Humberto Gonzalez

July 15, 2024

2.5: Assignment: Create Identity Access Management Security Policies Using a Framework

AC-1: Access Control Policy and Procedures

Justification:

Ensuring the protection of confidential data requires the establishment of thorough access control policies and processes. It harmonizes the organization-wide processes for granting, tracking, and revoking access. Establishing explicit policies increases the likelihood that staff members will follow excellent practices, lowering the possibility of unwanted access. Staff training and routine process updates ensure the efficacy and applicability of the policies. It is possible to implement this within a year if funds are set aside for training initiatives and policy creation.

Case Study Support:

"SnowBe Online processes most of its sales online through an AWS-hosted website, accepts and stores all credit cards, and retains customer information indefinitely."

AC-2: Account Management

Justification:

Managing accounts well is essential to limiting access to the systems and information within the company. The risk of unauthorized access is reduced by ensuring that only authorized users have accounts and that these accounts are properly managed. This entails establishing procedures for the creation, update, and cancellation of accounts. Identity and Access Management (IAM) systems can be used to systematically enforce these procedures. By integrating IAM solutions with current systems and providing personnel with account management training, it is possible to implement this control within a year.

Case Study Support:

"SnowBe Online processes the majority of its sales online through an AWS-hosted website, accepts and stores all credit cards, and retains customer information indefinitely."

(1) AC-2 | Automated System Account Management

Justification:

The administrative load and risk of human error associated with manual account administration are decreased by automated system account management. Automation improves consistency and security by ensuring that accounts are created, changed, and terminated in line with predetermined policies. IAM solutions that interface with current systems to automate these procedures can be used to do this. Additionally, automation makes it possible to handle high amounts of account changes more effectively, which is crucial for a company like SnowBe Online that has a sizable user base and volume of transactions. By utilizing existing technologies and incorporating them into the current infrastructure, this can be implemented within a year.

Case Study Support:

"The scale of SnowBe Online's operations requires automation to manage accounts efficiently across its multiple locations and platforms."

(2) AC-2 | Automated Temporary and Emergency Account Management

Justification:

Temporary access can be issued quickly, safely, and automatically revoked when it is no longer required with the help of automated temporary and emergency account management. This control lessens the possibility of exploitable residual access rights. Configuring the current IAM

tools to enable the creation of temporary accounts with automatic expiration dates will help implement this. This is especially crucial in dynamic settings where there is a constant demand for temporary access. Policies and system configurations may be changed to accommodate this degree of automation in less than a year, enhancing overall security and operational effectiveness.

Case Study Support:

"Given the dynamic nature of SnowBe Online's operations, including remote work, temporary access solutions are necessary for operational flexibility."

(3) AC-2 | Disable Accounts

Justification:

One essential security step to stop unwanted access is to disable accounts that are no longer in use. When users depart from the company or after extended periods of inactivity, automated procedures can guarantee that accounts are immediately disabled. This reduces the possibility of accounts going dormant and being hacked. Configuring system settings to automatically disable accounts based on established criteria is a manageable process that may be completed in a year to implement this control. Ensuring adherence to the policy through frequent audits and monitoring helps to keep the environment safe.

Case Study Support:

"The indefinite retention of customer information makes it critical to ensure that only active, authorized accounts can access the system."

(4) AC-2 | Automated Audit Actions

Justification:

Automated audit actions improve security by guaranteeing adherence to access control policies and offering constant monitoring and prompt response to suspect activity. Without human intervention, automated systems are capable of producing alarms, logging incidents, and starting predetermined responses. Integrating audit and monitoring technologies with the current security architecture is necessary for its implementation. These technologies can be set up to automatically monitor and react to specified actions for up to a year, which enhances the overall security posture by making sure that any anomalies are promptly found and fixed.

Case Study Support:

"SnowBe Online's need for compliance with regulations like PCI DSS makes continuous auditing crucial."

(5) AC-2 | Inactivity Logout

Justification:

By automatically ending sessions that have been idle for a predetermined amount of time, inactivity logout lowers the possibility of illegal access from unattended devices. This feature makes sure that when users leave their devices unattended, private information is not exposed. To put this into practice, system settings must be configured to impose inactivity timeouts, which may be done in less than a year. As an extra security protection, this technique is especially crucial in settings where workers can neglect to manually log out.

Case Study Support:

"Given the high volume of customer data processed, automatic logout enhances the security of unattended devices."

AC-3: Access Enforcement

Justification:

Access enforcement makes sure that all systems have actively implemented and enforced access control restrictions, rather than merely theoretical ones. By ensuring that only those with the appropriate authorization can access critical data and systems, this stops unwanted access. By utilizing current tools and technologies, it is possible to configure access control mechanisms in both software and hardware to implement this control in less than a year. Frequent audits and evaluations guarantee that the policies are appropriately implemented and continue to be successful over time.

Case Study Support:

"SnowBe Online's processing of sensitive customer data necessitates strict enforcement of access policies."

(3) AC-3 | Mandatory Access Control

Justification:

To maintain a high level of security, Mandatory Access Control (MAC) enforces strict access regulations set by the system administrator regardless of user identity. By preventing users from overriding security policies, this control guarantees that sensitive data is consistently protected. Setting up systems to enforce these standards is part of implementing MAC, and with the correct

resources and guidance, this can be done in less than a year. When it comes to highly sensitive data, MAC works especially well because it makes sure that access is strictly regulated and tracked.

Case Study Support:

"The need to protect sensitive customer data across multiple systems justifies the implementation of MAC."

(7) AC-3 | Role-Based Access Control

Justification:

Access management is made easier using Role-Based Access Control (RBAC), which assigns permissions based on user roles rather than individual users. By doing this, administrative overhead is decreased and users are guaranteed the right amount of access for the tasks assigned to them. Determining roles and related permissions, then setting up mechanisms to enforce these roles, are the steps involved in implementing RBAC. This can be accomplished over a year by carrying out a thorough review of job functions, defining roles, and updating systems to take these roles into account. RBAC improves security by guaranteeing uniform access controls throughout the company.

Case Study Support:

"SnowBe Online’s diverse employee roles necessitate a structured approach to access management."

AC-6: Least Privilege

Justification:

By ensuring that users have only the access required to carry out their job tasks, the concept of least privilege is enforced, lowering the danger of unauthorized access. This reduces the possibility of harm from unintentional or malevolent acts. To implement this control, user permissions must be routinely reviewed and adjusted to reflect their responsibilities. By conducting access evaluations and revising access policies, this can be completed in less than a year. A key security principle known as least privilege helps safeguard sensitive data by preventing unauthorized access.

Case Study Support:

"With sensitive customer information at stake, minimizing access reduces potential vulnerabilities."

(1) AC-6 | Authorized Access To Security Functions

Justification:

Limiting access to security features makes ensuring that security settings can only be changed by authorized workers, preventing unauthorized changes that could compromise security. System configuration is required for this control to limit access depending on user roles and permissions. By designating roles with access to security functions and making the necessary updates to system configurations, this can be implemented within a year. By guaranteeing that vital security features are shielded from unwanted access, this restriction improves security.

Case Study Support:

"Given the sensitive nature of security configurations, it’s crucial to restrict access to authorized personnel only."

(2) AC-6 | Non-Privileged Access For Non-security Functions

Justification:

Reducing the possibility of accidental or intentional abuse of privileges is achieved by guaranteeing that users carry out non-security tasks without privileged access. To do this, role-based permissions that distinguish between security-related and non-security-related tasks must be defined and enforced. By analyzing work functions, assigning suitable roles, and upgrading system configurations, this can be implemented within a year. By restricting the usage of privileged accounts to essential security duties alone, this restriction aids in the maintenance of a secure environment.

Case Study Support:

"SnowBe Online’s diverse operations require a clear separation of duties to maintain security."

(3) AC-6 | Network Access to Privileged Commands

Justification:

By limiting network access to privileged commands, security is improved by preventing illegal remote changes to system configurations. To restrict access to privileged commands, network settings like firewalls and access control lists (ACLs) must be configured. By identifying the important commands and making the necessary updates to the network setups, this can be

implemented within a year. By lowering the possibility of illegal changes to system configurations, this control safeguards the network's integrity and security.

Case Study Support:

"With remote work being a significant part of operations, controlling access to privileged commands is essential."

AC-7: Unsuccessful Logon Attempts

Justification:

By locking accounts after a certain number of unsuccessful login attempts, limiting the number of unsuccessful tries lowers the possibility of brute-force assaults. This control can be implemented in less than a year by modifying the system settings to enforce logon attempt restrictions. To make sure that legitimate users are fairly impacted, account lockouts are regularly monitored and reviewed. By blocking unwanted access through repeated guesses at login credentials, this measure improves security.

Case Study Support:

"The high volume of sensitive data processed necessitates robust protection against unauthorized access attempts."

(2) AC-7 | Purge or Wipe Mobile Device

Justification:

Data is protected in the event of device theft or loss by ensuring that mobile devices can be erased after a predetermined number of unsuccessful login attempts. This control, which may be put into effect in less than a year, entails setting up mobile device management (MDM) programs

to enforce wipe restrictions. If a device is lost or stolen, this feature is especially crucial for safeguarding sensitive data on remote work computers. Wipe policies are tested and reviewed frequently to make sure they work well and don't affect users who are authorized.

Case Study Support:

"SnowBe Online's use of laptops and mobile devices for remote work makes this control crucial."

AC-11: Session Lock

Justification:

Unauthorized access to unattended devices is prevented by locking sessions after a certain amount of idleness. This control can be implemented in less than a year by modifying system settings to enforce session locks. Session lock settings should be regularly reviewed and monitored to make sure they are efficient and do not negatively affect productivity. By guaranteeing that unattended devices are shielded from unwanted access, especially in public or shared workspaces, this control improves security.

Case Study Support:

"Given the sensitivity of customer data, session locks add a necessary layer of security."

(1) AC-11 | Pattern-Hiding Displays

Justification:

Displays with pattern-hiding stop people from looking at information on the screen without permission or shoulder surfing. This control entails hiding sensitive information when the device is not in use by setting up screensavers or utilizing screen filters. If the required hardware is

provided and system settings are updated, this can be implemented within a year. This safeguard is especially crucial in open-plan workplaces where uninvited visitors may access private data on screens that are left unattended. Pattern-hiding settings should be regularly reviewed and adjusted to maintain their effectiveness and user-friendliness.

Case Study Support:

"The open nature of some work environments necessitates measures to protect screen information."

AC-12: Session Termination

Justification:

Unattended sessions can be terminated at the user's request or after a period of inactivity to avoid unwanted access. Within a year, this control can be implemented by setting up the system to enforce session termination policies. Session termination settings should be regularly reviewed and monitored to make sure they are efficient and do not negatively affect productivity. By guaranteeing that unattended sessions are appropriately ended, this rule improves security by lowering the possibility of unwanted access.

Case Study Support:

"Given the volume of customer data, terminating inactive sessions is crucial for maintaining security."

(1) AC-12 | User-Initiated Logouts

Justification:

By enabling users to manually log out, you may lower the possibility of illegal access by ensuring that users can end sessions when not in use. This control entails teaching people the value of logging out and making logout choices easily accessible. By performing user training and changing system interfaces, this can be implemented within a year. Effective utilization of user-initiated logouts is ensured by routine monitoring and assessment. By giving users the authority to end their sessions on their own, this option improves security by lowering the possibility of unwanted access.

Case Study Support:

"SnowBe Online's diverse user base necessitates user-friendly security features."

(2) AC-12 | Termination Message

Justification:

To avoid confusion and potential security issues, a termination message is sent to users upon session termination to let them know that their session has finished. Within a year, this control can be implemented by setting up the system to display termination messages. Termination communications should be reviewed and adjusted regularly to guarantee clarity and effectiveness. By guaranteeing that users are informed of their session status, this measure improves security by lowering the possibility of unwanted access brought on by miscommunication or confusion.

Case Study Support:

"Clear communication of session termination enhances security awareness among users."

AC-17: Remote Access

Justification:

By limiting access to the network to authorized users only, remote access security guards against outside threats. To safeguard remote connections, this control entails setting up VPNs, multi-factor authentication (MFA), and other security precautions. By changing setups and utilizing current remote access technologies, this can be implemented within a year. Maintaining the effectiveness and integrity of remote access settings requires periodic monitoring and review. By guaranteeing that remote access is appropriately secured and shielding confidential data from unwanted access, this measure improves security.

Case Study Support:

"With a significant portion of operations conducted remotely, securing remote access is critical."

(1) AC-17 | Monitoring and Control

Justification:

Any efforts at unwanted access are guaranteed to be quickly identified and dealt with by monitoring and control of remote access. To monitor remote access activities, this control entails establishing intrusion detection systems (IDS) and monitoring tools. By combining monitoring tools with the current security architecture, this can be implemented within a year. To keep monitoring settings responsive and effective, they should be reviewed and adjusted regularly. By

continuously monitoring remote access activities and facilitating prompt response to possible threats, this control improves security.

Case Study Support:

"The distributed nature of SnowBe Online's operations necessitates robust monitoring of remote access."

(2) AC-17 | Protection of Confidentiality and Integrity Using Encryption

Justification:

Data confidentiality and integrity are ensured by encrypting remote access communications, which guards against manipulation and interception. Setting up VPNs and utilizing encryption techniques to protect remote connections are part of this control. By upgrading remote access setups and educating users on safe remote access procedures, can be implemented within a year. Encryption settings must be regularly reviewed and adjusted to stay current and functional. By guaranteeing that communications via remote access are appropriately safeguarded, this control improves security by lowering the possibility of data breaches.

Case Study Support:

"The sensitivity of customer information requires encryption to protect data in transit."

(3) AC-17 | Managed Access Control Points

Justification:

Keeping an eye on access control points improves security by ensuring that only approved remote connections are permitted. To restrict remote access to approved people and devices, this control entails setting firewalls and access control lists (ACLs). By regularly reviewing access

and upgrading network configurations, this can be implemented within a year. Access control points should be routinely inspected and adjusted to guarantee their continued effectiveness and adaptability to evolving security requirements. By guaranteeing that remote access is strictly regulated and lowering the possibility of unwanted access, this control improves security.

Case Study Support:

"SnowBe Online's reliance on remote work necessitates stringent control of access points."

AC-19: Access Control for Mobile Devices

Justification:

By implementing access control for mobile devices, unwanted access to the network can be prevented and only authorized devices can access it. Setting up mobile device management (MDM) programs to impose access controls is part of this control. By using the MDM tools that are already in place and making configuration updates, this can be implemented within a year. Mobile access settings are kept current and functional by routine inspection and monitoring. By guaranteeing that mobile devices are appropriately maintained and regulated, this management improves security by lowering the possibility of unwanted access.

Case Study Support:

"The use of laptops and mobile devices for remote work requires robust access controls."

(4) AC-19 | Restriction for Classified Information

Justification:

Sensitive data is kept safe by limiting access to classified information on mobile devices. To prevent unauthorized access to sensitive information, this control entails creating MDM policies

to restrict access based on data classification. By regularly reviewing access and modifying MDM setups, this can be implemented within a year. Access limits should be routinely reviewed and adjusted to ensure their continued effectiveness and responsiveness to evolving security requirements. By guaranteeing that classified information is appropriately safeguarded and lowering the possibility of data breaches, this control improves security.

Case Study Support:

"The sensitivity of customer information necessitates stringent controls on mobile access."

(5) AC-19 | Full Device or Container-Based Encryption

Justification:

Mobile device encryption protects sensitive data by guaranteeing that it is safe even in the event of device loss or theft. To implement encryption policies on devices and data containers, MDM systems must be configured. Updating MDM settings and educating users on encryption techniques will help implement this within a year. Encryption settings must be regularly reviewed and adjusted to stay current and functional. By guaranteeing that mobile devices are correctly encrypted and lowering the possibility of data breaches in the event of device loss or theft, this measure improves security.

Case Study Support:

"The use of mobile devices for accessing sensitive information requires encryption to protect data at rest."

Reference

AC: Access Control - CSF Tools