ITMR

योगः कर्मसु कौशलम्

WHITE PAPER ON

Identity & Access Management

Prepared by **Mohammed Samiuddin**

Contents

INTRODUCTION 2

IDENTITY AND ACCESS MANAGEMENT FRAMEWORK 3

AUTHENTICATION 3

AUTHORISATION 3

USER MANAGEMENT 4

CENTRAL USER REPOSITORY 4

IDENTITY AND ACCESS MANAGEMENT IN CLOUD 5

BEST PRACTICES IN IDENTITY AND ACCESS MANAGEMENT 6

LIMITATIONS OF IDENTITY AND ACCESS MANAGEMENT 7

CONCLUSION 7

ABOUT THE AUTHOR 8

REFERENCE 8

ABOUT ITMR 8

Introduction

To meet the challenges of today's world, organisations increase their business agility in secure environment and also invest huge sum in their IT infrastructure. The biggest challenge in information security is Identity and Access Management (IAM). In the recent years, IAM has emerged as the critical foundation for realising the business benefits in terms of cost savings, management control, and operational efficiency. Access to the information are scattered across the internal and external applications systems; thus, it is the responsibility of the organisation to manage them effectively.

IAM is the security discipline that authorises users to access corporate systems and information. It helps prevent fraudulent access and use of data that could potentially impact the business, its partners, or its customers. Any organisation that has less effective IAM is highly prone to security risks.

Identity and Access Management Framework

The main objective of IAM is to provide the right people with the right information at the right time. For the IAM framework to function properly, organisations must ensure correctness of the data. IAM components can be classified into four major categories: Authentication, Authorisation, User Management, and Central User Repository (Enterprise Directory).

Authentication

Authentication is the process of evaluating access credentials provided by the user. All the users need to be validated; users can be a person or an application. Authentication usually comprises of authentication management and session management. In this process, every user is authenticated and a session is created. User and the application interact through these sessions until the user logs off or the session is terminated due to time out. Authentication has become easier over the past few years, since more operating systems and applications now support technologies such as Active Directory (AD), LDAP, and Single Sign On / federation. Currently, organisations insist on "Strong Authentication", which refers to multi-factor authentication or authentication protected by cryptographic means. However, authenticating users in manageable and trustworthy manner has become a challenge with the evolution of new technologies like cloud computing.

Authorisation

Authorisation is the process of mapping the actions that a user is allowed to take in terms of access to services or processing steps. Therefore, authorisation is the module that determines whether a user is permitted to access a particular resource. Authorisation must be flexible enough to provide both general and precise access to resources. For example, general access allows all employees have access to a particular application, whereas precise access only allows employees in a specific department to perform a certain operation in an application between the hours of 9 AM and 5 PM. Users should map logically to roles, such as database administrator, helpdesk operator, or application user within the context of an organisation or application. Authorisation presents a larger issue than authentication because, most applications are not leveraging directory services. Rather, they have their own built-in authorisation systems.

Identity and Access Management Framework

User Management

User Management is an authentication feature that provides administrators with the ability to identify and control the state of users logged into the application. This module comprises of user management, password management, and user/group provisioning. User management functionalities include identity creation, propagation, and maintenance of user identity and privileges. The key benefit of User Management is visibility into active user sessions. This can be useful for identifying the general login status of users or for making real-time decisions such as immediately logging off a user. Self-service is another key benefit within user management, one such is the self-password reset which significantly alleviates the help desk workload to handle password reset requests.

Central User Repository

Central User Repository holds all the user identity information. Responsibilities of Central User Repository include, delivering identity information to other services and verifying credentials submitted by the users. Disparate identity data from different user repositories of applications and systems can be handled by Meta-Directory and Virtual Directory. Meta-Directory synchronises data from one or more external data sources into a single repository, providing an aggregate set of identity data. On the other hand, Virtual Directory delivers a unified LDAP view of consolidated identity information.

Identity and Access Management in Cloud

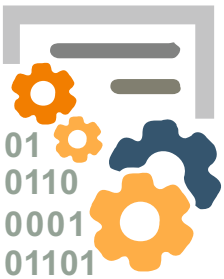
The Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS), (SPI) cloud delivery models call for IT departments and the Cloud Service Provider (CSP) to jointly extend the organisation's IAM practices, processes, and procedures to cloud services in ways that are scalable, effective, and efficient for both the provider and its customers. One of the major challenges for organisations adopting cloud computing services is the secure and timely management of on-boarding (provisioning) and off-boarding (de-provisioning) of users in the cloud. In addition to this, organisation tends to move their existing systems to cloud. One of the vital requirements while utilising cloud is authenticating users in manageable and trustworthy manner.

The access control requirements in SPI (SaaS, PaaS, and IaaS) environments include establishing trusted user profile and policy information, which is used to control access within the cloud service. For organisations that rely on cloud, it is important to understand how identity management can enable compliance with internal or regulatory requirements. Well-designed identity management can ensure that information about accounts, access grants, and segregation of duty enforcement at cloud providers, can all be pulled together to satisfy an organisation's audit and compliance reporting requirements.

Best Practices in Identity and Access Management

To follow the hybrid nature of current technologies, organisations are forced to develop strategies in managing user identities and access to IT resources. The key task is managing access to applications and organisation data from different locations and devices without compromising on security.

- Wide range of users access various applications and managing the users requires more effort. A robust IAM system ensures the software applications are updated as necessary and eliminates the requirement of manual intervention for provisioning and de-provisioning of users.
- Accessing various applications and pages from different devices has become a necessity in the current world. Most of the applications require credentials to access, and remembering passwords is a challenge. IAM reduces the effort required by providing Single Sign On facility.
- Using the advanced technologies, users are allowed to access applications remotely from different devices using different browsers. IAM takes the responsibility of handling access requests from disparate browsers without compromising on security.
- A successful cloud infrastructure hosting must allow for integration of applications and frequent changes
- Using cloud-based applications allows to pay for usage, in such cases, the IT departments are not able to trace the consumption levels. An Enterprise IAM solution must provide detailed reports on utilisation of resources
- Efforts required in managing the reconciliation tasks should be avoided by automating the processes



Limitations of Identity and Access Management

Complexity:

Large organisations face challenges in identifying the job roles of employees and mapping them to appropriate level of access. For example: Two different resources with same designation may be performing different tasks and mapping them to applications for which they require access is not so easy. Role-based identity is highly complex and difficult to manage.

Underestimating the need for IAM:

Many business leaders underestimate the need of identity and access management. Organisations adoption to identity and access management requires a lot of effort.

Conclusion

Business demands and regulatory compliance require organisations to take a comprehensive approach to identity and access management. Implementation of IAM depends not only on the organisation IT team, but also on the management. In today's world, market changes rapidly. Therefore, it is the need for the organisation to implement a better IAM strategy - one that aligns with specific business needs without significantly increasing costs or risk. The implementation of IAM is a difficult project; however, it cannot be put at the bottom of the list due to resource or financial constraint.

IAM will be effectively implemented only when organisations realise nothing is of higher priority than protecting the sensitive data. As IT organisations look to fully implement IAM while being pressured to manage expenses and head count, a hosted IAM solution will be the right choice. This is where cloud can be a valuable idea for an organisation. Hosted or In-house, an effective IAM is always a boon for organisations.

About the Author

Mohammed Samiuddin spearheads the branding aspects & managing client relationships of ITMR. His passion includes speaking on cyber security threats, data security practices and new technological areas.

Reference

http://www.karingroup.com/eng/about/what_is_identity.pdf

http://blogs.rsa.com/adaptive-iam-on-the-front-lines-of-cyber-security/

http://www.incommon.org/docs/iamonline/20130410-IAM-Online.pdf

http://www.verizonenterprise.com/resources/whitepapers/wp_identity-and-access-mgmt-imperative_en_xg.pdf

http://www.okta.com/pdf/Okta_Whitepaper_Top_8.pdf

https://identacor.com/blog/best-practices-to-implement-safer-identity-and-access-management/

http://www.csoonline.com/article/2132719/federated-identity/three-id-management-challenges.html

About ITMR

Institute of Technology, Management and Research (ITMR), a division of Mamta Trust, is a premier institute that provides world class professional training programs for the corporates and academic sector. ITMR's motto 'yogah karmasu kausalam' means 'Yoga is excellence in action' and is the foundation of its vision to evolve into a "CENTRE OF EMINENCE" to offer cutting edge vocational skills and mold professionals to become business and technical domain experts. ITMR's professional and corporate training programs include several cutting edge to help working professionals acquire domain expertise and meet the current and emerging challenges in the IT world.

Our flagship training program on Cyber security has (PDCIL) Professional Diploma in Cyber Investigations and Laws is a top of the class cyber security program in the country that trains top officials in the Police departments, Indian and International Banks, Military, Legal fraternity, Fortune 100 Global companies and Blue Chip India IT companies.

ITMR also offers research programs on Cyber Security (network security monitoring and access products), in association with Secure IQ, a leading provider of network security software products with headquarters in Fairfax, Virginia, USA and operations and development in Chennai, India.

Institute of Technology Management & Research

(Division of Mamta Trust)

2/850, Mugaliwakkam Road, Mugaliwakkam, Chennai - 600 125, Tamil Nadu, INDIA.
Admin Office: HTC Towers, No.41, GST Road, Guindy, Chennai – 600 032,
Tamil Nadu, INDIA. Phone: +91 44 4345 3500 / +91 44 4345 3349
Contact for More Information: training@htcitmr.ac.in