**Access Control Policy Analysis using NIST SP 800-53 (Rev.4)**

Ishan Prabhune (A20538828)

[iprabhune@hawk.iit.edu](mailto:iprabhune@hawk.iit.edu)

College of Computing,

Illinois Institute of Technology

ITMS 528: Database Security

Prof. Maurice Dawson

September 21, 2023

**Task 1: Selecting Access Controls:**

1. AC-3 ACCESS ENFORCEMENT
2. AC-4 INFORMATION FLOW ENFORCEMENT
3. AC-5 SEPARATION OF DUTIES
4. AC-6 LEAST PRIVILEDGE
5. AC-7 UNSUCCESSFUL LOGON ATTEMPTS
6. AC-8 SYSTEM USE NOTIFICATION
7. AC-9 PREVIOUS LOGON NOTOFICATION
8. AC-10 CONCURRENT SESSION CONTROL
9. AC-11 DEVICE LOCK
10. AC-12 SESSION TERMINATION
11. AC-13 SUPERVISION AND REVIEW – ACCESS CONTROL
12. AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION
13. AC-15 AUTOMATED MARKING
14. AC-16 SECURITY AND PRIVACY ATTRIBUTES
15. AC-17 REMOTE ACCESS

**Task 2: Access Control Write-up**

**SHALL Requirement and Elaboration of Details**

1. AC-3 ACCESS ENFORCEMENT

AC-3 SHALL Requirement:

The database system shall enforce access controls to ensure that only authorized users are granted access to the database resources.

Explanation:

This requirement is essential to database security since it addresses the fundamental idea of only allowing authorized users access. Access controls are essential for protecting sensitive data and guarding against unauthorized access, data breaches, and harmful database activity. During implementation, user roles must be established, suitable privileges must be granted, and access policies must be set up using the least privilege concept. Organizations can reduce the risk of data exposure, preserve data integrity, and comply with compliance requirements by enforcing this rule, such as those described in data protection regulations like GDPR or HIPAA. (NIST Special Publication 800-53 (Rev. 4))

1. AC-4 INFORMATION FLOW ENFORCEMENT

AC-4 SHALL Requirement:

The database system shall enforce information flow controls to prevent unauthorized data transfers or leakage between security domains.

Explanation:

Maintaining the security and integrity of sensitive data within a database system depends on this need. In order to prevent data from accidentally moving from higher to lower security domains or vice versa, it addresses the need to manage the flow of information across different security domains or levels. Mandatory access controls (MAC), data labeling, and data classification techniques are frequently used during implementation. It is especially important in circumstances when data categorization and access controls are essential, such as when protecting classified information or personally identifiable information that is subject to severe privacy rules. (NIST Special Publication 800-53 (Rev. 4))

1. AC-5 SEPARATION OF DUTIES

AC-5 SHALL Requirement:

The database system shall implement separation of duties controls to prevent conflicts of interest and ensure that users have appropriate roles and responsibilities.

Explanation:

The requirement to distribute duties and privileges among users in a way that prevents the concentration of power and lowers the possibility of abuse or misuse of authority is addressed by this need, which is essential for database security. Separation of responsibilities is a key security principle that ensures no single user or entity has complete authority over all facets of a crucial procedure or function, hence assisting in the prevention of fraud, mistakes, and unwanted access. In order to implement controls, users roles, responsibilities and access permissions must be clearly defined. These controls must then be enforced within the database system. Organizations can reduce the possibility of internal threats, improve accountability, and guarantee compliance with legal requirements that call for the separation of roles by enforcing this rule. (NIST Special Publication 800-53 (Rev. 4))

1. AC-6 LEAST PRIVILEDGE

AC-6 SHALL Requirement:

The database system shall follow the principle of least privilege, ensuring that users are granted only the minimum privileges necessary to perform their authorized tasks.

Explanation:

This requirement, which is a crucial aspect of database security, emphasizes the significance of restricting user access to only that which is necessary for their assigned tasks and responsibilities. By preventing users from accessing, altering, or deleting data or performing activities beyond what is strictly necessary, the principle of least privilege reduces the possibility of abuse or unintended consequences. During implementation, user responsibilities must be precisely defined, access permissions must be assigned, and these privileges must be periodically reviewed and changed as necessary. It is important to enforce this criterion since doing so decreases the attack surface, lowers the danger of data breaches, and improves system security overall by prohibiting unauthorized activity. (NIST Special Publication 800-53 (Rev. 4))

1. AC-7 UNSUCCESSFUL LOGON ATTEMPTS

AC-7 SHALL Requirement:

The database system shall log and track unsuccessful login attempts and take appropriate actions as defined in organizational policies.

Explanation:

As it covers the requirement to monitor and react to potential unauthorized access attempts, this requirement is essential for database security. Unsuccessful login attempts are recorded and tracked by the system, which allows it to spot patterns of questionable behavior and possible security risks. Implementation involves setting up the database system such that it keeps track of failed login attempts and details like the source, username, and timestamp. This data, when combined with the right policies and automated actions, can aid organizations in identifying and reducing insider risks, illegal access, and brute-force attacks. It is essential for enterprises to maintain audit trails of login activity for security and forensic purposes in order to comply with security standards and laws. (NIST Special Publication 800-53 (Rev. 4))

1. AC-8 SYSTEM USE NOTIFICATION

AC-8 SHALL Requirement:

The database system shall display a system use notification message to users upon successful authentication, informing them that their activities are monitored.

Explanation:

Maintaining accountability and transparency in database security depends on this criterion. Clients are bound to act dependably and consistently when they are made mindful that their activities are being watched and evaluated. Execution includes setting up the data set framework so that, after effective confirmation, a message is created and shown to clients. This message serves as a reminder of the company's security guidelines and the repercussions of unauthorized or improper database activity. Significantly, it facilitates investigations by explicitly establishing user awareness of monitoring methods in the event of security incidents or breaches, fosters adherence to data access restrictions, and serves to deter hostile activity. In particular, in areas with strict data protection standards, this requirement is in line with appropriate security procedures and legal compliance. (NIST Special Publication 800-53 (Rev. 4))

1. AC-9 PREVIOUS LOGON NOTOFICATION

AC-9 SHALL Requirement:

The database system shall provide users with a notification indicating the date and time of their previous successful login.

Explanation:

Because it enables users to monitor their own login activities and identify any unwanted access to their accounts, this criterion is important for database security. The implementation process involves setting up the database system to notify users after a successful login and display details about that successful login, including the time and date. This notice acts as an alert system, enabling consumers to spot any shady or unauthorized access to their accounts right away. Additionally, it encourages user responsibility and awareness of their own account security. Users can quickly respond to unwanted access or potential compromise by changing their passwords or reporting the issue, helping to create a more secure database environment. (NIST Special Publication 800-53 (Rev. 4))

1. AC-10 CONCURRENT SESSION CONTROL

AC-10 SHALL Requirement:

The database system shall enforce controls to limit the number of concurrent user sessions per user account.

Explanation:

This criterion, which limits the number of concurrent connections that a single user account can initiate, is crucial for managing and securing database resources. During implementation, the database system must be set up to keep track of and control the amount of active sessions connected to each user account. As too many concurrent sessions may result in illegal access or excessive resource utilization, significance lies in preventing potential abuse or misuse of credentials. Organizations can limit the risk of credential sharing, illegal access, and denial-of-service attacks by enforcing this restriction. In situations where resource allocation is crucial, like in financial organizations or healthcare systems, it also complies with best practices for access control and security. (NIST Special Publication 800-53 (Rev. 4))

1. AC-11 DEVICE LOCK

AC-11 SHALL Requirement:

Users shall be required to lock their devices when not in use to prevent unauthorized access to the database.

Explanation:

The security of information base frameworks should be fortified by this necessity, particularly when clients access touchy information on their gadgets. Implementation entails implementing a rule requiring users to turn on device locks, such as password-protected screensavers or device screen locks, when their devices are not being actively used. This criterion is important since it guards against unauthorized users physically accessing a user's device and hence the database. Device locks give an extra degree of security, making sure that even when a device is briefly left unattended, it is still safe and that unauthorized people cannot access vital data. This rule strengthens data security and is consistent with larger security strategies meant to protect sensitive data from outside threats and unauthorized users. (NIST Special Publication 800-53 (Rev. 4))

1. AC-12 SESSION TERMINATION

AC-12 SHALL Requirement:

The database system shall automatically terminate user sessions after a predefined period of inactivity.

Explanation:

Due to its ability to reduce the risk of illegal access or data disclosure caused by user idleness, this requirement is essential for database security. Implementation entails setting up the database system to keep track of user sessions and log users out automatically after a predetermined amount of idle time. This criterion is significant since it narrows the exposure window for potential security concerns. The system makes sure that even if a user forgets to log out or leaves their session unattended, unauthorized users cannot take advantage of the open session to access sensitive data by immediately ending inactive sessions. In contexts where several users use the same system or device, this control also adheres to security best practices. (NIST Special Publication 800-53 (Rev. 4))

1. AC-13 SUPERVISION AND REVIEW – ACCESS CONTROL

AC-13 SHALL Requirement:

Regular reviews of access control policies, user accounts, and permissions shall be conducted to ensure compliance with security policies.

Explanation:

This mandate highlights the significance of constant monitoring and assessment of access control protocols inside a database system. It comprises routinely checking user accounts, access rights, and access control rules to make sure they are in line with the changing security demands and policies of an organization. The implementation entails planning and carrying out regular evaluations, audits, or reviews of user credentials and access control configurations. The importance of this need is tied to keeping access controls legitimate and efficient over time. Organizations can spot security flaws, unauthorized accesses, and potential dangers by routinely checking access policies and user accounts. By doing this, they can make sure that only authorized people have the right amount of access to database resources. (NIST Special Publication 800-53 (Rev. 4))

1. AC-14 PERMITTED ACTIONS WITHOUT IDENTIFICATION OR AUTHENTICATION

AC-14 SHALL Requirement:

The database system shall restrict certain actions to be performed without proper user identification and authentication as specified by organizational policies.

Explanation:

This prerequisite is necessary to impose stringent security controls within a database system. It stipulates that certain operations, as outlined by the organization's policies, must be carried out only after the user's identification has been verified. The database system must be configured during implementation to recognize and enforce these particular actions and the corresponding authentication requirements. This need is significant because it guards against anonymous or unauthorized access to vital information or services, especially those that could be highly risky to security. Organizations can ensure that actions requiring user identity and authentication are carried out securely by imposing this restriction, lowering the possibility of unauthorized access or malicious activity. Additionally, this criterion promotes adherence to legal standards for access control and authentication as well as security best practices. (NIST Special Publication 800-53 (Rev. 4))

1. AC-15 AUTOMATED MARKING

AC-15 SHALL Requirement:

The database system shall automatically apply security markings and labels to data based on its sensitivity and classification.

Explanation:

In contexts where data classification is crucial, this requirement is crucial for guaranteeing the proper treatment and security of data within a database system. Implementation entails setting up the database system so that security labels and markings are automatically applied to data in accordance with predetermined standards, such as sensitivity, classification, or content. This requirement's importance lies in streamlining and improving data management and protection. Organizations may consistently and precisely label data by automating the marking process, ensuring that it is handled in compliance with security regulations. Additionally, it helps with access control, data encryption, and auditing, lowering the risk of data breaches and assuring adherence to legal and contractual responsibilities as well as compliance with data protection legislation. (NIST Special Publication 800-53 (Rev. 4))

1. AC-16 SECURITY AND PRIVACY ATTRIBUTES

AC-16 SHALL Requirement:

Security and privacy attributes shall be applied to sensitive data within the database to protect confidentiality, integrity, and privacy.

Explanation:

This prerequisite is essential for protecting sensitive data kept in databases. It stipulates that sensitive data must be protected from unauthorized access by applying security and privacy features including encryption, access limits, and data masking. Implementation involves setting up the database system so that these qualities are applied to sensitive data in accordance with its usage and classification. This requirement's importance is in ensuring that private data is effectively safeguarded from unauthorized access, data breaches, and privacy violations. Organizations can comply with regulatory standards, prevent data exposure, and uphold the confidence of their stakeholders by implementing these security and privacy qualities. (NIST Special Publication 800-53 (Rev. 4))

1. AC-17 REMOTE ACCESS

AC-17 (NIST Special Publication 800-53 (Rev. 4)) SHALL Requirement: Remote access to the database system shall be restricted to authorized users and devices, and secure authentication methods shall be enforced.

Explanation:

In modern businesses, where users may need to access the database from outside the actual network border, this requirement addresses the need for secure remote access to the database system. To ensure the confidentiality and integrity of data in transit, it requires that only authorized users and trusted devices be permitted to establish distant connections. Secure authentication techniques, such as VPNs or secure tunneling protocols, are also required. Prior to allowing remote access, the database system must be configured to verify user credentials, device IDs, and connection types. Organizations can prevent data breaches, maintain data privacy, and satisfy compliance requirements by establishing secure remote access controls, especially in sectors where data protection and confidentiality are crucial, like healthcare or finance. (NIST Special Publication 800-53 (Rev. 4))

**References**

·       *Language-Based Information-Flow Security*. <https://ieeexplore.ieee.org/abstract/document/1159651>. Accessed 22 Sept. 2023.

·       *Access Control and Session Management in the HTTP Environment*. [https://ieeexplore.ieee.org/abstract/document/895139. Accessed 22 Sept. 2023](https://ieeexplore.ieee.org/abstract/document/895139.%20Accessed%2022%20Sept.%202023).

·       *BDSS-FA: A Blockchain-Based Data Security Sharing Platform With Fine-Grained Access Control*. <https://ieeexplore.ieee.org/abstract/document/9086734>. Accessed 22 Sept. 2023.

·       Blobel, Bernd, et al. “Modelling Privilege Management and Access Control.” *International Journal of Medical Informatics*, vol. 75, no. 8, Aug. 2006, pp. 597–623. *ScienceDirect*, <https://doi.org/10.1016/j.ijmedinf.2005.08.010>.

·       *Context-Based Access Control Systems for Mobile Devices*. <https://ieeexplore.ieee.org/abstract/document/6807727>. Accessed 22 Sept. 2023.

·       De Capitani Di Vimercati, Sabrina, et al. “Access Control: Principles and Solutions.” *Software: Practice and Experience*, vol. 33, no. 5, Apr. 2003, pp. 397–421. *DOI.org (Crossref)*, <https://doi.org/10.1002/spe.513>.

·       Hu, Vincent C., and Karen Scarfone. *Guidelines for Access Control System Evaluation Metrics*. NIST IR 7874, National Institute of Standards and Technology, Sept. 2012, p. NIST IR 7874. *DOI.org (Crossref)*, <https://doi.org/10.6028/NIST.IR.7874>.