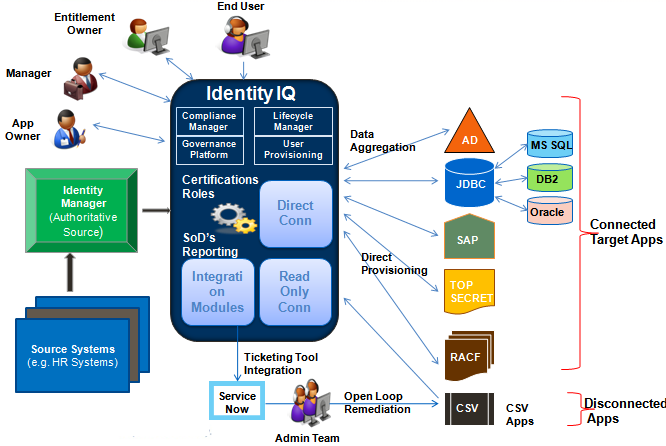
**Alternatives**

In agile methodologies such as extreme programming or scrum formal, static documentation such as a software requirements specification (SRS) are usually eschewed in favour of a more lightweight documentation of the requirements, namely by means of user stories and acceptance tests.

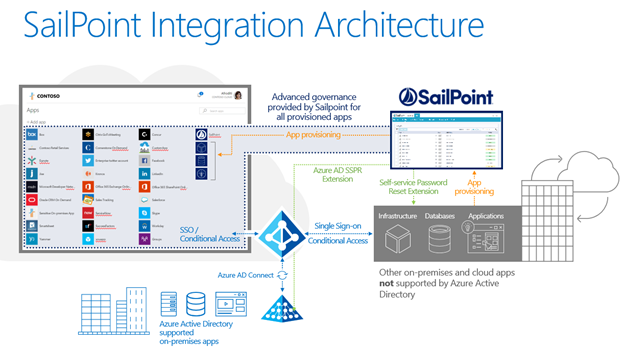
This approach requires that the customer is easily accessible to provide clarification on the requirements during development and also assumes that the team members responsible for writing the user stories with the customer will be the developers building the system. A more formal approach may be needed if the customer is inaccessible and/or a separate team of business analysts will be developing the requirements.

In Rapid Application Development (RAD) methodologies such as DSDM or Unified Process (RUP, AUP) the requirements specification is often kept at a higher-level with much of the detailed requirements embodied in prototypes and mockups of the planned system.

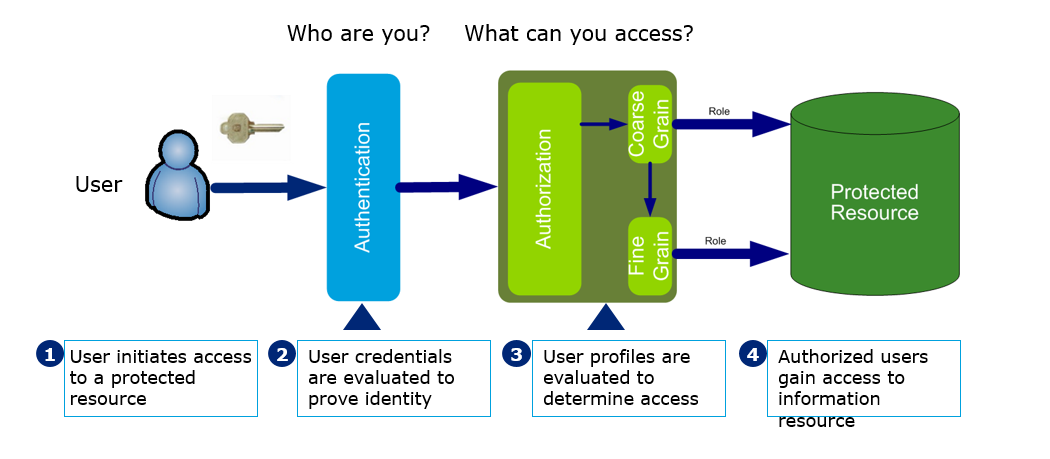
**3. ARCHITECTURE**

****

**Fig.4 : Architecture of Sailpoint Identity IQ**

****

**Fig.5 : Sailpoint Integration Architecture**



**Fig.6 : IAM solution overview**



**Fig. 7 : User Creation and provisioning solution diagram**

****

**Fig.8 : Role Based Access Control (RBAC) solution diagram**

****

**Fig.9 : User Identity Maintenance and Audit Diagram**

****

**Fig.10 : User Termination Solution Overview**

**4. PROJECT METHODOLOGY**

**4.1 Test Plan:**

A Software Test Plan is a document describing the testing scope and activities. It is the basis for formally testing any software/product in a project.

* **Test plan:** A document describing the scope, approach, resources and schedule of intended test activities. It identifies amongst others test items, the features to be tested, the testing tasks, who will do each task, degree of tester independence, the test environment, the test design techniques and entry and exit criteria to be used, and the rationale for their choice, and any risks requiring contingency planning. It is a record of the test planning process.
* **Master Test plan:**A test plan that typically addresses multiple test levels.
* **Phase Test plan:**A test plan that typically addresses one test phase.

**Test Plan Types**

One can have the following types of test plans:

* Master Test Plan: A single high-level test plan for a project/product that unifies all other test plans.
* Testing Level Specific Test Plans:Plans for each level of testing.
* Unit Test Plan
* Integration Test Plan
* System Test Plan
* Acceptance Test Plan
* Testing Type Specific Test Plans: Plans for major types of testing like Performance Test Plan and Security Test Plan.

**Test Plan Template**

The format and content of a software test plan vary depending on the processes, standards, and test management tools being implemented. Nevertheless, the following format, which is based on IEEE standard for software test documentation, provides a summary of what a test plan can/should contain.

**Test Plan Identifier:**

* Provide a unique identifier for the document. (Adhere to the Configuration Management System if you have one.)

**Introduction:**

* Provide an overview of the test plan.
* Specify the goals/objectives.
* Specify any constraints.

**References:**

* List the related documents, with links to them if available, including the following:
* Project Plan
* Configuration Management Plan

**Test Items:**

* List the test items (software/products) and their versions.

**Features to be tested:**

* List the features of the software/product to be tested.
* Provide references to the Requirements and/or Design specifications of the features to be tested.

**Features not to be tested:**

* List the features of the software/product which will not be tested.
* Specify the reasons these features won’t be tested.

**Approach:**

* Mention the overall approach to testing.
* Specify the testing levels [if it’s a Master Test Plan], the testing types, and the testing methods [Manual/Automated; White Box/Black Box/Gray Box]

**Item Pass/Fail Criteria:**

* Specify the criteria that will be used to determine whether each test item (software/product) has passed or failed testing.

**Suspension Criteria and Resumption Requirements:**

* Specify criteria to be used to suspend the testing activity.
* Specify testing activities which must be redone when testing is resumed.

**Test Deliverables:**

* List test deliverables, and links to them if available, including the following:
* Test Plan (this document itself)
* Test Cases
* Test Scripts
* Defect/Enhancement Logs
* Test Reports

**Test Environment:**

* Specify the properties of test environment: hardware, software, network etc.
* List any testing or related tools.

**Estimate:**

* Provide a summary of test estimates (cost or effort) and/or provide a link to the detailed estimation.

**Schedule:**

* Provide a summary of the schedule, specifying key test milestones, and/or provide a link to the detailed schedule.

**Staffing and Training needs:**

* Specify staffing needs by role and required skills.
* Identify training that is necessary to provide those skills, if not already acquired.

**Responsibilities:**

* List the responsibilities of each team/role/individual.

**Risks:**

* List the risks that have been identified.
* Specify the mitigation plan and the contingency plan for each risk.

**Assumptions and Dependencies:**

* List the assumptions that have been made during the preparation of this plan.
* List the dependencies.

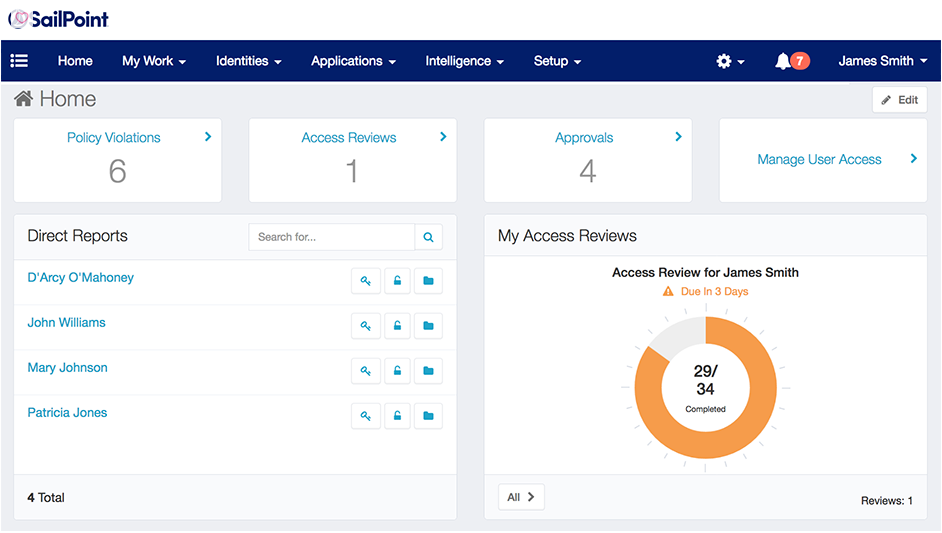
**Approvals:**

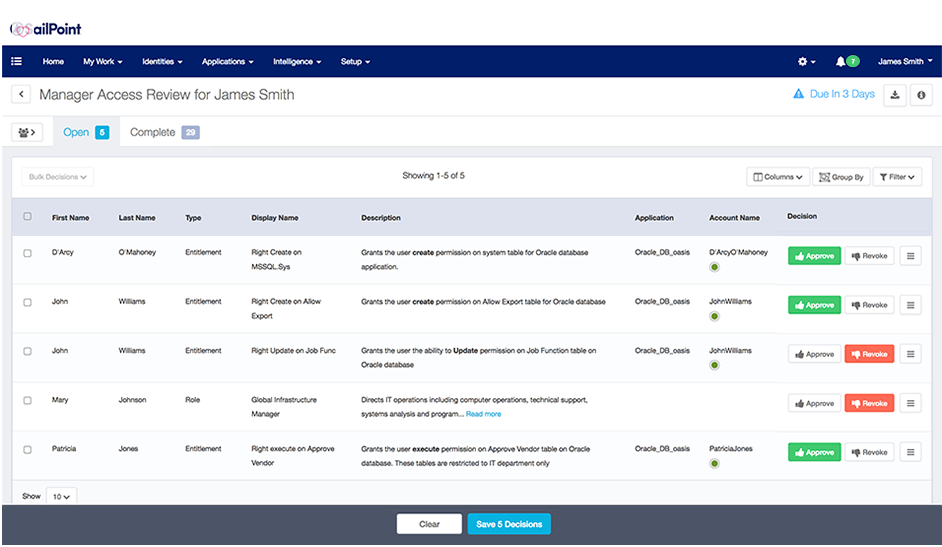
* Specify the names and roles of all persons who must approve the plan.
* Provide space for signatures and dates. (If the document is to be printed.)

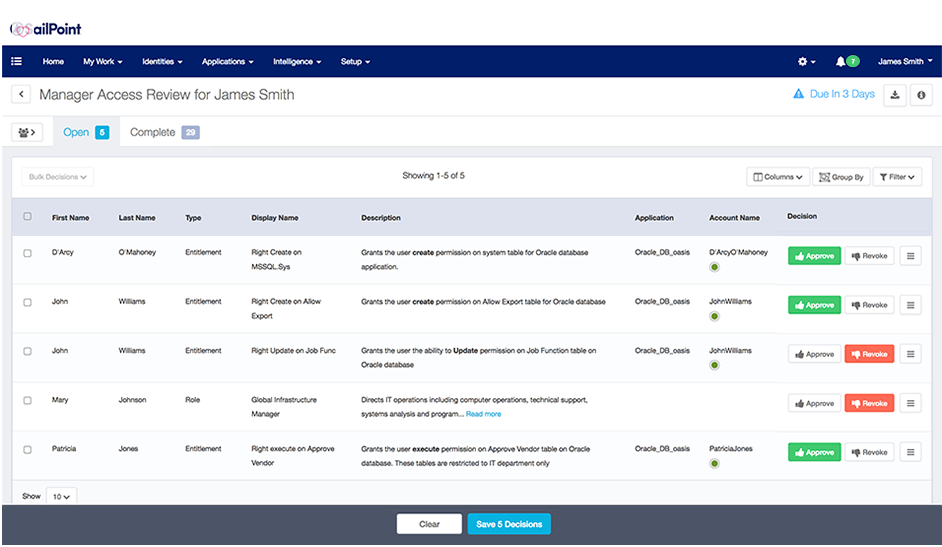
**Test Plan Guidelines**

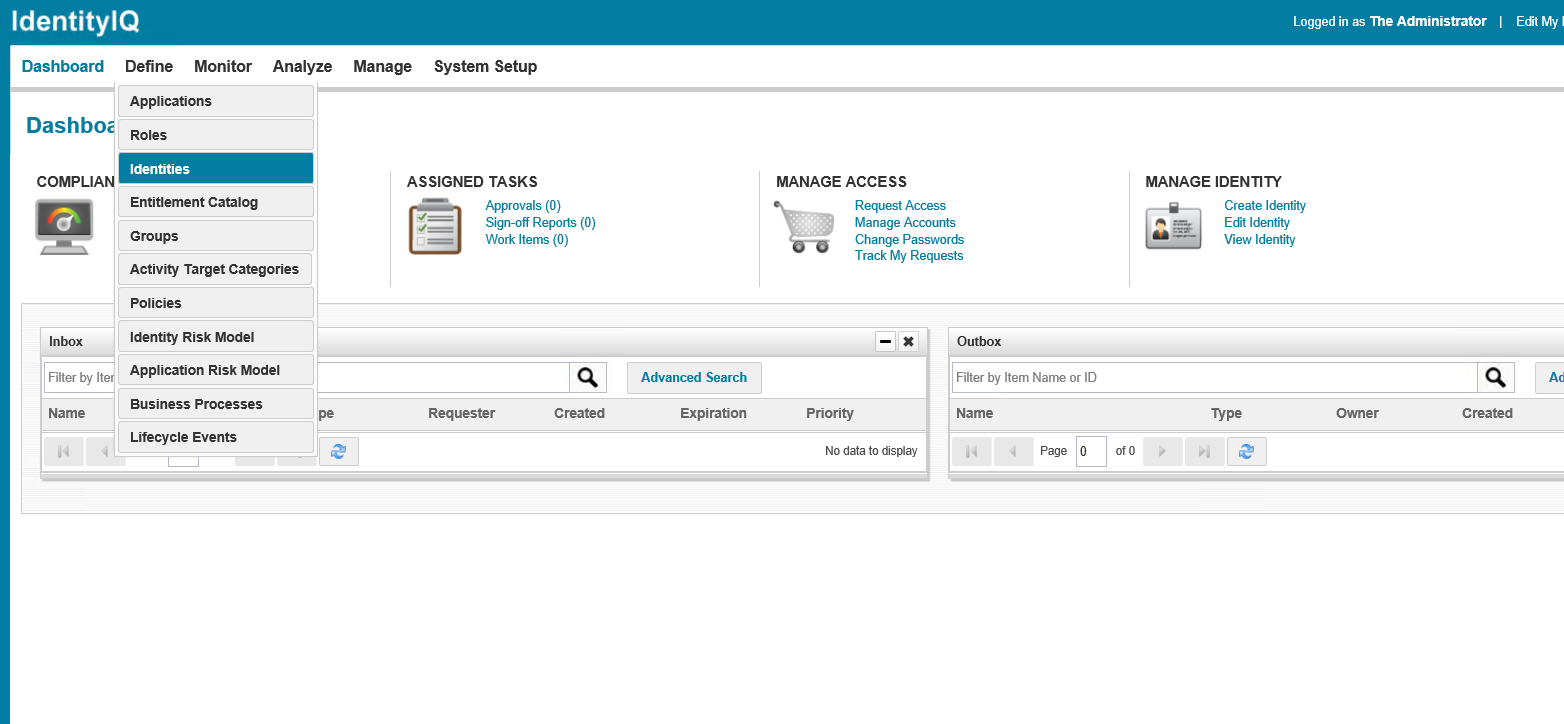
* Make the plan concise. Avoid redundancy and superfluousness. If you think you do not need a section that has been mentioned in the template above, go ahead and delete that section in your test plan.
* Be specific. For example, when you specify an operating system as a property of a test environment, mention the OS Edition/Version as well, not just the OS Name.
* Make use of lists and tables wherever possible. Avoid lengthy paragraphs.
* Have the test plan reviewed a number of times prior to base lining it or sending it for approval. The quality of your test plan speaks volumes about the quality of the testing you or your team is going to perform.
* Update the plan as and when necessary. An out-dated and unused document stinks and is worse than not having the document in the first place.

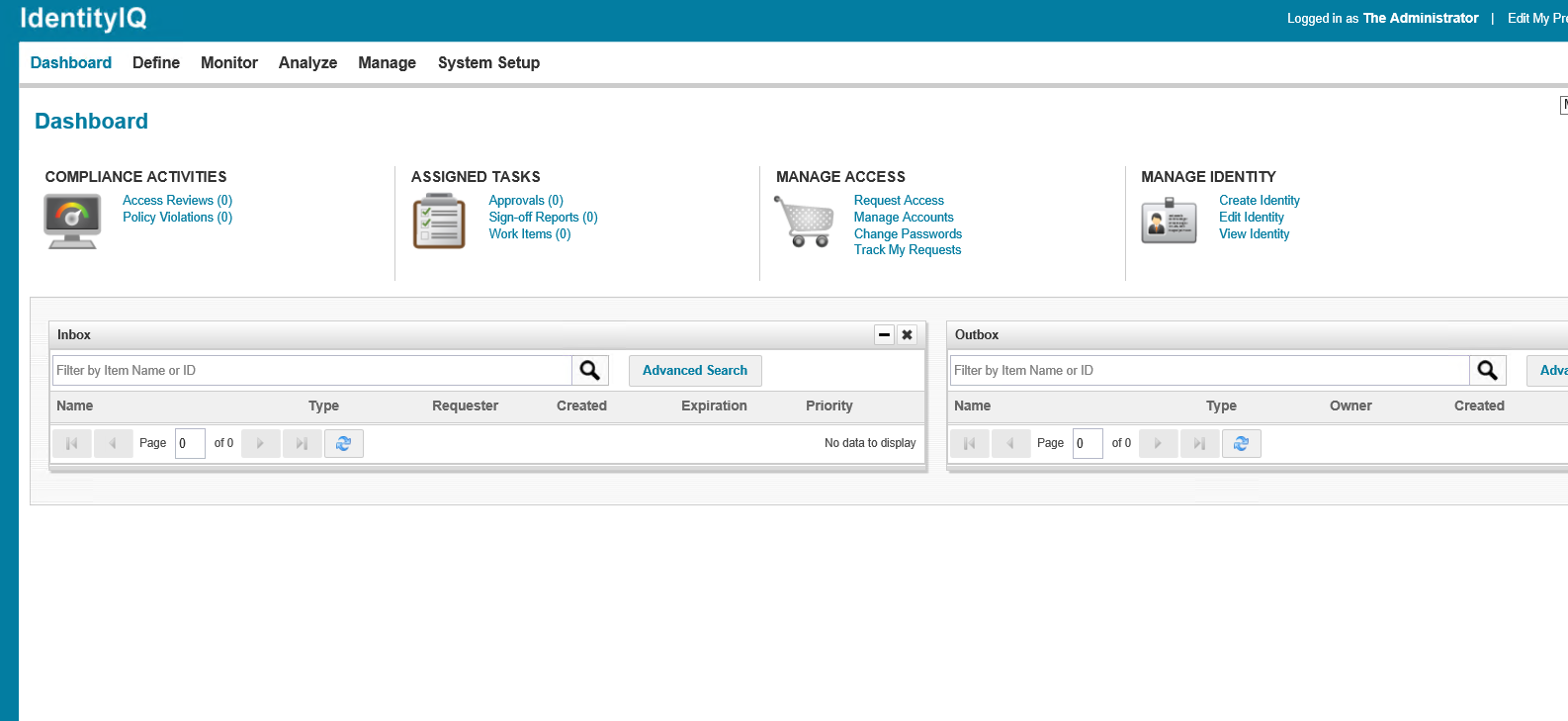
1. **SCREENSHOTS**

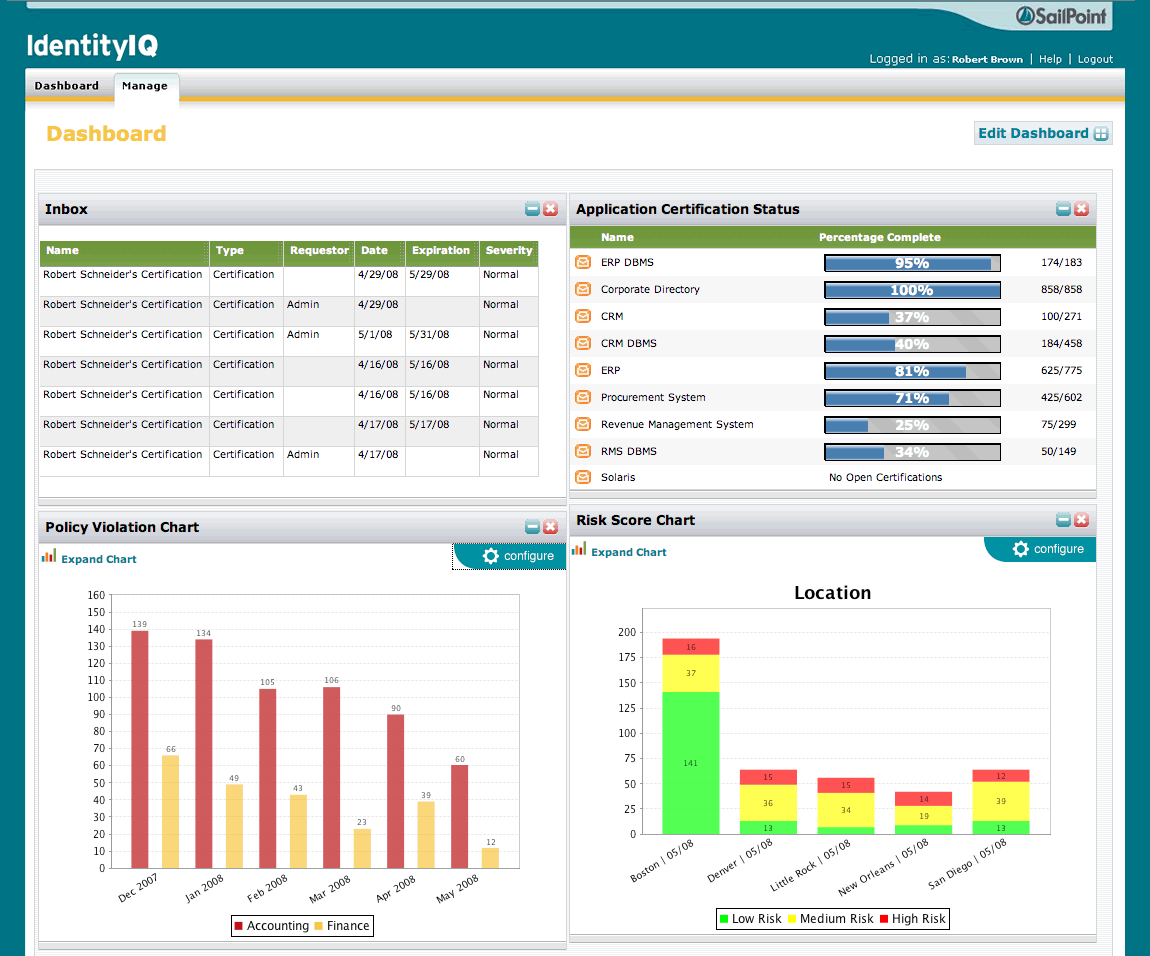
****

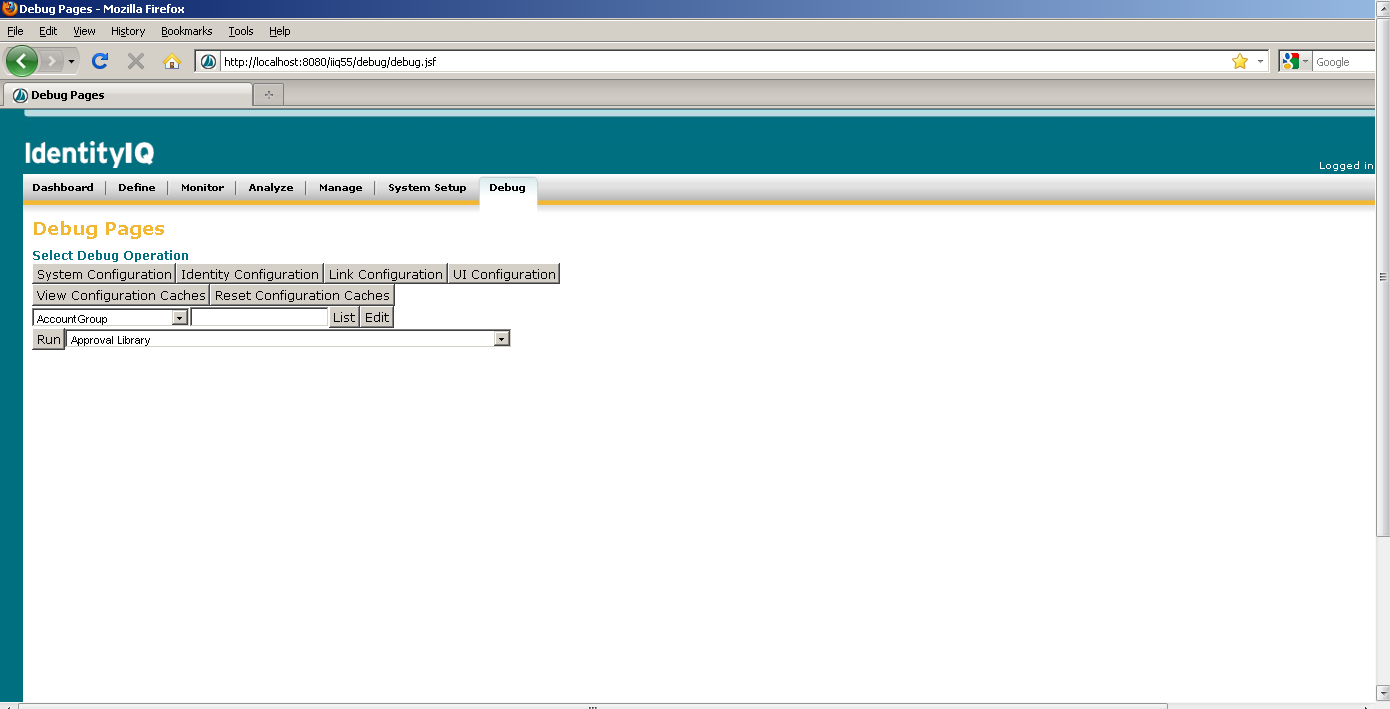
****

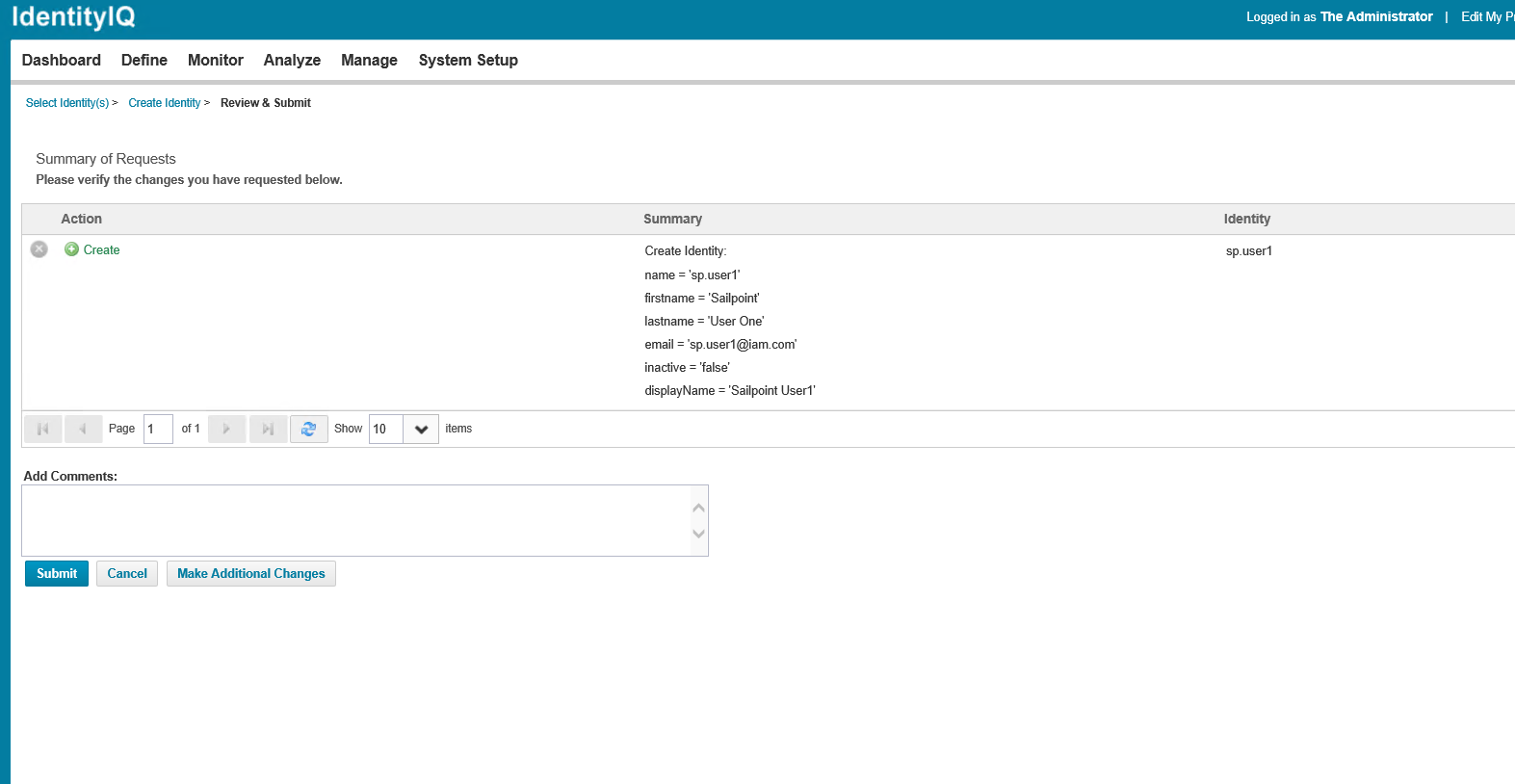
****

****









1. **CONCLUSION AND FUTURE SCOPE**

This case study and implementation of Identity and Access Management solution with the help of Sailpoint IdenityIQ helped us to understand the infrastructure, resources and effort required to implement an Identity and Access Management solution with scratch. Moreover, it thought us how to interact with clients and help our clients to refine their requirements and make informed decisions on as to which vendor to prefer while implementing the solution. We learned how to set up Sailpoint IdentityIQ and deploy it on client servers. We learned how to perform application on boarding, certifications, reports, life cycle management on Sailpoint IdentityIQ.

Identity and Access Management (IAM) is bound to be increasingly an integral part of our personal and business lives as the technological and societal landscape continues to rapidly change. Although we can not fully and accurately predict anything beyond the near future, it is likely that technology will continue to change our lives in future years which will require a new approach to identity and access management.

“When considering that users’ inability to protect and manage passwords causes over 90% of cyber-attacks, it is evident that our current IAM approach which mostly uses passwords for authentication cannot support the security of the future state where many devices will be interconnected” says Henry Bagdasarian, Founder of Identity Management Institute and cybersecurity thought leader.

For example, IAM will expand beyond humans, pets, and other living things to include identities of robots and smart devices. Anything that needs to be connected to something for data sharing and automated tasks will be connected to make human lives easier, collaborative, and more productive.

As distributed and interconnected systems increase in numbers, seamless, continuous, and accurate access to all resources with advanced authentication systems such as biometric and artificial intelligence technology will be prevalent. Password will be the thing of the past as user controlled access will be replaced by machine controlled access management. There will be no more passwords to access systems or badges to enter buildings. Smart systems will be able to recognize and greet us using some of our personal and distinct features when we use ATMs, enter stores and restaurants, visit online websites, enter office locations, drive cars, and access business systems.

Identity management and artificial intelligence will revolutionize security beyond people, places, and things that we manage today as increasing number of devices and systems will communicate with and learn from one another without human intervention. For example, household systems which will be a big part of the Internet of Things will communicate with each other to control and manage our lives. Refrigerators will order food items when the inventory goes down, fire detection systems will contact the fire department and other nearby households in case of fire, doctors will be notified when our vital signs show trouble and much more. Almost everything will have an identity which will change today’s definition of identity theft.

Form a business standpoint, distributed and trusted identity concept will be adopted by every object, service, and system.  A person may have multiple identities but still be recognized as the person and the identities of smart things will be linked to persons owning the objects. With the increasing number of highly potent identities, global identity service providers will register identities and maintain identity directories.

**7. REFERENCE**

1. Sergiy Fefilatyev, “Algorithms for Visual Maritime Surveillance with Rapidly Moving Camera”, Doctoral dissertation, University of South Florida, 2012.
2. Domenico Bloisi, Luca Iocchi, Michele Fiorini, Giovanni Graziano, “Automatic Maritime Surveillance with Visual Target Detection”, International Defense and Homeland Security Simulation Workshop (DHSS), September 2011.
3. Domenico Bloisi, Luca Iocchi, Michele Fiorini, Giovanni Graziano, “Camera Based Target Recognition for Maritime Awareness”, Information Fusion (FUSION), 15th International Conference, July 2012.

[4]. Rodrigo Da Silva Moreira, Nelson Francisco Favilla Ebecken, Alexandre Soares Alves, Frédéric Livernet4, Aline Campillo-Navetti, “A Survey on Video Detection and Tracking of Maritime Vessels”, IJRRAS 20, July 2014.

1. Digi-key Corporation. <http://www.digikey.com/>
2. Alldatasheet. <http://www.alldatasheet.com/>