**ARDHI UNIVERSITY**



**DEPARTMENT OF COMPUTER SYSEMS AND MATHEMATICS**

**INFORMATION SYSTEM MANAGEMENT (ISM)**

**IS 353 INFORMATION SYSTEMS AUDIT AND CONTROL**

**GROUP 9 ISM 3**

**INSTRUCTOR’S NAME:** MR. EMMANUEL MWAKASEGE

|  |  |  |
| --- | --- | --- |
| **STUDENT NAME** | **STUDENT NUMBER** | **SIGNATURE** |
| EMMANUEL MMBAGA | 26953/T.2021 |  |
| THEOFIL T. FRIMIN | 27016/T.2021 |  |
| IZACK D. SHABANI | 26967/T.2021 |  |
| REHEMA P. BAHEGWA | 27004/T.2021 |  |
| WITNESS SASUMA | 27023/T.2021 |  |
| CELINA JOHN JAPHET | 27843/T.2021 |  |
| MESHACK ANDONDILE | 26988/T.2021 |  |

QUESTION;

With respect to organization controls over information and processes, discuss the following in details. Provide clear examples to support your explanations.

1. Access controls

Access control is a critical aspect of organizational controls over information and processes. It involves managing who can access what resources, data, and functionalities within an organization's systems. Access control systems perform identification, authentication, and authorization of users and entities by evaluating required login credentials that may include passwords, pins, bio-metric scans, or other authentication factors. There are several types of access controls as follows;

**Physical access controls**, refers to the access control that control physical access to buildings, rooms, and equipment. For instance, a company might use key cards, biometric scanners, and security guards to control access to its data center by making sure that only employees with the appropriate clearance and key cards can enter to the data center, for the purpose of ensuring that sensitive information is prevented from unauthorized individuals.

**Logical access controls**, is an access control that restrict access to computer systems, network, and data. Logical access control systems perform identification authentication and authorization of users and entities by evaluating the required login credentials that can include usernames, passwords, personal identification numbers, and biometric scans. For example, a user might need to enter a username and password, with a unique code from their mobile device, to access sensitive company data.

**Role-Based Access Control (RBAC),** is an access control framework that assigns system access rights and permissions to users based on their roles within an organization. For example, a financial analyst in a company might have access to sensitive financial data but would not have the same access to the company’s HR records. RBAC is widely adopted due to its simplicity and ease of administration.

**Attribute-Based Access Controls (ABAC),** is a security framework that uses a set of policies to grant or deny access to resources. For example, an online banking system may use Attribute-Based Access control to grant access to account information. Access may be granted if the user’s attribute such as age, account type meets a certain criterion like being over 18 years old and having a specific account type.

**Discretionary Access Control (DAC),** is an access control that owners of resources can control access to their resources and can assign permission to others. In DAC, the owner of the information or resource decides who can access specific resources. For example, file systems in operating systems often use DAC. Uses can set permissions for files and directories, and they can grant access to other users.

**Mandatory Access Control (MAC),** is an approach where access control is based on security labels assigned to resources and clearance level assigned to users. For example, a system might enforce that only users with a certain security clearance level can access top-secret documents. This is commonly used in government and military settings where information classification is critical.

The following are some of the methods on how an organization controls access over information and processes.

Firstly, Authentication. This is the process of verifying the identity of users, devices, or processes attempting to access resources. Authentication methods include passwords, biometrics, security tokens, and multi-factor authentication (MFA). Strong authentication mechanisms are essential to ensure that only authorized entities can access the system. For example, A user logging into an online banking portal with their username and password. The system verifies the credentials before granting access to the user's account.

Secondly, Authorization. This method determines what actions users or processes are permitted to perform and what resources they can access. Authorization mechanisms enforce policies based on roles, permissions, attributes, or other factors. For example, in a healthcare system, a nurse may have permission to view patient records but not modify them, while a doctor may have both view and edit permissions. This authorization is based on the roles and responsibilities of each user.

Thirdly, Least Privilege Principle. This principle dictates that users should only be granted the minimum level of access necessary to perform their job functions. By limiting privileges to what is required, organizations can reduce the risk of unauthorized access and limit the potential damage in case of a security breach. For example, a customer service representative is granted access only to customer support tools and data relevant to their job function. They do not have access to financial records or sensitive HR information, reducing the risk of unauthorized access to critical data.

Also, Encryption. This is used to protect data from unauthorized access by converting it into an unreadable format that can only be deciphered with the appropriate decryption key. Data encryption is essential for safeguarding sensitive information both at rest and in transit. For example, data transmitted over a secure connection (HTTPS) is encrypted to prevent eavesdropping. Even if intercepted, the data remains unreadable without the encryption key, ensuring confidentiality.

Also, Segregation of Duties (SOD). This involves separating tasks and privileges among different individuals or roles to prevent conflicts of interest and reduce the risk of fraud or errors. For example, the person who approves a transaction should not be the same person who executes it. Another good example is in a financial institution, the person responsible for approving transactions should not have the ability to initiate them. This separation of duties ensures checks and balances and reduces the risk of fraud.

Lastly, Auditing and Logging. Access control systems should include auditing and logging capabilities to record access attempts, changes to permissions, and other relevant events. Audit logs provide visibility into who accessed what resources and when, facilitating / monitoring, incident investigation, and security analysis. For example, an organization maintains logs of user access attempts, including login times, IP addresses, and actions performed. These logs are regularly reviewed to identify suspicious activity and ensure compliance with security policies.

In conclusion, these examples illustrate how access control mechanisms are applied in various contexts to protect information, prevent unauthorized access, and ensure compliance with security standards. By implementing comprehensive access control measures, organizations can protect sensitive information, prevent unauthorized access, comply with regulatory requirements, and mitigate security risks effectively. Access control is an integral part of an organization's overall security strategy and requires ongoing monitoring, assessment, and improvement to adapt to evolving threats and business needs.