Portfolio Assignment

Identity Management – CYBR 3030

Arr Domingo

Student ID: 200458099

Instructor: Sam El-Awour

Table of Contents

[Introduction 1](#_Toc209136606)

[IAM Fundamentals 2](#_Toc209136607)

[1.0 Foundations of Identity & Access Management (IAM) 2](#_Toc209136608)

[2.0 Authentication Mechanism & Management 3](#_Toc209136609)

[3.0 Authorization & Accountability 4](#_Toc209136610)

[4.0 Managing IAAA in Windows 5](#_Toc209136611)

[5.0 Managing IAAA in Linux 5](#_Toc209136612)

[Enterprise IAM 5](#_Toc209136613)

[6.0 Enterprise Identity Repository 5](#_Toc209136614)

[7.0 Privileged Access Management 5](#_Toc209136615)

[8.0 Enterprise Password Policy Management 5](#_Toc209136616)

[9.0 Integrated Access Management & IDM 5](#_Toc209136617)

[10.0 Applying Access Management & IDM 5](#_Toc209136618)

[11.0 Network Authentication & Access Protocol 5](#_Toc209136619)

[IAM Governance 5](#_Toc209136620)

[12.0 Data Ownership & Access Validation 5](#_Toc209136621)

[13.0 Identity & Access Validation 5](#_Toc209136622)

[14.0 Segregation of Duties & Job Rotation 5](#_Toc209136623)

# Introduction

In today’s digital age, organizations are exposed to an intentional and unauthorized actions against a computer system or network to compromise its data or functionality. Such action includes cyberattack, cyber intrusion, security breach, malicious hacking, and unauthorized access.

Having a solid policies and security architecture that will safeguard organization’s management of digital identities is the key role of Identity Management. The goal is to keep data and systems secure by managing network users and devices an access to internal resources. This means that a process must be implemented to properly identify, authenticate, and authorize people, groups of people, or software applications including user access rights and restriction, which will ensure that users have an appropriate access to the right resources at the right time.

Essentially, identity management is to guarantee that all company networks, system applications and internal resources are not only protected but also accessible for necessary users. Without a system in place, this would be an extremely complex and time-consuming process. Therefore, it is a critical component within the IT security space that a strong strategy will establish the first line of protection for organization’s networks and resources.

Lastly, this document will cover the core security principles of Identification, Authentication, Authorization, and Accountability (IAAA). These principles form the foundational pillars of identity and access management (IAM) in cybersecurity, which is vital for managing the access control to avoid risks.

# IAM Fundamentals

One of the crucial components of an organization’s security strategy is often referred to as Identity and Access Management (IAM). IAM ensures that the right people, machines, and software components access the right digital resources at the right time and for the right reasons.

## Foundations of Identity & Access Management (IAM)

IAAA (Identification, Authentication, Authorization, Accountability) is the foundation of Identity and Access Management (IAM). IAM is a discipline and a type of framework for solving the challenge of secure access to digital resources.

The core of IAM is digital identity. Typically, it is a user account such as customer, employee, member, or participant. User accounts can also represent non-humans, such as software, Internet of Things devices, or robotics. Identification is the process of identifying a user or entity which provides uniqueness in a system. This is generally asking a question of “Who are you?”.

Authentication is the validation of a digital identity. As an analogy, when someone enters the building, the guard compares the photo on the ID to your face to get proof that you are who you claim to be. If it matches, the guard lets you through the door to try to access the building. This is typically using passwords, multi-factor authentication (MFA), or smart cards. This is generally asking a question of “Can you prove it?”.

Authorization is the process to determine what resources a user can access based on the rights that are configured. This typically provides control over granting and denying access to different resources. As an analogy from the previous scenario, you can access your private office but not those belonging to your colleagues. It is generally asking a question of “What are you allowed to do?”.

Accountability, often referred to as auditing, is the process of recording the action carried out by digital identity which involves keeping track of who did what, and when. This would help with reporting, compliance, and security monitoring. This final phase generally asking a question of “What did you do?”.

## 2.0 Authentication Mechanism & Management

Authentication provides a way of identifying a user. It can be done through various mechanisms: something you know, something you have, something you are, and multi-factor authentication.

Something you know happens with your knowledge. This can be a PIN, password, key, pet’s name, etc. This is the most common authentication implemented today and one of the cheapest authentication mechanisms. Something you have happens with ownership. An access ID card, credit card, RSA token, and security badge are all examples of things you can own and authenticate yourself with. In case this badge is stolen or lost, this could be an issue in those cases. Something you are happens with your characteristics. Physical attributes are used to authenticate you such as fingerprints, voice prints, eye scans, palm prints, etc. are examples of characteristics or biometrics. An issue with this can be you can never change your characteristics if someone gets hold of your biometrics, unlike a password which can be changed. Multi-factor authentication is using more than one factor to authenticate user. An example would be a PIN + Access ID care, which is a combination of something you know and something you have.

Authentication management is done through the process called identity lifecycle. It is a strategic process of managing every digital identity from the moment it’s created to the moment it’s deactivated - securely, efficiently, and without manual chaos. It involves stages such as provisioning (creation and initial access), re- provisioning (ongoing changes and updates), and de-provisioning (removal of access).

Provisioning is the process of creating a digital identity when someone joins the organization - whether they’re a full-time employee, a consultant, or even a system. As someone’s role evolves, their digital identity changes. This is the re- provisioning stage. This ongoing stage involves managing changes to user roles, updating credentials, and continuously monitoring user access activity. Lastly, when a user's tenure ends (whether it’s an employee, contractor, or vendor) or their access is no longer needed, the de-provisioning stage removes their identity and revokes all access rights from the system. This prevents potential security risks from former employees or inactive accounts.

## 3.0 Authorization & Accountability

Once the system has successfully validated a user through authentication, it moves to the stage where a system determines the specific actions and resources a user is allowed to access. This is the authorization stage where it ensures that users or systems can only access resources and perform actions they are permitted to. Proper authorization prevents unauthorized actions and access within the system.

To enforce the principle of least privilege and limit access to only necessary resources, authorization criteria is implemented based on factors like user roles, permissions, rights, and privileges. Role-based criteria often assign users to roles (e.g., user, administrator, auditor), and each role is granted a specific set of permissions. Permissions, rights, and privileges define the actual actions a user can take, such as read (r), write (w), or execute (x).

On the other hand, accountability is the final piece where it keeps track of system log actions performed by authenticated and authorized users. It involves monitoring user activities to create an auditable trail, ensuring that actions can be traced back to a specific authenticated user for incident response and maintaining system integrity.

## 4.0 Managing IAAA in Windows

.

## 5.0 Managing IAAA in Linux

# Enterprise IAM

## 6.0 Enterprise Identity Repository

## 7.0 Privileged Access Management

## 8.0 Enterprise Password Policy Management

## 9.0 Integrated Access Management & IDM

## 10.0 Applying Access Management & IDM

## 1.0 Network Authentication & Access Protocol

# IAM Governance

## 12.0 Data Ownership & Access Validation

## 13.0 Identity & Access Validation

## 14.0 Segregation of Duties & Job Rotation

References

Nexus Group. (n.d.). Identity Management (IdM) Introduction. <https://www.nexusgroup.com/resources/identity-management-introduction/>

EnigmaTracer. (n.d.). Cybersecurity Basics: Understanding IAAA Access Control. <https://enigmatracer.com/cybersecurity-basics-understanding-iaaa-access-control-3212769b40f0>

Auth0. (n.d.). Introduction to Identity and Access Management (IAM).

<https://auth0.com/docs/get-started/identity-fundamentals/identity-and-access-management>

Pahwa, M. (n.d.). Identification, Authentication, Authorization, and Accountability. Learning Security with Mayur. <https://mayurpahwa.com/blog/cybersecurity/identification-authentication-authorization-and-accountability>

SecurEnds. (2025, May 14). Identity Lifecycle Management: A Complete Guide. <https://www.securends.com/blog/identity-lifecycle-management/>

09/23/2025: 1 on 1 meeting with Sam

change the font of first page to fit the entire page.

table of contents - OK

intro - rework at the end so other topic will be included.

main topic (ex, IAM Fundamentals) - its ok to put 1 or 2 sentences.

subtopic (1.0 Foundations, etc)

- it should be 1 page long. Its ok to exceed 1 page.

- 3 paragraph each

1st paragraph - area of self reflection. ex, this is what i learn...

2nd paragraph - critical thinking. pros and cons, think as student

3rd paragraph - additional comments, ex. Netflix use this, etc.

- max 18 pages for all

referencing : if using chatgpt , dont use it entirely. use it only for grammar checking, spelling.

- reference the whole convo in chatgpt. share the convo and put it in reference