Access Control Policy

Code	ICT-POL-005
Controls	5.15 Access Control 5.16 Identity Management 5.17 Authentication Information 5.18 Access rights 8.2 Privileged access rights 8.3 Information access restriction 8.5 Secure Authentication
Version	4.1
Date of Version	1/18/2023
Created by	Saied Avash
Approved by	Corina Guardado
Confidentiality level	Protected
Authorized users	Employees, contractors, and suppliers.

Version Control

Date	Version	Change/reviewed by	Description of the change/review by
8/22/2018	1.0	Saied Avash	Policy Creation
7/08/2019	1.1	Corina Guardado	General use and ownership,align with the ISMS scope
10/25/2019	1.2	Corina Guardado	Specify details of usage of passwords
4/20/2020	1.3	Corina Guardado	Update policy and controls
5/18/2021	2.0	Corina Guardado	Define Roles and Responsibilities of employees.
1/26/2022	2.1	Luis Morales	Add PCI room and legend for orange color access.
3/21/2022	3.0	Jorge Huezo	Updated policy to new format
9/1/2022	3.1	Saied Avash	Review and Approval
1/18/2023	4.0	Jorge Huezo	Updated to new format
2/23/2023	4.1	Jorge Huezo	Added considerations from the new norm format.
4/12/2023	4.2	Jorge Huezo	Updated consideration for new controls on the SOA
5/22/2023	4.3	Jorge Huezo	Added considerations for privileged access controls, updated introduction, purpose and scope

Contents

Version Control 2
Introduction 5
Purpose 5
Scope 5
Access Control Requirements Determination 6
Information Security and Business Requirements 6
Communication with Relevant Parties 6
Access Control Principles 7
Principle of Least Privilege 7
Segregation of Duties 7
Need-to-Know 7
Defense-in-Depth 7
Roles and Responsibilities 8
Executive Management 8
Information Security Department 8
System Owners 8
Data Owners 9
IT Administrators 9
Employees and Users 9
Access Control Considerations 10
Entities Requiring Access 10
Security of Applications 10
Privileged Access Restrictions 10
Compliance with Legislation, Regulations, and Contracts 10
Logging Considerations 10
Access Control Measures 11
Physical Access Control 11
Logical Access Control 11
User Authentication 11
User Authorization 11
Access Control Lists 11
User Account Management 12
Account Creation and Provisioning 12

Account Modification and Termination 12
User Account Review 13
Identities Management 13
Authentication information 14
Allocation of authentication information 14
Password management system 14
Access Control Enforcement 15
Access Rights 15
Provision and revocation of access rights 15
Privileged Access Rights 15
Network Access Control 17
Application Access Control 18
Data Access Control 18
Mobile Device Access Control 18
Remote Access Control 19
Cloud Services Access Control 19
Monitoring and Auditing 20
Access Logs and Event Monitoring 20
Intrusion Detection and Prevention Systems 20
Incident Response and Reporting 19
Access Control Rules Implementation 21
Defining Access Rights and Restrictions 21
Role Assignment to Entity Groups 21
Consistency with Information Classification 21
Consistency with Physical Perimeter Security 22
Consideration of Available Connections in Distributed Environments 22
Dynamic Access Control Elements 21
Dynamic Elements and Granularity 22
Dynamic Access Control Elements 22
Granularity of Access Control 23

Introduction

The Access Control Policy serves as a vital framework for protecting information and associated assets within an organization. This policy establishes rules and procedures to regulate both physical and logical access, ensuring that authorized individuals can access resources while preventing unauthorized access and safeguarding the confidentiality, integrity, and availability of information. This document provides an overview of the Access Control Policy, outlining its purpose, scope, and the key considerations for implementing effective access control measures.

Purpose

The Access Control Policy ensures that only authorized individuals are granted access to information and associated assets, while preventing unauthorized access. By defining access control rules based on business and information security requirements, this policy aims to minimize the risk of unauthorized disclosure, modification, or destruction of sensitive and critical data. It provides guidance on determining access rights, implementing appropriate controls, and establishing accountability for access-related activities.

Scope

The Access Control Policy applies to all individuals and entities accessing or managing information and associated assets within the organization. This policy covers both physical and logical access control measures and extends to all computing devices, including personal devices used for work purposes. It encompasses considerations such as determining access requirements, securing applications, managing physical access, authorization and dissemination of information, restrictions on privileged access, segregation of duties, compliance with applicable laws and regulations, and the management of access control functions.

Access Control Requirements Determination

Information Security and Business Requirements

Determining the access control requirements is a critical step in developing an effective Access Control Policy. The owners of information and associated assets should collaborate with the information security department and other relevant stakeholders to identify the specific requirements based on information security and business needs.

The information security requirements encompass protecting the confidentiality, integrity, and availability of sensitive and critical information. These requirements may include restrictions on who can access certain types of information, ensuring data confidentiality through encryption or access restrictions, and maintaining data integrity by implementing access controls to prevent unauthorized modifications.

Business requirements related to access control involve understanding the operational needs, roles, and responsibilities within the organization. This includes identifying the various entities (both human users and technical/logical items) that require access to information and associated assets to perform their tasks efficiently. By considering these business requirements, the Access Control Policy can be tailored to provide appropriate access privileges and restrictions, ensuring that individuals have the necessary access to perform their job functions.

Communication with Relevant Parties

Effective communication is essential in establishing and implementing access control requirements. Once the information security and business requirements are determined, it is crucial to communicate these requirements to all relevant parties. This includes stakeholders such as executives, managers, system owners, data owners, IT administrators, and employees who interact with the organization's systems, networks, applications, and data.

Clear and concise communication helps to ensure that everyone understands the access control requirements and their roles in enforcing them. This may involve conducting training sessions, disseminating written guidelines, or organizing workshops to address any questions or concerns. By involving and informing all relevant parties, the organization can foster a shared understanding and commitment to access control practices, thereby enhancing the overall security posture.

Regular communication and ongoing collaboration with relevant parties are also vital for adapting the Access Control Policy to evolving business needs and changing security threats. This facilitates a proactive approach to access control management, ensuring that the policy remains up to date and aligned with the organization's goals and objectives.

Access Control Principles

Access control principles provide fundamental guidelines for establishing effective access control measures within an organization. These principles help ensure that access is granted only to authorized individuals and that appropriate security measures are in place to protect information and associated assets.

Principle of Least Privilege

The Principle of Least Privilege states that individuals should be granted the minimum level of access necessary to perform their job functions. This principal limits access rights to only what is required, reducing the risk of unauthorized access and potential misuse of privileges. By implementing the Principle of Least Privilege, organizations can minimize the impact of a security breach or insider threat and mitigate the potential for unauthorized disclosure, modification, or destruction of sensitive information.

Segregation of Duties

The Segregation of Duties principle involves dividing critical tasks or operations among multiple individuals to prevent a single individual from having complete control over a process. This principle helps ensure that no one person can bypass controls, commit fraud, or carry out malicious activities without detection. By separating duties, organizations can establish checks and balances, increase accountability, and reduce the risk of conflicts of interest.

Need-to-Know

The Need-to-Know principle states that access to information should be granted only to individuals who require it to fulfill their job responsibilities. This principle is based on the understanding that different roles or tasks require different levels of access to specific information. By adhering to the Need-to-Know principle, organizations can limit exposure to sensitive information, protect confidentiality, and minimize the risk of unauthorized data disclosure.

Defense-in-Depth

The Defense-in-Depth principle emphasizes the implementation of multiple layers of security controls to protect information and associated assets. This principle acknowledges that a single security measure is not sufficient to defend against all threats. By deploying a layered approach to access control, organizations can enhance their security posture and reduce the likelihood of successful attacks. Defense-in-Depth may include measures such as network segmentation, firewalls, intrusion detection systems, strong authentication mechanisms, and encryption.

Roles and Responsibilities

Effective access control requires clear delineation of roles and responsibilities among various stakeholders within an organization. The following roles and responsibilities contribute to the implementation and enforcement of access control measures:

Executive Management

Executive management plays a crucial role in establishing a culture of security and allocating resources to support access control initiatives. Their responsibilities include:

- Setting the tone for security by endorsing and promoting access control policies and practices.
- Allocating appropriate budget and resources to implement and maintain effective access control measures.
- Ensuring that access control is integrated into the organization's overall risk management strategy.
- Providing support and direction to the Information Security Department and other stakeholders in aligning access control with business objectives.

Information Security Department

The Information Security Department is responsible for the development, implementation, and maintenance of the Access Control Policy. Their responsibilities include:

- Defining access control requirements based on information security and business needs.
- Developing access control guidelines, procedures, and standards.
- Conducting risk assessments and audits to identify vulnerabilities and gaps in access control.
- Monitoring and analyzing access control logs and reports to detect and respond to unauthorized access attempts.
- Providing guidance, training, and support to system owners, IT administrators, and employees regarding access control best practices.
- Collaborating with system owners, data owners, and IT administrators to ensure consistent enforcement of access control measures.

System Owners

System owners are responsible for the proper management and security of specific systems and applications. Their responsibilities include:

- Defining access control requirements for their systems and applications.
- Implementing access controls in accordance with the Access Control Policy.
- Regularly reviewing and updating access rights and permissions based on business and user requirements.

- Monitoring access logs and reports to identify any suspicious activities or access anomalies.
- Reporting any access control issues or incidents to the Information Security Department.

Data Owners

Data owners are responsible for the management and protection of specific sets of data. Their responsibilities include:

- Defining access control requirements for their data sets based on confidentiality, integrity, and availability requirements.
- Collaborating with system owners and IT administrators to implement appropriate access controls for the data.
- Regularly reviewing and updating access rights to ensure alignment with data ownership and business needs.
- Ensuring that data classification and labeling are consistent with access control requirements.

IT Administrators

IT administrators are responsible for managing and maintaining the organization's IT infrastructure and systems. Their responsibilities include:

- Implementing access control measures on systems, networks, and applications as defined by system owners and data owners.
- Managing user accounts, roles, and permissions.
- Monitoring and responding to access control-related incidents or requests.
- Maintaining access control logs, reports, and auditing mechanisms.
- Ensuring compliance with access control policies and standards.

Employees and Users

Employees and users have an important role in adhering to access control policies and practices. Their responsibilities include:

- Using their assigned access rights and permissions solely for authorized purposes.
- Safeguarding their login credentials and not sharing them with unauthorized individuals.
- Reporting any suspected or observed unauthorized access or suspicious activities to the appropriate authorities.
- Participating in access control training and awareness programs.
- Complying with access control procedures and guidelines provided by the organization.

Access Control Considerations

To ensure effective access control, Emaya needs to consider various factors and aspects related to access management. The following should be considered when developing and implementing access control measures:

Entities Requiring Access

Identifying the entities that require access to information and associated assets is a critical step in access control. This includes both human users and technical or logical items such as machines, devices, or services. Understanding the specific access needs of these entities allows for the appropriate allocation of access privileges and restrictions. Any entity that will have access granted to an information asset must undergo the same authorization procedure.

Security of Applications

Applications play a significant role in access control. It is essential to ensure that applications are implemented and configured securely. This involves implementing appropriate authentication mechanisms, access controls within the application, and secure coding practices. Regular testing and vulnerability assessments should also be conducted to identify and address any application security weaknesses. Security of applications is handled through Project Management and Change Management procedures where their security requirements are determined, implemented, tested and updated.

Privileged Access Restrictions

Privileged access, which grants higher-level privileges and permissions, should be restricted to only those individuals who require it to perform their authorized duties. This includes administrators, system owners, and other individuals with elevated access rights. Privileged access should be carefully monitored, audited, and reviewed to minimize the risk of misuse or unauthorized actions.

Compliance with Legislation, Regulations, and Contracts

Access control measures should align with applicable legislation, regulations, and contractual obligations. This includes considering any specific requirements regarding the limitation of access to data or services imposed by relevant laws or industry standards. Compliance with these requirements helps ensure that access control practices meet legal and regulatory obligations.

Logging Considerations

Logging is an essential aspect of access control. Organizations should establish logging mechanisms to capture access-related events, including successful and

failed access attempts, privilege escalations, and administrative activities. Logging enables organizations to monitor and detect any suspicious or unauthorized access, investigate security incidents, and support compliance requirements.

Access Control Measures

To effectively implement access control, Emaya employs a combination of physical and logical measures. The following access control measures have been implemented:

Physical Access Control

Physical access control measures involve securing physical premises and restricting entry to authorized personnel. These measures are found in the **ICT-POL-006 Physical Access Management Policy**

Logical Access Control

Logical access control measures are applied to digital systems, networks, and applications to ensure authorized access. This includes the following components:

User Authentication

User authentication verifies the identity of individuals seeking access to systems or applications. It typically involves the use of unique identifiers (e.g., usernames) and confidential credentials (e.g., passwords, PINs) or other authentication factors (e.g., biometrics, smart cards).

User Authorization

User authorization determines the access privileges granted to authenticated users. It involves assigning appropriate access rights, roles, or permissions to individuals based on their job functions and responsibilities. Authorization mechanisms should be designed to enforce the principle of least privilege, ensuring that users only have access to the resources necessary to perform their tasks.

Access Control Lists

Access control lists (ACLs) are used to define and enforce specific access permissions for individual users, groups, or system resources. ACLs provide granular control over access rights, allowing organizations to restrict or grant access to specific files, directories, or network resources based on predefined rules. Below are the two ACLs that control the main records and systems managed by Emaya. When needed additional matrices can be created for specific records or systems.

ICT-CTRL-034 Records Control Matrix

User Account Management

Effective user account management practices contribute to access control by ensuring that user accounts are created, modified, and terminated in a secure and controlled manner. Key aspects of user account management include:

Account Creation and Provisioning

When creating user accounts, organizations should follow standardized procedures, such as user registration, identity verification, and assignment of appropriate access rights. Account provisioning should be based on documented approval processes to ensure that access is granted to authorized individuals only.

Accounts shall be created based on a legitimate business need and approved by authorized personnel. The following procedures shall be followed:

1. Accounts shall be created through a secure mechanism and password complexity requirements shall be enforced.
2. Accounts shall be created with the least privilege necessary to perform the job duties.
3. Accounts shall be created following the principle of separation of duties.
4. All accounts shall be reviewed periodically to ensure that access privileges are appropriate and necessary.
5. Accounts for privileged users shall be created following a higher level of scrutiny.

Account Modification and Termination

Account modification and termination processes should be established to manage changes in user roles, responsibilities, or employment status. This includes updating access privileges, removing unnecessary access rights, and promptly disabling or deleting accounts when individuals no longer require access.

Access Update

Access shall be updated based on a legitimate business need and approved by authorized personnel. The following procedures shall be followed:

1. Access shall be updated through a secure mechanism and password complexity requirements shall be enforced.
2. Access shall be updated with the least privilege necessary to perform the job duties.
3. Access shall be updated following the principle of separation of duties.
4. All access shall be reviewed periodically to ensure that access privileges are appropriate and necessary.
5. Access for privileged accounts shall be updated following a higher level of scrutiny.

Internal Reallocations

When an employee changes roles within the organization, their access to systems, applications, and data shall be reviewed to ensure that their access privileges are appropriate for their new role. The following procedures shall be followed:

1. A review of the employee's access privileges shall be conducted when a change of role is requested or identified.
2. Access privileges shall be updated based on the new role and the principle of least privilege.

Access Removal

When an employee leaves the organization or no longer requires access, their access to systems, applications, and data shall be promptly removed. The following procedures shall be followed:

1. Accounts and access privileges shall be disabled or deleted promptly when access is no longer required access.

User Account Review

Regular reviews of user accounts are essential to ensure that access rights and permissions remain appropriate and up to date. Periodic account reviews should be conducted to identify and remove any dormant or inactive accounts, detect potential misuse or abuse, and validate that authorized access is still required.

Identities Management

Identity management is critical to ensuring that only authorized individuals and entities have access to our systems, applications, and data. The following guidance outlines the processes that should be used in the context of identity management:

- For identities assigned to persons, a specific identity should be linked to a single person to enable accountability for actions performed with that identity.
- Identities assigned to multiple people, such as shared identities, should only be permitted when necessary for business or operational reasons and subject to dedicated approval and documentation.
- Identities assigned to non-human entities should be subject to appropriately segregated approval and independent ongoing oversight.
- Identities should be disabled or removed promptly when no longer required, such as when their associated entities are deleted or no longer used, or when the person linked to an identity has left the organization or changed roles.
- In a specific domain, a single identity should be mapped to a single entity to avoid mapping multiple identities to the same entity within the same context.
- Records of all significant events concerning the use and management of user identities and authentication information should be kept, enabling effective auditing and monitoring.

Authentication information

Allocation of authentication information

- Access control policy dictates that the allocation and management process of authentication information must ensure the following:
- Personal passwords or personal identification numbers (PINs) generated automatically during enrolment processes as temporary secret authentication information are non-guessable and unique for each person. Users are required to change them after the first use.
- Procedures are established to verify the identity of a user before providing new, replacement or temporary authentication information.
- Authentication information, including temporary authentication information, is transmitted to users securely (e.g., over an authenticated and protected channel).
- The use of unprotected (clear text) electronic mail messages for this purpose is prohibited.
- Users must acknowledge receipt of authentication information.
- Default authentication information as predefined or provided by vendors is changed immediately following installation of systems or software.
- Records of significant events concerning allocation and management of authentication information are kept, and their confidentiality is ensured. The record-keeping method must be approved (e.g., by using an approved password vault tool).

Password management system

To ensure secure use of passwords as authentication information, the password management system must:

- Allow users to select and change their own passwords and include a confirmation procedure to address input errors.
- Enforce strong passwords according to good practice recommendations, as outlined in "User responsibilities."
- Force users to change their passwords at first login.
- Enforce password changes as necessary, for example, after a security incident, or upon termination or change of employment when a user has known passwords for identities that remain active (e.g., shared identities).
- Prevent re-use of previous passwords.
- Prevent the use of commonly used passwords and compromised usernames and password combinations from hacked systems.
- Not display passwords on the screen when being entered.
- Store and transmit passwords in protected form.

Password encryption and hashing must be performed using approved cryptographic techniques for passwords.

Access Control Enforcement

Access Rights

Provision and revocation of access rights

Access rights provisioning and revocation process should include the following:

- Obtaining authorization from the information and other associated assets' owner for the use of information and other associated assets, and separate approval for access rights by management where appropriate;
- Considering the business requirements and the organization's topic-specific policy and rules on access control;
- Considering segregation of duties, including segregating the roles of approval and implementation of the access rights and separation of conflicting roles;
- Ensuring access rights are removed when someone does not need to access the information and other associated assets, in particular ensuring access rights of users who have left the organization are removed in a timely fashion;
- Considering giving temporary access rights for a limited period and revoking them at the expiration date, for temporary personnel or temporary access required by personnel;
- Verifying that the level of access granted is in accordance with the topic-specific policies on access control and is consistent with other information security requirements such as segregation of duties;
- Ensuring that access rights are activated only after authorization procedures are successfully completed;
- Maintaining a central record of access rights granted to a user identifier (ID, logical, or physical) to access information and other associated assets;
- Modifying access rights of users who have changed roles or jobs;
- Removing or adjusting physical and logical access rights, which can be done by removal, revocation, or replacement of keys, authentication information, identification cards, or subscriptions;
- Maintaining a record of changes to users' logical and physical access rights.

Privileged Access Rights

The allocation and use of privileged access rights must be carefully managed and restricted within the organization. This section outlines the guidelines and considerations for controlling privileged access rights:

Authorization Process

The allocation of privileged access rights should be governed by an established authorization process, which aligns with the organization's topic-specific policy on access control. The following factors should be considered:

a) Identification of users: Identify the specific users who require privileged access rights for each system or process, such as operating systems, database management systems, and applications.

b) Event-based allocation: Privileged access rights should be allocated to users on an as-needed and event-by-event basis, in accordance with the topic-specific policy on access control. Access should only be granted to individuals who possess the necessary competence to carry out activities that require privileged access, based on the minimum requirements of their functional roles.

c) Authorization and record-keeping: Maintain an authorization process to control the allocation of privileged access rights. This includes determining the appropriate personnel who can approve such access and maintaining a record of all privileges allocated.

d) Expiry requirements: Define and implement requirements for the expiration of privileged access rights. Regularly review and revoke access that is no longer necessary or justified based on changes in organizational roles or responsibilities.

User Awareness and Authentication

To ensure awareness and proper authentication, the following measures should be implemented:

a) User awareness: Users should be made aware of their privileged access rights and understand when they are in privileged access mode. Specific user identities, user interface settings, or dedicated equipment can be employed to indicate privileged access.

b) Authentication requirements: Authentication for privileged access rights may require higher levels of assurance compared to normal access rights. Re-authentication or authentication step-up may be necessary before performing tasks with privileged access rights.

Review and Monitoring

Continuous monitoring and periodic review of privileged access rights are essential for maintaining security and accountability. Consider the following:

a) Regular review: Regularly review the individuals working with privileged access rights to validate if their duties, roles, responsibilities, and competence still qualify them for such access. This review should be conducted periodically and after any organizational changes.

b) Avoiding generic administration user IDs: Establish specific rules to avoid the use of generic administration user IDs (e.g., "root") based on the capabilities of the

systems. Adequate management and protection of authentication information for such identities should be ensured.

c) Temporary privileged access: Grant temporary privileged access only for the necessary time window required to implement approved changes or critical activities, rather than permanently granting privileged access rights. This approach, often referred to as the "break glass procedure," can be automated through privilege access management technologies.

Logging and Identity Management

To enhance accountability and traceability, the following practices should be implemented:

a) Logging privileged access: All privileged access to systems should be logged for audit purposes. Comprehensive logs should be maintained to track privileged activities and detect any unauthorized or suspicious actions.

b) Individual identities: Avoid sharing or linking identities with privileged access rights among multiple persons. Instead, assign each person a separate identity that allows for the assignment of specific privileged access rights. Grouping identities (e.g., using an administrator group) can facilitate the management of privileged access rights.

c) Separate administrative tasks: Limit the use of identities with privileged access rights solely for administrative tasks, separate from day-to-day general tasks such as checking email or accessing the web. Users should have a separate normal network identity for these routine activities.

By implementing appropriate controls and measures, the organization can effectively manage and monitor privileged access rights, reducing the risk of unauthorized activities and enhancing overall security.

Network Access Control

Network access control involves implementing measures to regulate and control access to the organization's network infrastructure. This includes:

- Firewalls and network segmentation: Deploying firewalls to monitor and filter network traffic and segmenting the network to create separate zones with different access restrictions based on security requirements.
- Intrusion detection and prevention systems: Implementing systems to detect and prevent unauthorized access attempts, network attacks, and suspicious activities.

- Virtual private networks (VPNs): Utilizing VPN technologies to establish secure remote connections and control access to the organization's network resources.
- Network access control (NAC) solutions: Implementing NAC solutions to enforce security policies and authenticate devices before granting access to the network.

Application Access Control

Application access control focuses on regulating access to software applications and systems. This includes:

- Role-based access control (RBAC): Implementing RBAC models to assign access permissions and privileges based on predefined roles and job responsibilities.
- Single sign-on (SSO): Implementing SSO solutions to enable users to authenticate once and access multiple applications without re-authentication.
- Multi-factor authentication (MFA): Utilizing MFA methods, such as biometrics, smart cards, or one-time passwords, to provide an additional layer of authentication for accessing applications.
- Session management: Implementing session controls to monitor and manage user sessions, including automatic session timeouts, session termination upon user inactivity, and session monitoring for suspicious activities.

Data Access Control

Data access control involves implementing controls to safeguard sensitive information and regulate access to data resources. This includes:

- Data classification and labeling: Applying appropriate classification labels to data based on its sensitivity and confidentiality levels and implementing access controls accordingly.
- Data encryption: Employing encryption mechanisms to protect data both at rest and in transit, ensuring that only authorized parties can access and decrypt the information.
- Data loss prevention (DLP): Implementing DLP solutions to detect and prevent unauthorized access, disclosure, or exfiltration of sensitive data.
- Database access controls: Applying access controls at the database level, including user access privileges, role-based permissions, and auditing mechanisms to monitor database activity.

Mobile Device Access Control

Mobile device access control focuses on securing access to organizational resources from mobile devices. This includes:

- Mobile device management (MDM): Implementing MDM solutions to enforce security policies, manage device configurations, and control access to corporate resources.
- Mobile application management (MAM): Utilizing MAM solutions to control access to and manage the lifecycle of mobile applications, including authentication, authorization, and data protection.
- Mobile containerization: Employing containerization techniques to separate corporate data and applications from personal data on mobile devices, ensuring controlled access and data separation.

Remote Access Control

Remote access control measures are necessary to secure access to organizational resources from remote locations. This includes:

- Virtual private networks (VPNs): Utilizing VPN technologies to establish secure connections between remote users and the organization's network, encrypting data transmission and authenticating remote users.
- Secure remote desktop protocols: Implementing secure remote desktop protocols, such as Remote Desktop Protocol (RDP) or Secure Shell (SSH), to allow authorized remote access to systems while protecting against unauthorized access.
- Two-factor authentication (2FA): Requiring users to authenticate through multiple factors, such as passwords and one-time tokens, to strengthen remote access security.

Cloud Services Access Control

Cloud services access control focuses on securing access to cloud-based resources and services. This includes:

- Identity and access management (IAM): Implementing IAM solutions to centrally manage user identities, access privileges, and authentication mechanisms across cloud services.
- Role-based access control (RBAC): Defining roles and assigning appropriate access permissions based on users' responsibilities and job functions within the cloud environment.
- Cloud access security brokers (CASBs): Employing CASBs to enforce security policies, monitor cloud activities, and control access to cloud resources.
- Encryption and data protection: Utilizing encryption techniques and data protection mechanisms to safeguard data stored in the cloud and control access to sensitive information.

Monitoring and Auditing

This section outlines key considerations for monitoring and auditing access control activities:

Access Logs and Event Monitoring

Access logs and event monitoring play a crucial role in tracking and detecting unauthorized access attempts and suspicious activities. Key considerations include:

- Logging access events: Enabling logging mechanisms to record access attempts, including successful and unsuccessful logins, changes to access privileges, and other relevant access-related events.
- Centralized log management: Implementing centralized log management systems to collect, store, and analyze access logs from various systems and applications.
- Log retention and review: Establishing policies for log retention duration and conducting regular reviews of access logs to identify potential security incidents or policy violations.
- Real-time monitoring: Implementing real-time monitoring systems to promptly detect and respond to suspicious access activities, unauthorized access attempts, or policy violations.
- Automated alerting: Configuring automated alerting mechanisms to notify security personnel of critical events, such as repeated failed login attempts or unauthorized access activities.

Intrusion Detection and Prevention Systems

Intrusion detection and prevention systems (IDPS) play a vital role in identifying and mitigating security incidents related to access control. Considerations include:

- Deploying IDPS solutions: Implementing IDPS solutions to monitor network traffic, detect anomalies, and identify potential unauthorized access attempts or malicious activities.
- Real-time alerting: Configuring IDPS systems to generate real-time alerts and notifications when suspicious activities or potential security breaches are detected.
- Incident response integration: Integrating IDPS with incident response processes to enable timely investigation and remediation of security incidents related to access control.
- Regular tuning and updates: Ensuring regular tuning and updating of IDPS systems to maintain their effectiveness and keep up with emerging threats and attack techniques.

Access Control Rules Implementation

To effectively enforce access control, organizations need to implement access control rules that align with their security requirements. This section outlines key considerations for implementing access control rules:

Defining Access Rights and Restrictions

Access rights and restrictions should be clearly defined for each entity based on their roles, responsibilities, and the information or assets they require access to. Key considerations include:

- Access rights determination: Identifying which entities require access to specific information and associated assets based on their job functions and responsibilities.
- Access restriction definition: Specifying limitations or restrictions on access rights to prevent unauthorized access or misuse of information and assets.
- Least privilege principle: Applying the principle of least privilege, where entities are granted the minimum access privileges necessary to perform their tasks effectively.

Role Assignment to Entity Groups

To simplify access control management, specific roles can be assigned to groups of entities. Considerations include:

- Role-based access control (RBAC): Implementing RBAC to define roles, their associated access permissions, and assigning entities to relevant roles based on their job functions and responsibilities.
- Role hierarchy: Establishing a role hierarchy to ensure appropriate access delegation and control within the organization.
- Regular review: Conducting regular reviews to validate and update role assignments as job roles and responsibilities change.

Consistency with Information Classification

Access control rules should be consistent with the classification and sensitivity of information. Considerations include:

- Information classification: Determining the classification levels and labeling of information based on its sensitivity, confidentiality, integrity, and availability requirements.
- Access controls based on classification: Aligning access control rules with information classification levels to ensure that only authorized entities can access and handle sensitive information.
- Periodic review: Conducting periodic reviews to reassess information classification and adjust access controls accordingly.

Consistency with Physical Perimeter Security

Access control rules should be consistent with physical perimeter security measures in place. Considerations include:

- Access control integration: Integrating logical access controls with physical security measures, such as locks, alarms, and surveillance systems, to ensure a comprehensive security approach.
- Access restrictions based on physical location: Implementing access controls that align with the physical location of entities and assets to prevent unauthorized access from physical entry points.

Consideration of Available Connections in Distributed Environments

In distributed environments, access control rules should consider the various types of connections available to entities. Considerations include:

- Network access controls: Implementing network-level access controls, such as firewalls and network segmentation, to restrict access based on entities' authorization and the type of network connection being used.
- Secure remote access: Establishing secure remote access mechanisms, such as virtual private networks (VPNs) or multi-factor authentication, to ensure that remote entities can access resources securely and within authorized boundaries.

Dynamic Elements and Granularity

Access control policies should account for dynamic elements and consider the appropriate level of granularity. This section explores the considerations related to dynamic access control elements and granularity:

Dynamic Access Control Elements

Dynamic access control elements allow for contextual and real-time decision-making regarding access permissions. Considerations include:

- Contextual factors: Incorporating contextual information, such as user location, time of access, device characteristics, and behavior patterns, to determine access permissions dynamically.
- Risk-based access control: Implementing risk-based access control mechanisms that assess the risk associated with specific access requests and adjust access permissions accordingly.
- Continuous monitoring: Utilizing continuous monitoring and analysis of access activities to identify anomalies, detect unauthorized access attempts, and adjust access controls in response to evolving threats.
- Event-driven access control: Integrating event-driven mechanisms that trigger access control decisions based on specific events or conditions, such as triggering additional authentication steps for high-risk activities.

Granularity of Access Control

Granularity refers to the level of detail at which access control is defined and enforced. Considerations include:

- Data field-level access control: Implementing access controls that are granular enough to restrict access to specific data fields within a larger dataset, ensuring that entities only have access to the specific information they require.
- System and application-level access control: Defining access controls at the system or application level to regulate access to entire systems or specific functionalities within applications.
- Network and infrastructure-level access control: Establishing access controls at the network or infrastructure level to restrict access to network resources, devices, or infrastructure components.
- Resource-specific access control: Tailoring access controls to specific types of resources, such as files, databases, or APIs, to ensure appropriate access permissions for each resource type.

Secure Authentication

Selection of Authentication Techniques and Strength

Carefully choose appropriate authentication techniques that can effectively verify the claimed identity of users, software, messages, and other entities.

The strength of authentication should be commensurate with the sensitivity and classification of the information being accessed.

Consider employing alternative authentication methods, such as digital certificates, smart cards, tokens, or biometric means, when stronger authentication and identity verification are required.

Multi-Factor Authentication

Enhance the security of critical information systems by implementing multi-factor authentication, which involves using additional authentication factors beyond passwords.

Utilize a combination of multiple factors, such as knowledge-based (passwords, PINs), possession-based (smart cards, tokens), and inherence-based (biometrics), to establish a layered and robust authentication process.

Implement rules and patterns to trigger the requirement of additional authentication factors under specific circumstances, such as accessing systems from unfamiliar locations, devices, or unusual times.

Biometric Authentication Considerations

When using biometric authentication, establish procedures to invalidate compromised biometric data and ensure alternative authentication methods are available.

Consider potential limitations of biometric authentication, such as environmental conditions (e.g., moisture or aging), and have contingency plans in place.

Secure Log-on Procedures and Technologies

Log-on procedures must be defined with a focus on minimizing the risk of unauthorized access by following this guidance:

- Delay displaying sensitive system or application information until the log-on process is successfully completed to prevent aiding unauthorized users.
- Include clear notice indicating that the system, application, or service is exclusively for authorized users.
- Avoid providing help messages during the log-on procedure that might assist unauthorized users in identifying correct or incorrect data.
- Validate log-on information only after all input data has been provided to prevent potential exploitation.
- Implement measures to counter brute-force log-on attempts, such as CAPTCHA, password reset after a defined number of failed attempts, or temporary user blocking.
- Log both unsuccessful and successful log-on attempts to monitor and detect potential breaches of log-on controls.
- Promptly alert users and system administrators upon detecting suspicious log-on activity, such as repeated incorrect password attempts.
- Provide separate channels to communicate post-log-on information, including the date and time of the previous successful log-on and details of any unsuccessful log-on attempts since then.
- Safeguard passwords by not displaying them in clear text during entry and preventing their transmission over the network in plain text to avoid interception.
- Terminate inactive sessions after a defined period of inactivity, particularly in high-risk locations or on user endpoint devices.
- Control connection duration times to bolster security for high-risk applications and limit the window of opportunity for unauthorized access.