Access Authorization and Identity Access Management Policy

Bhavana Kukkapalli

Varun Sai Muthyapu

Viharika Deverapally

Aasritha Devi Surapaneni

Asma Ouili

Arizona State University

IFT 483/598- Developing a Security Policy

Dr. Tatiana Walsh

December 2nd, 2022

Table of Contents

Introduction

The emergence of technology and the increased reliance on it led to a world where businesses are managed through computer systems that are accessed with digital identities. Technological advancements revolutionized businesses and industries with automation and computer systems that make it possible for a manager to supervise a production site remotely. The opportunity to have access to real time data and oversee the functionality of processes, be notified instantly whenever problems occur, and take the necessary decisions to fix these issues based on the information available is a great advantage to businesses that comes with its drawbacks, organizations need to ensure that only authorized personnel have the ability to access and interact with their data. If access is not properly controlled, the risks of breaches and security incidents will increase because access is not restricted to employees who needs it to perform tasks related to their roles and responsibilities within the organization**.** Allowing users to access sensitive data where it is not necessary might incentivize curious or malicious users to access processes that are critical to the functioning of the business and modify them in a way that might inhibit the business's operability. Therefore, it is crucial for organizations to manage adequately the processes of authentication, access authorizations, and access controls.

Organizations rely on information systems to run operations by granting employees permissions within these systems that enable them to perform their work appropriately. However, giving employees the possibility to access and process data essential to ensure the continuity of the business and its underlying operations is a huge vulnerability that can lead to threats if it is not handled correctly. Hence, organizations need to clearly define and manage the permissions given to entities that interact with their systems, applications, and data. An Identity and Access Management (IAM) system allow organizations to configure the necessary requirements to handle authentication, authorizations, and user management services. To understand the importance of an access authorizations and identity access management policy often referred to as an IAM, it is necessary to understand the processes it regulates. Authentication is the process of ensuring that users are identified before they can access the organizations IT resources. Authorizations is the process of properly configuring access levels based on roles and responsibilities of the entity. User management services is the process of granting unique digital identifications to users within the information system and managing their access within that system.

The requirements and rules configured on IAM are defined within an Access Authorization and Identity Access Management Policy which clearly explains what should be done to secure authentication and ensure that adequate access authorizations and controls methods will be used. This policy outlines who has permission to do what on which data and why? (Koelewijn, G. 2009). It is important that an IAM policy clearly defines the rules within the organization for what level of access should be given to employees based on their roles and restrict their access to strictly the necessary resources indispensable for them to perform job functions as expected.

Research Statement

Access authorization and identity management policy defines the requirements for creating and managing access control and authorizations. Additionally, it explains the process of creating digital identities and the criteria for granting access privileges to users' accounts within an organization. This policy will ensure that users will be authenticated before accessing the system and that they will only be able to see and process information and applications necessary to perform their responsibilities. The policy requirements will be reflected through the implementation of security controls that are aligned with the business core mission and objectives. These controls will guarantee the confidentiality, integrity, and availability of the systems and applications necessary to run the organization.

The Purpose of the Policy

Organizations need to clearly define and manage the permissions given to entities that interact with systems, applications, and data. An IAM policy will allow organizations to achieve this goal by setting up the who, what, which, and why. The “who” being the process of authenticating users, the “what” and “which” reflect access control and authorizations given to authenticated entities (Koelewijn, G. 2009). The “why” is the criteria used to define and grant permissions for different employees, permissions are not static and continuously change as employees change roles within the company (Koelewijn, G. 2009). This policy provides answers to these questions by defining the measures required to properly implement accounts management, access control, and users’ rights. Additionally, it outlines the process of issuing credentials, authenticating identities, managing authorizations, and granting access privileges. Several business drivers lead organizations to invest in creating an IAM, the most notable one being security. The main purpose of this policy is to implement security safeguards that will mitigate the risks related to unauthorized access to data and the systems that process it which will ensure the confidentiality, integrity, and availability of these resources.

Demonstrating Mastery-Significance

Authentication is what verifies the identity and Authorization verifies the privileges. A security gap in many of today's networks leads to unauthorized access, which is the main reason to implement the Authorization and Identity Access Management Policy. A network could be compromised or breached in many different ways. Attacks can happen through the devices communicating with one another, ranging from host machines to application, file, web, DNS, and communication servers, remote access servers to edge hubs and workgroup switches, and WAN-oriented routers to LAN- or ATM-oriented core switches and routers. Additionally, businesses cannot afford to have their data especially sensitive data compromised by unauthorized users. Individuals should be aware of the threats associated with unauthorized access to protect their personal data as well. To protect against such unauthorized attacks, there is a rising demand and need for an Authorization and Identity Access Management policy. IAM policies create company-wide identity and access management requirements including the following:

- Setting the requirements for creating and managing passwords. Example: mandating users to log in with two-factor authentication to access the network.
- Setting the requirements for granting access privileges to employees based on their roles and responsibilities within the organization.
- Setting the requirements for controlling the user's access. Defines how the IAM system will manage users' identification, authentications, and authorizations.
- These policies protect from unauthorized access and help companies from revenue loss and brand name.

A system's authorization is any procedure that confers or revokes permission to access information or carry out a particular task. Authentication is typically required whenever a person wants to access a system. By comparing the user's credentials to an authorization list, access control systems decide which operations the user is entitled to perform. Controls for access consist of permissions in a file system which govern actions including creating, reading, editing, and deleting files. Permissions for running an application including actions like access to the system's processor and memory. Access privileges such as viewing or modifying database records (Ishaq Azhar Mohammed, 2017).

Ultimately, access control aims to help keep facilities, data, and people secure to reduce the risk to a business or organization. Data loss, theft, and violations of privacy and data protection rules are just some of the issues that could impede business operations without adequate access control.

The benefits of using an access-control list include Authorization checklists to streamline the delegation of powers. The authorization list defines the user's permissions, rather than the objects themselves. If a new object is added to the authorization list, the users on that list will be granted access to that object. A single action is needed to grant access to everything on the list. Authorization lists improve security by limiting the number of private authorities on the system. Each user's permission list is a separate object to which they have access (Ishaq Azhar Mohammed, 2017).

An IAM system's primary functions are to verify and validate the identities of users based on their assigned roles and external factors like location, time of day, and (trusted) network membership. Logins will be recorded and captured. Control access to, and edit, the company's identification database system resources and how they can utilize those resources, as well as keep tabs on any modifications to those controls. Take charge of the process of giving and revoking permissions to users.

Using an IAM system, you can monitor employee actions with more ease. It will be difficult for unauthorized persons to acquire access if they know that only certain personnel can see programs and applications. The system can be configured to monitor suspicious activity, erroneous messages, and other problems that could otherwise go unreported.

Companies with growth plans benefit from identity and access management systems. New workers should be given more responsibilities and privileges as they advance in the company and acquire more experience and education. Using IAM lowers your vulnerability to workplace disruptions and improves your chances of succeeding in the following areas: Impeding the spread of malicious software. The introduction of the company's online site to prospective customers. Keeping an eye on how hard people are working. Raising the bar for the entire user experience (single-sign-on or multi-factor credentials).

The significance of this policy is to maintain the confidentiality, integrity, and availability of the data.

Argument for the Position

The method by which the operating system determines whether or not a given process is authorized to perform its intended function on this system is called access authorization. The most common form of such a security is the username, which is familiar to us all since it is needed every time we log into a platform. Three different methods exist to control access to information systems within an organization, role-based access authorization, discretionary access authorization, and mandatory access authorization. Organizations can benefit from an IAM by assigning roles, restricting access, and granting privileges and rights to their employees. Using an IAM, you may fortify your platform's current defenses. Security administrators are able to enforce access controls and managing authorizations according quickly and effortlessly to the rules defined in an IAM policy. The advantages of having an Access Authorization and Identity Access Management on the systems are:

- **Prevention against Data breaches:** When digital identities are created and managed adequately by setting proper roles to each user, the risk of data breaches is mitigated because the attack vector is minimized by allowing only authenticated users to access IT resources and restricting access to the minimum access necessary for them to perform their job functions (Morefieldcommunications, 2022). This is referred to as least privilege principle which is on the best practices for configuring access authorizations.
- **Achieve the required level of security or conform to regulatory standards:** Organizations that must be in compliance with HIPAA should ensure that their implemented access control safeguards cover the requirements of HIPAA regarding access control. An IAM policy allows organizations to know whether they are adhering with

regulations through audits which provides insight into the effectiveness of the controls implemented in applying the rules stipulated in the policy and the governing regulations.

- **Effortless Communication of Data:** An effective IAM policy enables communication between different parties within an organization. Moreover, information dissemination is managed more efficiently using IAM's unified database where data can be safely and easily shared with coworkers or clients using this platform. Organizational credibility is bolstered as a result of improved trust and communication (Morefieldcommunications, 2022).
- **The ease of access for employees in an organization:** An IAM policy makes it possible to decide who has access to which services of the system and why. The requirements defined in the policy state the methods that can be used to authenticate users and the criteria for granting access privileges. These requirements can be configured and monitored for compliance with an IAM system. Implementing single-sign-on authentication for instance, will enable authorized users to authenticate themselves only once using one credential. Once granted access, users can perform the tasks necessary to fulfil their duties and access different applications and systems within the corporate network. Individual can quickly and easily gain access to any desired location by just scanning an access card or entering a passcode (Morefieldcommunications, 2022).
- **Assign and manage access privileges from one location:** Since IAMs are highly centralized, they can improve an organization's security and privacy practices by implementing the rules, setups, conventions, and permissions defined in policies. Moreover, organizations can more easily scale their security by allowing central administration of users' identities and permissions. In addition, IAMs are a unified and

accessible approach that simplify the process of removing inappropriate access privileges, discover violations, and remove accounts as needed (Morefieldcommunications, 2022).

- **Maximizes Satisfaction Among Users:** Integrating Authentication and Authorization reduces the need for labor-intensive manual procedures. Self-service methods, such as password recovery, are automated so that individuals can take care of their own identities and queries. Each user is free to select their own exclusive password. The Single Sign-On (SSO) method eliminates the need for users to create and remember separate passwords for each of the organization's services (Benefits of implementing an access control system, 2022). User experience with IAM is streamlined and straightforward after an efficient deployment.
- **Help improve the performance of Security Personnel:** Security administrators can standardize policy enforcement throughout locations, teams, and technologies by using an IAM policy. The majority of today's IAMs are hosted in the cloud (SaaS), making it simple to employ all necessary safety procedures by means of common web browsers and mobile devices (Morefieldcommunications, 2022).
- **Reduces IT workload:** By implementing an IAM policy through automated systems that attribute and manage user identities and their access authorizations within the information systems.
- **Facilitates Workflow and Increases Efficiency:** Due to their built-in mechanization and AI-driven algorithms that understand security parameters, new IAM services involve authentication and authorization more easily (Morefieldcommunications, 2022). By streamlining formerly manual processes, IAM policies can boost efficiency by streamlining the administration of identifying users, access control policies, and other related processes. Some IAMs employ neural network models to quickly identify security risks and implement risk-based authorization and governance policies.

Criticizing Arguments

Even while this policy offers many firm game-changing advantages, the solution must nevertheless be strategically integrated into a comprehensive security plan. IAM deployment is a continual process that calls for in-depth planning, change-management experience, and constant knowledge of IAM technology. IAM implementation has its own set of difficulties, and many small- and medium-sized businesses (SMBs) lack the funds required to complete the task. As a result, the implementation of IAM by SMBs frequently lags behind that of bigger businesses. Hackers are creating new threats specifically aimed at smaller firms because of this drawback. The following crucial points should be kept in mind when deploying IAM:

- **Centralized target :** As you start to consolidate the administration of identities and authentication methods, a significantly larger and more concentrated security target is produced. As a result, employing various network-based security techniques, significant care must be taken to safeguard this platform appropriately.
- **Infrequent audits**: We must remember to update audit practices, so they apply to the current access policies even though IAM makes the deployment of business policies a straightforward, streamlined process. Businesses are encouraged to keep setting aside time for routine audits in order to define what can and should be automated as well as to allow for the potential identification of vulnerabilities. In addition, audits give firms information about how to enhance security by deleting unauthorized access points.
- **Business scaling issue:** IAM platforms need scalability to meet growing demands as companies expand and technological requirements shift. The degree of scalability of a platform may occasionally be constrained by IAM products.

- **Incorrect definition of rules:** Role-based access control, RBAC management within an organization is another potential disadvantage in this policy. RBAC is a technique used by administrators to categorize a number of users according to their access rights. Although using access groups is an excellent technique to lessen the amount of access policies that would need to be generated and maintained, many firms put an excessive number of people into a single group. As a result, some users have access to services and applications they don't require. In the best situation, this leads to a circumstance wherein user access isn't as restricted as it may be. In the worst-case scenarios, this may lead to users who have an insufficient separation of roles, which may result in access control compliance violations.
- **Offboarding of the employees:** There are numerous moving components if it refers to access management. If repetitive tasks are not automated, administrators may fail to complete some tasks within a sufficient length of time. Offboarding of employees is a prime illustration of how a shortage of automation can put organizations at risk when the administrator forgets to invoke the access rights then employees leave the firm but have their access intact.
- **Improper password security:** 61% of data leaks across all industries involve compromised credentials, according to Verizon's Data Breach Investigation Report. These violations are also expensive: According to IBM Security's Cost of a Data Breach Report, a data breach typically costs $4.24 million. Users must follow best practices for creating secure passwords and mitigate the threat, hence this policy has great dependency on password creation and management policy.

- **Time consuming:** This can be time consuming as well. For example: If the policy wants you take two factor authentication. It takes more time than the single factor authentication as its verification needs identity check twice.
- **Shortage of technical professionals:** To manage all these IAM tools one must require professionals. Small companies might find it hard to invest and recruit the on-demand tech professionals as they are expensive and limited.

Considering Potential Objections

Upon reading the disadvantages of having an IAM policy within organizations, one might argue that this policy is not worth it. However, it is important to remember that the advantages outweigh the disadvantages, having an IAM policy will ensure the confidentiality, integrity, and availability of the IT resources necessary to organization. An IAM policy will allow organization to mitigate unauthorized access to internal resources through authentication and authorization mechanisms. Additionally, it will demonstrate compliance with regulations and laws that are applicable to the business. Furthermore, managing identities and authorizations can be a cumbersome task when the requirements are not formalized, investing resources to create a policy that defines the controls needed will allow organization to automate these processes.

Conclusion

The advent of technology and its expansion throughout different industries and businesses altered the way companies operate. Remote access capabilities made it possible for organizations to ensure some level of business continuity during the COVID-19 pandemic. This remote access is possible because of the underlying IT infrastructure that allows businesses to operate whenever and wherever. However, just like technological advancements improved how business run operations and processes, they created new problems and challenges as well. The reliance on information systems within organizations led to higher security and privacy risks. Data breaches attacks which threaten the most valuable asset organizations have, data, are continuously increasing and becoming difficult to prevent. Unauthorized access is the one of the main root causes of data breaches. Organizations need to understand the risks entailed with unauthorized access to IT resources and the impact of such attacks on the business. one possible solution to mitigate these risks and preserve the confidentiality, integrity, and availability of the systems and the data processed on these systems would be to create access authorization and identity access managements policies.

Access authorization and identity access management policies play a key role in creating the rules for who can access which IT service and why. The policy achieves this goal by defining the requirements and security controls necessary to create and manage identities within an organization, the methods for authenticating users before they access the corporate network, and the criteria for establishing and maintaining access privileges for authorized users once they access the network. Organizations apply the least privilege principle when assigning access control and setting up authorizations, this principle minimizes the threat vector of security incidents by restricting access to the minimum necessary for employees to perform their tasks. The main goal behind this policy is to implement the security safeguards that will implement the policy and mitigate unauthorized access to resources and prevent the possibility of compromising data or the systems in any way. It ensures that any security gaps within the IT infrastructure were properly addresses using adequate security controls. Additionally, it helps organizations stay in compliance with the governing regulations. Furthermore, this policy enables communication among different parties within the organization and reduces IT costs by relying on a centralized and automated system to ensure proper authentication and authorization processes.

While this policy addresses the concern of unauthorized access and the threat of data breaches, some question its importance by focusing on some of its side effects such as the fact that it provides a centralized system to store access authorizations databases which makes this database a common target for threats that intend to gain access to that information or the limited scalability that some models have. However, it is important to remember the benefits of this policy outweighs its disadvantages and the role it plays in preserving the confidentiality, integrity, and availability of the data and the systems.

Appendix

Access authorizations and Identity Access Management Policy

Overview

This policy describes the process of creating digital identities for employees and users within the organization, the requirements for providing access privileges to different accounts, and the managements of existing accounts within the corporate IT infrastructure.

Purpose

Implementation of proper security controls to manage accounts, access privileges, authentication acceptable methods, and password requirements will mitigate risks related to unauthorized access to resources and will guarantee the confidentiality, integrity, and availability of the systems, applications, and data processed on them.

Scope

This policy applies to all departments, users, system, applications, and different entities that access the corporate network including those with special access privileges such as IT administrators.

Policy

Responsibilities employees, vendors, and contractors

- Authorized users must follow the requirements set in this policy for authentication.
- Users must create strong passwords
- Users must not share their login credentials with anyone.

- Users must use their access privileges according to their roles and the reason behind the attribution of the privilege.

Responsibilities of Systems Administrators

a. <u>Accounts</u>

- Creating unique account for every employee.
- Shared accounts are created to support multiple users sharing the same identity.
- Service accounts are used when it is necessary for systems or applications
- Privilege accounts may have extra privileges related to the management of a device or application.

b. <u>Access Control</u>

Administrators should only provide the permissions necessary for the function to be performed. Following the least principle helps to guarantee that suitable procedures are followed and that access to functions that may expose data is kept to a minimum.

c. <u>Authentication</u>

- Authentication is the process by which a system or application confirms that a person or device really is who or what it is claiming to be and through which access to the requested resource is authorized.
- Strong authentication protocols help both to protect personal and company information and prevent misuse of resources.
- Enterprise Authentication Services for centrally created accounts.
- Federated Authentication mechanism may authenticate identities using our enterprise authentication services by federating with them.

d. Authorization

- Authorizations are the implicit or explicit permission to use a resource associated with an account.
- Once the use of an account is authenticated, a system or resource may determine if the person or software requesting access is authorized to use it.

e. Deprovisioning

- Users that are not affiliated with the organization must not have accounts.
- The prompt removal of employees' accounts as they leave the organization.

f. Auditing

- Internal Audit and Advisory Services may make routine or ad-hoc requests to audit the accounts and authorizations of any company information system along with the associated audit trail.
- These audits will ensure that accounts and authorizations are consistent with this document including right account privileges, requests approved both by an administrative and technical manager, requests compliant with applicable regulation and policy.

Policy Compliance

Policy Measurement

Compliance with this policy will be enforced through different methods, including but not limited to, walk-throughs, internal and external audits, business reports, and inspections, and will report any findings to the business unit manager and the policy owner.

Exceptions

Exceptions to this policy must be approved and documented by the IT department and the policy owner.

Non-Compliance

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

Business partners or vendors found in violation of this policy may result in termination of their agreement and financial liability for any damage resulting from the violation.

Revision Log

Date of change	Responsible	Summary of change
11-27-2022	Policy Team	Creation of the policy.
12-02-2022	Policy Team	Update Responsibilities

References

Admin. (2022, November 16). *9 key benefits of identity and Access Management (IAM)*. vSecureLabs. Retrieved December 2, 2022, from https://vsecurelabs.co/benefits-of-identity-and-access-management/

Gaedke, M., Meinecke, J., & Nussbaumer, M. (2005). A modeling approach to federated identity and Access Management. *Special Interest Tracks and Posters of the 14th International Conference on World Wide Web - WWW '05*. https://doi.org/10.1145/1062745.1062916

Hayes, J. (2002, August 6). *Policy-based Authentication and Authorization: Secure Access to the network infrastructure*. IEEE Xplore. Retrieved October 2, 2022, from https://ieeexplore.ieee.org/abstract/document/898887?casa_token=9n4355cW7NAAAAAA%3AllV9S3Ox0YD9IHKGElpHYVj8dzm67jnIDjgYHpoMsbKJRHE0NQH29RcKDeng8_fRNbXgRG6g9A

Hummer, M., Kunz, M., Netter, M., et al. (2016). Adaptive identity and access management—contextual data based policies. *EURASIP Journal on Information Security,19*. https://doi.org/DOI 10.1186/s13635-016-0043-2

Ishaq Azhar Mohammed. (2011). Identity and Access Management System: a Web Based Approach for an Enterprise. SSRN Electronic Journal, 1(4), 2278-7844. https://www.researchgate.net/publication/353887611_Identity_and_Access_Management_System_a_Web-_Based_Approach_for_an_Enterprise

Identity and Access Management Policy. Identity and Access Management Policy | Policies. (n.d.). Retrieved December 2, 2022, from https://www.bu.edu/policies/identity-and-access-management/

Koelewijn, G. (2009). *Identity & Access Management: Get in control: IT governance, people, permission and technical challenges.* TU Delft Repositories. Retrieved December 1, 2022, from https://repository.tudelft.nl/islandora/object/uuid:47e228e5-645e-497c-a5e2-ec3b4df5e299?collection=education

Mohammed, I. A. (2011). *Identity and Access Management System: A web- based approach for an Enterprise*. Identity and Access Management System: a web based Approach for an Enterprise. Retrieved October 3, 2022, from https://www.researchgate.net/profile/Ishaq-Azhar-Mohammed/publication/353887611_Identity_and_Access_Management_System_a_Web-_Based_Approach_for_an_Enterprise/links/6116a022169a1a0103fc6432/Identity-and-Access-Management-System-a-Web-Based-Approach-for-an-Enterprise.pdf

Morefield communications. (2022, November 22). *Benefits of implementing an access control system*. Morefield. Retrieved December 2, 2022, from https://www.morefield.com/blog/benefits-of-an-access-control-system/

R. S. Sandhu and P. Samarati, "Access control: principle and practice," in *IEEE Communications Magazine*, vol. 32, no. 9, pp. 40-48, Sept. 1994, doi: 10.1109/35.312842.

Tang, C. (2020, December 24). *Policy-based network access and Behavior Control Management*. IEEE Xplore. Retrieved October 2, 2022, from https://ieeexplore.ieee.org/document/9295916

Thakur, M. A., & Gaikwad, R. (2015). User Identity and Access Management Trends in IT Infrastructure - An Overview. In *International Conference on Pervasive Computing (ICPC)*.

Systematic review of Identity Access Management in Information Security. (n.d.). Retrieved December 3, 2022, from https://www.researchgate.net/profile/Ishaq-Azhar-Mohammed/publication/353887659_SYSTEMATIC_REVIEW_OF_IDENTITY_ACCESS_MANAGEMENT_IN_INFORMATION_SECURITY/links/61169c5d1ca20f6f861e4496/SYSTEMATIC-REVIEW-OF-IDENTITY-ACCESS-MANAGEMENT-IN-INFORMATION-SECURITY.pdf?origin=publication_detail

Uddin, M., & Preston, D. (2015). A systematic review of Identity Access Management in Information Security. *Journal of Advances in Computer Networks, 3*(2), 150–156. https://doi.org/10.7763/jacn.2015.v3.158