**Security Assessment Report (SAR)**

# **Executive Summary**

## Overview:

The Security Assessment Report (SAR) for JohnDoe&Co has been prepared to evaluate the current security posture of the organization's information systems. This assessment encompasses a comprehensive review of implemented controls, risk management practices, and adherence to security standards as outlined in the System Security Plan (SSP). The objective of this assessment is to identify potential vulnerabilities, assess risks, and recommend enhancements to fortify the security environment.

## Purpose:

The primary purpose of this assessment is to ensure that JohnDoe&Co's information systems are protected against emerging threats and vulnerabilities while maintaining compliance with regulatory and industry standards. This report provides an in-depth analysis of the current security controls, evaluates their effectiveness, and identifies areas requiring improvement.

## Scope:

The assessment covers all critical aspects of JohnDoe&Co's IT infrastructure, including network security, data protection, access controls, incident response capabilities, and compliance with relevant security policies. The scope also includes a review of the Plan of Action and Milestones (POAM), risk assessments, and the effectiveness of implemented security controls.

## Key Findings:

1. Strengths: The assessment identified several strengths in JohnDoe&Co's security posture, including robust access control mechanisms, comprehensive data encryption practices, and a well-defined incident response plan. The organization has implemented numerous security controls that effectively mitigate many common threats.
2. Areas of Concern: Despite the strengths, the assessment uncovered several vulnerabilities that require immediate attention. These include outdated software components, insufficient monitoring of network traffic, and gaps in employee security awareness training. These weaknesses present potential risks to the integrity, confidentiality, and availability of JohnDoe&Co's information systems.
3. Risk Management: The risk assessments conducted revealed that while JohnDoe&Co has made significant progress in managing risks, there are areas where risk mitigation strategies need to be strengthened. Particularly, the risk associated with third-party vendors and the management of privileged access require enhanced controls and continuous monitoring.

Conclusion:

The SAR concludes that while JohnDoe&Co has established a solid foundation of security controls, there are critical areas that require improvement to achieve a more resilient security posture. Addressing the identified vulnerabilities and enhancing the current risk management practices will be essential in safeguarding JohnDoe&Co's information systems against future threats. The report provides detailed recommendations to guide the necessary improvements and ensure ongoing compliance with security standards.

## **1.1 Purpose of the Security Assessment Report**

* The purpose of this Security Assessment Report (SAR) is to evaluate the current security posture of JohnDoe&Co's information systems by identifying vulnerabilities, assessing the effectiveness of existing security controls, and analyzing associated risks. The assessment aims to ensure that the organization's security practices comply with industry standards and legal requirements while providing actionable recommendations to mitigate risks and enhance overall security. This report serves as a vital tool for guiding leadership decisions on security investments and strategic planning to protect JohnDoe&Co’s sensitive data and maintain a resilient IT environment.

## **1.2 Overview of the System**

The system under assessment is the **JohnDoe&Co Information System**, a critical infrastructure designed to support the organization’s operations, data management, and secure communication needs. The primary purpose of this system is to ensure the confidentiality, integrity, and availability of sensitive information processed, stored, and transmitted within JohnDoe&Co’s operational environment.

This assessment covers the entire JohnDoe&Co Information System, including its hardware, software, and network components. The scope of the assessment includes evaluating the system's security controls, identifying potential vulnerabilities, and assessing the risks associated with these vulnerabilities.

The JohnDoe&Co Information System operates within a **Moderate Impact** environment, categorized as such due to the potential impact on confidentiality, integrity, and availability should a security breach occur. The system is interconnected with several other external systems, including third-party cloud services and partner networks, which are integral to its operations. These interconnections are managed with stringent security protocols to ensure that data exchanges remain secure and that the system’s overall security posture is not compromised.

**1.3 Summary of Findings**

* Provide a high-level summary of the key findings from the security assessment.
* Highlight the most critical vulnerabilities, the effectiveness of the implemented controls, and any significant residual risks.

# **2. Assessment Methodology**

**2.1 Assessment Approach**

* The security control assessment of the JohnDoe&Co Information System was conducted using a comprehensive and methodical approach to evaluate the effectiveness of the implemented security controls. The assessment leveraged a combination of techniques to ensure a thorough evaluation, including:
* Interviews: Structured interviews were conducted with key personnel involved in the management, operation, and security of the system. These interviews aimed to gather insights into the system's security practices, control implementations, and incident response procedures.
* Document Reviews: A detailed review of security-related documentation was performed, including the System Security Plan (SSP), Plan of Action and Milestones (POAM), risk assessments, and incident response plans. This review helped to verify that the documented security controls align with the organization's security policies and standards.
* Vulnerability Scanning: Automated vulnerability scanning tools were employed to identify potential security weaknesses within the system’s network, applications, and devices. The scans focused on detecting unpatched software, misconfigurations, and other vulnerabilities that could be exploited by attackers.
* Penetration Testing: Targeted penetration testing was conducted to simulate real-world attacks on the system. This testing provided an in-depth analysis of the system’s defenses by attempting to exploit identified vulnerabilities and assess the effectiveness of the implemented security controls in mitigating these threats.
* The assessment was conducted in alignment with recognized security frameworks and standards, specifically NIST SP 800-53 and NIST SP 800-171. These frameworks provided a structured and standardized approach to evaluating the security controls, ensuring that the assessment was comprehensive and consistent with industry best practices.
* This multi-faceted approach allowed for a robust evaluation of the JohnDoe&Co Information System’s security posture, providing the organization with a clear understanding of its strengths and areas requiring improvement.

# **3. Detailed Findings**

**3.1 Control Assessment Results**

### Control Identifier: IA-5(6)

Control Description: Authenticator Management | Protection of Authenticators. This control is focused on ensuring that authenticators, such as passwords or tokens, are protected in accordance with the security category of the information they permit access to. Specifically, for systems containing multiple security categories without reliable physical or logical separation, the control mandates that authenticators be protected at a level commensurate with the highest security category of information present.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a noted risk of password exposure. While the control is implemented, passwords may still be exposed to unauthorized parties during storage or transmission. This vulnerability poses a significant risk as it could lead to unauthorized access, data breaches, and the potential loss of sensitive information.

Assessment Status: Implemented

Associated Risk: The risk associated with the current implementation is moderate to high. Despite the control being in place, the exposure of passwords during storage or transmission remains a concern. If exploited, this vulnerability could result in severe security incidents, including unauthorized access to critical systems and sensitive data breaches. To mitigate this risk, it is recommended to implement stronger cryptographic protections for passwords during storage and transmission. This would ensure that even if passwords are intercepted or accessed, they cannot be easily deciphered, thus bolstering the overall security of the authentication process within the organization.

### Control Identifier: SC-7(10)

Control Description: Boundary Protection | Prevent Exfiltration. This control is designed to prevent the unauthorized exfiltration of information from the system. It includes both intentional and unintentional exfiltration prevention and requires the organization to conduct regular exfiltration tests. Techniques to prevent exfiltration may be implemented at various points, including internal endpoints, external boundaries, and managed interfaces. These techniques include adherence to protocol formats, monitoring for abnormal activity, and employing data loss prevention tools. Devices like deep packet inspection firewalls and XML gateways are used to enforce strict adherence to protocol formats at the application layer.

Assessment Findings: The control is In Place within the JohnDoe&Co Information System. However, there remains a risk associated with unauthorized access or data breaches, particularly concerning remote devices. The current setup allows remote devices to potentially connect simultaneously to both organizational systems and external networks. This creates a vulnerability that could be exploited by attackers to exfiltrate data.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is significant due to the potential for remote devices to establish split tunneling, which could lead to unauthorized access and data breaches. If attackers exploit this vulnerability, they could gain access to sensitive information and exfiltrate it without detection. The likelihood of such an incident is moderate to high, given the existing conditions. To mitigate this risk, it is crucial to ensure that remote devices cannot connect to both the internal network and external networks simultaneously, thereby reducing the chances of unauthorized data exfiltration and enhancing the overall security of the network.

### Control Identifier: SC-7(5)

Control Description: Boundary Protection | Deny by Default — Allow by Exception. This control requires that network communications traffic be denied by default and only allowed by exception. It applies to both inbound and outbound traffic, ensuring that only essential and approved system connections are permitted. This approach helps to enforce a strict security posture by allowing only necessary and explicitly authorized communications while blocking all others by default.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a potential risk of unauthorized access or data breaches due to overly permissive network traffic rules. While the control is implemented, if not properly configured or maintained, it could allow unauthorized or malicious network traffic to enter the network.

Assessment Status: Implemented

Associated Risk: The risk associated with this control arises from the possibility that unauthorized or malicious network traffic could bypass security measures due to misconfigurations or exceptions that are too permissive. This could lead to security breaches and other harmful events, such as data theft or network compromise. The likelihood of such incidents is moderate, but the impact could be severe. To mitigate this risk, it is essential to ensure that the deny-by-default, allow-by-exception policy is strictly enforced and regularly reviewed to prevent any unauthorized communications from occurring. This policy significantly reduces the chances of unauthorized access, thereby enhancing the overall security of the network.

### Control Identifier: IA-5

Control Description: Authenticator Management. This control involves managing system authenticators by verifying the identity of the recipient during initial distribution, ensuring the strength of authenticators, and implementing procedures for their distribution, replacement, and revocation. It also includes changing default authenticators before first use, periodically refreshing authenticators, and protecting their content from unauthorized disclosure or modification. The control applies to a range of authenticators, including passwords, cryptographic devices, biometrics, certificates, and one-time password devices.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. Despite its implementation, there is a risk that users may create weak or easily guessable passwords. Although the control mandates minimum password complexity, the potential for users to bypass these requirements or choose weak passwords remains a concern.

Assessment Status: Implemented

Associated Risk: The risk associated with this control arises from the possibility that users could create weak or easily guessable passwords, which could significantly increase the likelihood of unauthorized access to systems. If exploited, this vulnerability could lead to severe security incidents, such as data breaches or system compromises. The likelihood of such incidents is moderate, given the existing controls, but the impact could be severe. To mitigate this risk, it is essential to enforce stringent password complexity requirements and ensure regular password updates. Additionally, user training on secure password practices could further reduce the chances of passwords being compromised, thereby enhancing overall system security.

### Control Identifier: SC-15

Control Description: Collaborative Computing Devices and Applications. This control requires the prohibition of remote activation of collaborative computing devices and applications, except in organization-defined situations where it is explicitly allowed. Additionally, the control mandates providing clear indications to users when these devices and applications are in use. Collaborative computing devices include remote meeting tools, networked whiteboards, cameras, and microphones. The goal is to prevent unauthorized or unnoticed activation that could lead to unauthorized monitoring or recording.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there remains a risk of unauthorized monitoring or recording if these collaborative computing devices are remotely activated without the user's awareness. Even though the control is implemented, the potential for devices to be activated remotely by malicious actors poses a significant security concern.

Assessment Status: Implemented

Associated Risk: The risk associated with this control arises from the possibility that collaborative computing devices could be remotely activated without the user's knowledge, leading to unauthorized monitoring or recording of sensitive information. This could result in data loss or information disclosure incidents. The likelihood of such an event is moderate, given the existing control measures, but the impact could be severe, particularly if sensitive discussions or activities are recorded without authorization. To mitigate this risk, it is crucial to strictly enforce the prohibition on remote activation and ensure that all users are explicitly notified whenever these devices are in use, thereby reducing the likelihood of unauthorized surveillance and protecting the organization's sensitive information.

### Control Identifier: CA-5

Control Description: Plan of Action and Milestones (POAM). This control involves developing a plan of action and milestones for the system to document the organization's planned remediation actions. These actions aim to correct weaknesses or deficiencies identified during control assessments and to reduce or eliminate known vulnerabilities in the system. Additionally, the control requires that the POAM be regularly updated based on findings from control assessments, independent audits, and continuous monitoring activities. The POAM is essential for tracking and prioritizing remedial actions to ensure that security deficiencies are addressed in a timely manner.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, unresolved vulnerabilities and deficiencies remain in the system, indicating that while the POAM exists, it may not be fully effective in addressing all identified issues. The control's implementation appears to be functioning, but gaps in the timely remediation of identified weaknesses are a concern.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that the organization may fail to effectively address security deficiencies and vulnerabilities, leading to prolonged exposure to threats. If unresolved vulnerabilities persist, they could be exploited by attackers, resulting in significant security incidents, such as data breaches, information disclosure, and operational disruptions. The likelihood of such incidents increases with delays in remediation, making it critical to ensure that the POAM is not only maintained but also actively followed and updated. This would reduce the likelihood of prolonged exposure to threats and mitigate the impact of potential security breaches.

### Control Identifier: CA-7

Control Description: Continuous Monitoring. This control requires the development and implementation of a system-level continuous monitoring strategy that aligns with the organization's overall continuous monitoring approach. The strategy includes establishing specific system-level metrics to monitor, determining monitoring frequencies, and conducting ongoing control assessments. The control also involves analyzing the information generated from these assessments, taking appropriate response actions, and reporting the security and privacy status of the system regularly to designated personnel.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a potential risk of security controls becoming outdated or ineffective over time. While the control is implemented, the effectiveness of continuous monitoring activities may diminish if not properly maintained, particularly in dynamic environments where threats and vulnerabilities are constantly evolving.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that security controls may become outdated or ineffective, increasing the system's vulnerability to attacks. If continuous monitoring is not adequately performed, the organization may fail to detect and respond to changes in the environment, leading to security controls that no longer provide the necessary protection. The likelihood of such incidents increases without consistent and thorough monitoring, and the impact could be severe, including damage to or destruction of critical assets. Implementing this control effectively mitigates the risk by ensuring that security controls are continuously evaluated and adjusted as needed, enabling proactive management of security threats and reducing the chances of security breaches.

### Control Identifier: SC-7(3)

Control Description: Boundary Protection | Access Points. This control requires limiting the number of external network connections to the system. By reducing the number of external access points, the organization can better monitor inbound and outbound communications traffic, thereby enhancing the security of the system. This approach is particularly important during periods of technological transition, such as moving from older to newer network protocols, which may temporarily increase the number of access points.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there remains a risk associated with external attackers gaining access to internal networks through publicly accessible systems. Although the control limits the number of external connections, the presence of publicly accessible components could still serve as potential entry points for attackers.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that publicly accessible systems could be exploited by attackers to gain unauthorized access to internal networks. This could lead to serious security incidents, including data breaches and unauthorized access to sensitive information. The likelihood of such incidents is moderate, but the impact could be severe if attackers manage to use compromised public-facing systems to move laterally into more secure internal networks. To mitigate this risk, it is crucial to ensure that public-facing components are isolated in separate subnetworks (e.g., DMZs) and that strict monitoring and control measures are in place to prevent lateral movement from these systems to internal networks. This reduces both the likelihood and impact of potential security breaches.

### Control Identifier: IA-2(1)

Control Description: Identification and Authentication (Organizational Users) | Multi-factor Authentication to Privileged Accounts. This control mandates the implementation of multi-factor authentication (MFA) for access to privileged accounts. MFA requires the use of two or more different factors to achieve authentication, such as something you know (e.g., a PIN), something you have (e.g., a physical authenticator), or something you are (e.g., a biometric). This control is designed to enhance the security of privileged accounts by requiring multiple forms of verification before granting access, thus reducing the likelihood of unauthorized access.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a significant risk associated with unauthorized access to both privileged and non-privileged accounts. Although the control is implemented, the organization remains vulnerable if multi-factor authentication is not consistently applied across all access points.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that the organization is highly vulnerable to unauthorized access if MFA is not rigorously enforced. Without MFA, an attacker who compromises a password could easily gain access to sensitive systems, including both privileged and non-privileged accounts. This could lead to severe security incidents, such as data breaches, system compromises, and unauthorized modifications. The likelihood of such incidents is moderate to high, particularly if MFA is not consistently applied, but the impact could be catastrophic. Implementing and strictly enforcing MFA across all privileged accounts significantly mitigates this risk by adding an additional layer of security, making unauthorized access more difficult and reducing the overall risk to the organization's systems and data.

### Control Identifier: IA-2(1)

Control Description: Identification and Authentication (Organizational Users) | Multi-factor Authentication to Privileged Accounts. This control mandates the implementation of multi-factor authentication (MFA) for access to privileged accounts. MFA requires the use of two or more different factors to achieve authentication, such as something you know (e.g., a PIN), something you have (e.g., a physical authenticator), or something you are (e.g., a biometric). This control is designed to enhance the security of privileged accounts by requiring multiple forms of verification before granting access, thus reducing the likelihood of unauthorized access.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a significant risk associated with unauthorized access to both privileged and non-privileged accounts. Although the control is implemented, the organization remains vulnerable if multi-factor authentication is not consistently applied across all access points.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that the organization is highly vulnerable to unauthorized access if MFA is not rigorously enforced. Without MFA, an attacker who compromises a password could easily gain access to sensitive systems, including both privileged and non-privileged accounts. This could lead to severe security incidents, such as data breaches, system compromises, and unauthorized modifications. The likelihood of such incidents is moderate to high, particularly if MFA is not consistently applied, but the impact could be catastrophic. Implementing and strictly enforcing MFA across all privileged accounts significantly mitigates this risk by adding an additional layer of security, making unauthorized access more difficult and reducing the overall risk to the organization's systems and data.

### Control Identifier: IA-1

Control Description: Policy and Procedures. This control requires the development, documentation, and dissemination of identification and authentication (IA) policies and procedures at the organization, mission/business process, or system level. The IA policy must address the purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance. It must also be consistent with applicable laws, directives, regulations, and standards. Procedures should be established to facilitate the implementation of the IA policy and controls, and regular updates to these policies and procedures should be conducted based on organizational needs and external factors such as audit findings or changes in regulations.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there remains a significant risk associated with unauthorized access to systems and data. The IA policy and procedures, while implemented, must be continuously reviewed and enforced to ensure that all users, processes, and devices are properly identified and authenticated before access is granted.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that unauthorized users, processes, or devices may gain access to the organization's systems if the IA policies and procedures are not adequately enforced or updated. This could lead to significant security incidents, including data breaches, system compromises, and a loss of trust in the organization's ability to protect its information. The likelihood of such incidents is moderate to high, especially if policies are outdated or not consistently applied. The impact could be severe, resulting in loss of sensitive data and reputational damage. Implementing and rigorously enforcing IA policies and procedures mitigates this risk by ensuring that all access points are secure, and that only authenticated and authorized entities can interact with the organization's systems and data, thereby reducing the likelihood and impact of unauthorized access.

### Control Identifier: SC-13

Control Description: Cryptographic Protection. This control requires the organization to determine its specific cryptographic needs and implement the appropriate types of cryptography to support those needs. Cryptography is employed to secure various types of information, including classified and controlled unclassified information (CUI), support digital signatures, and enforce information separation. The use of cryptography must align with applicable standards such as FIPS-validated cryptography and NSA-approved cryptography, depending on the sensitivity of the information being protected.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a significant risk of unauthorized access to CUI during transmission. While cryptographic mechanisms are implemented, the potential for CUI to be intercepted and accessed without authorization remains a concern, particularly if encryption standards or practices are not uniformly enforced.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that CUI could be intercepted during transmission, leading to unauthorized access and potential security incidents. If cryptographic protection is not consistently applied or is weakened, attackers could exploit this vulnerability to gain access to sensitive information. The likelihood of such incidents is moderate to high, particularly in the absence of robust encryption practices, but the impact could be severe, leading to breaches of confidentiality and potential legal and reputational consequences. Implementing strong cryptographic mechanisms and ensuring they are applied consistently across all transmissions mitigates this risk by encrypting CUI, thus protecting its confidentiality and reducing the likelihood and impact of potential breaches.

### Control Identifier: SC-7

Control Description: Boundary Protection. This control requires the monitoring and control of communications at external managed interfaces to the system as well as key internal managed interfaces within the system. It includes the implementation of subnetworks (such as demilitarized zones, or DMZs) for publicly accessible system components that are physically or logically separated from internal organizational networks. Additionally, connections to external networks or systems are only allowed through managed interfaces consisting of boundary protection devices, such as gateways, routers, firewalls, and other security devices, aligned with the organization’s security and privacy architecture.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a significant risk of unauthorized access to or tampering with communications at critical system boundaries. While boundary protection mechanisms are implemented, the potential for sensitive information transmitted across these boundaries to be intercepted, modified, or compromised by unauthorized parties remains a concern.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that sensitive information transmitted across system boundaries could be intercepted, modified, or otherwise compromised by unauthorized parties. This could lead to serious security incidents, including data breaches and loss of system integrity. The likelihood of such incidents is moderate to high, particularly if boundary protection measures are not consistently monitored or updated to address evolving threats. The impact could be severe, resulting in unauthorized access to sensitive data and potential system compromises. Implementing and maintaining robust boundary protection controls mitigates this risk by ensuring that all communications at key system boundaries are monitored, controlled, and protected, thereby reducing both the likelihood and impact of potential security breaches.

### Control Identifier: MP-5(4)

Control Description: Media Transport | Cryptographic Protection. This control, although withdrawn and incorporated into SC-28(1), originally required the implementation of cryptographic mechanisms to protect controlled unclassified information (CUI) during transport on digital media. The use of cryptography ensured that even if the media was intercepted or accessed during transit, the information remained secure and confidential.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a significant risk of unauthorized access to CUI during transport. Although cryptographic protection is applied, the potential for CUI on digital media to be exposed during transport remains a concern, especially if encryption practices are not consistently enforced or if alternative physical safeguards are not implemented when cryptographic protection is not feasible.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that CUI on digital media could be exposed during transport, leading to unauthorized access and potentially severe security incidents. The likelihood of such incidents is moderate, particularly if cryptographic protection is not applied consistently or if physical safeguards are not in place when encryption is not feasible. The impact could be significant, resulting in the loss of sensitive information and potential legal and reputational consequences. Implementing strong cryptographic mechanisms mitigates this risk by ensuring that the information remains secure during transit, and where cryptographic protection is not possible, alternative physical safeguards must be employed to protect the media.

### Control Identifier: MA-4

Control Description: Nonlocal Maintenance. This control requires the organization to approve and monitor nonlocal maintenance and diagnostic activities. It mandates the use of nonlocal maintenance tools only when consistent with organizational policy and documented in the system's security plan. The control also requires strong authentication methods for establishing nonlocal maintenance sessions, maintaining records of these activities, and ensuring that all sessions and network connections are securely terminated once maintenance is completed. Strong authentication methods include techniques resistant to replay attacks, such as multi-factor authentication (MFA) and Public Key Infrastructure (PKI) with tokens.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a significant risk of unauthorized access during remote maintenance sessions. While the control is implemented, the absence of consistent multi-factor authentication increases the likelihood of unauthorized access, and improper termination of sessions can leave systems vulnerable to continued attacks.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that remote maintenance sessions could be accessed by unauthorized individuals, potentially leading to significant security incidents. The likelihood of such incidents is moderate to high, particularly if MFA is not enforced, and if sessions are not properly terminated. The impact could be severe, including unauthorized access to sensitive systems and data, leading to system compromises and data breaches. Implementing and strictly enforcing MFA for remote maintenance sessions and ensuring that all sessions are securely terminated after use mitigates this risk by reducing the likelihood of unauthorized access and protecting the organization's systems from potential security breaches.

### Control Identifier: AC-4

Control Description: Information Flow Enforcement. This control requires the enforcement of approved authorizations to control the flow of information within a system and between connected systems, based on organization-defined information flow control policies. Information flow control regulates the paths that information can take within and between systems, without regard to who is accessing the information. The goal is to prevent unauthorized transfers of information, such as ensuring that Controlled Unclassified Information (CUI) does not flow to unauthorized destinations or that external traffic claiming to be from within the organization is blocked.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a significant risk related to the unauthorized transfer of sensitive information, including CUI. While the control is implemented, the current mechanisms may not fully prevent data from being improperly transferred between different parts of a system or between systems, which can lead to potential data leaks or breaches.

Assessment Status: Implemented

Associated Risk: The primary risk associated with this control is that sensitive information, such as CUI, could flow freely within or between systems and potentially be transmitted to unauthorized entities or systems. The lack of rigorous enforcement of information flow policies heightens the risk of data leaks, breaches, and non-compliance with regulatory requirements. This could result in significant legal, operational, and reputational damage to the organization. The likelihood of such incidents is moderate, particularly if enforcement mechanisms are not robust or consistently applied. The impact could be severe, including loss of sensitive information, regulatory penalties, and damage to the organization's reputation. Implementing stronger enforcement of information flow policies mitigates this risk by ensuring that information is only transferred in accordance with approved policies, thereby reducing the likelihood and impact of potential security incidents.

### Control Identifier: PS-3

Control Description: Personnel Screening. This control requires that individuals be screened before being authorized to access the system. It also mandates that individuals be rescreened based on organization-defined conditions and at a frequency determined by the organization. Personnel screening and rescreening activities are designed to reflect applicable laws, regulations, policies, and specific criteria established for the risk designations of assigned positions. Screening typically includes background investigations and agency checks, ensuring that individuals with access to sensitive systems and information are trustworthy.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a significant risk associated with the potential for insider threats. While the control is implemented, if personnel are not properly vetted or rescreened, there is an increased likelihood that individuals with malicious intent could gain access to systems containing Controlled Unclassified Information (CUI).

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that individuals who have not been properly vetted may be granted access to systems containing CUI, leading to an increased likelihood of insider threats and significant security incidents. The likelihood of such incidents is moderate to high, particularly if screening processes are not rigorous or if rescreening is not conducted at appropriate intervals. The impact could be severe, including unauthorized access to sensitive information, data breaches, and potential operational disruptions. Implementing thorough and consistent personnel screening and rescreening processes mitigates this risk by ensuring that only trustworthy individuals are authorized to access sensitive information, thereby reducing the likelihood and impact of potential insider threats.

### Control Identifier: MP-4

Control Description: Media Storage. This control mandates the physical control and secure storage of both digital and non-digital media within organization-defined controlled areas. It also requires that system media be protected until it is either destroyed or sanitized using approved equipment, techniques, and procedures. The types of media covered by this control include flash drives, external hard drives, magnetic tapes, paper documents, and more. Secure storage can involve locked drawers, cabinets, or controlled media libraries, with the level of control being commensurate with the security classification of the information on the media.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a significant risk of unauthorized access, theft, or loss of Controlled Unclassified Information (CUI) on system media. While secure storage mechanisms are implemented, there remains a concern that CUI on system media may still be exposed to unauthorized individuals if these mechanisms are not consistently applied or if physical controls are inadequate.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that CUI on system media could be exposed to unauthorized individuals, leading to serious security incidents, such as data breaches and loss of sensitive information. The likelihood of such incidents is moderate, especially if physical controls and secure storage practices are not rigorously enforced. The impact could be severe, including unauthorized access and disclosure of sensitive information, which could have legal, operational, and reputational consequences for the organization. Implementing this control mitigates the risk by ensuring that all media containing CUI is securely stored and physically controlled, thereby reducing the likelihood of unauthorized access and minimizing the potential impact of such incidents.

### Control Identifier: AC-17(2)

Control Description: Remote Access | Protection of Confidentiality and Integrity Using Encryption. This control requires the implementation of cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions. This can be achieved using virtual private networks (VPNs) or cryptographic protocols like Transport Layer Security (TLS), which provide end-to-end security for communications over networks, ensuring that sensitive data transmitted during remote access sessions remains confidential and unaltered.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a significant risk of interception and unauthorized access to sensitive data during remote access sessions. While cryptographic mechanisms are implemented, the potential for remote access sessions to be intercepted and compromised by attackers remains a concern, especially if encryption is not consistently applied or if weaker encryption methods are used.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that remote access sessions could be intercepted and compromised by attackers. Without strong encryption, sensitive data transmitted during these sessions is vulnerable to unauthorized access, leading to potential data breaches, loss of data integrity, and overall system compromise. The likelihood of such incidents is moderate, particularly if encryption practices are not uniformly enforced or updated to counter evolving threats. The impact could be severe, resulting in operational disruptions, financial loss, legal penalties, and significant damage to the organization's reputation. Implementing and maintaining strong encryption protocols, such as TLS or VPNs, mitigates this risk by ensuring that all remote access sessions are securely protected, thereby reducing the likelihood and impact of potential security breaches.

### Control Identifier: SI-3

Control Description: Malicious Code Protection. This control requires the implementation of signature-based and/or non-signature-based malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code. It also mandates automatic updates to these protection mechanisms as new releases become available, in accordance with organizational configuration management policies. The control further requires periodic system scans and real-time scans of files from external sources, as well as appropriate actions (e.g., blocking or quarantining malicious code) in response to detections.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a significant risk of malware infections that could compromise the integrity, confidentiality, and availability of organizational systems and data. While malicious code protection mechanisms are implemented, there remains a concern that organizational systems could still be vulnerable to sophisticated or emerging types of malware, particularly if these mechanisms are not consistently updated or if false positives are not adequately addressed.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that organizational systems could become infected with malware, leading to serious security incidents. Malicious code can compromise system integrity, confidentiality, and availability, leading to unauthorized access, data corruption, data breaches, and significant operational disruptions. The likelihood of such incidents is moderate to high, especially if malicious code protection mechanisms are not consistently updated or are ineffective against certain types of malware. The impact could be severe, resulting in data modification, destruction, corruption, and operational downtime. Implementing and regularly updating malicious code protection mechanisms mitigates this risk by ensuring that designated locations within the system are protected against malicious code, thereby reducing both the likelihood and impact of malware-related security breaches.

### Control Identifier: SI-3(1)

Control Description: Malicious Code Protection | Central Management. This control was withdrawn and incorporated into PL-9. The original intent of this control was to ensure that malicious code protection mechanisms were centrally managed to provide consistent protection across all organizational systems. Central management of these mechanisms ensures that updates, scans, and responses to detected malware are uniform and effective across the entire organization.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there remains a significant risk of malware infections that go undetected. While central management mechanisms are implemented, the potential for malicious code to infiltrate the organization’s systems unnoticed is a concern, especially if scanning and detection methods are not consistently applied or if updates are not timely.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that malicious code could infiltrate the organization's systems unnoticed, leading to serious security incidents. This could result in data modification, destruction, or corruption, potentially causing significant operational disruptions and data breaches. The likelihood of such incidents is moderate, particularly if malware detection and response mechanisms are not centrally managed or are inconsistently applied. The impact could be severe, with potential for data loss, system downtime, and compromise of sensitive information. Implementing and maintaining central management of malware protection mitigates this risk by ensuring that all systems are regularly scanned for malware and that files from external sources are checked in real-time, reducing both the likelihood and impact of malware infections.

### Control Identifier: MP-5

Control Description: Media Transport. This control requires the protection and control of system media during transport outside of controlled areas using organization-defined controls. It mandates maintaining accountability for system media during transport, documenting associated activities, and restricting transport activities to authorized personnel. System media includes both digital (e.g., flash drives, CDs, hard drives) and non-digital media (e.g., paper, microfilm). Controlled areas are spaces where physical or procedural controls are in place to protect information and systems. Protective measures for media during transport may include cryptographic protections and the use of locked containers to prevent unauthorized access.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a significant risk of unauthorized access to Controlled Unclassified Information (CUI) on system media during transport. While controls are implemented, the potential for CUI to be accessed or distributed by unauthorized individuals during transport remains a concern, especially if accountability measures are not strictly enforced.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that CUI on system media may be accessed by unauthorized individuals during transport, leading to significant security incidents, including data breaches and unauthorized distribution of sensitive information. The likelihood of such incidents is moderate, particularly if controls during transport are not strictly applied or if transport activities are not adequately documented and monitored. The impact could be severe, resulting in unauthorized access to sensitive information, data leaks, and potential legal and reputational consequences for the organization. Implementing strong protective measures and maintaining strict accountability during media transport mitigates this risk by ensuring that only authorized users have access to CUI on system media, thereby reducing the likelihood of unauthorized access and minimizing the potential impact of such incidents.

### Control Identifier: MP-6

Control Description: Media Sanitization. This control requires the sanitization of organization-defined system media prior to disposal, release out of organizational control, or reuse, using organization-defined sanitization techniques and procedures. The sanitization process is designed to remove information from system media so that it cannot be retrieved or reconstructed. The strength and integrity of the sanitization mechanisms must be commensurate with the security category or classification of the information. This control applies to both digital and non-digital media, ensuring that sensitive information is not exposed when media is disposed of or reused.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is a significant risk of unauthorized access to Controlled Unclassified Information (CUI) through discarded or reused media. While media sanitization mechanisms are implemented, there remains a concern that CUI could be recovered from media that is improperly sanitized or destroyed, potentially leading to unauthorized disclosure of sensitive information.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that CUI could be recovered from media that is improperly sanitized or destroyed, leading to significant security incidents, including data breaches and unauthorized disclosure of sensitive information. The likelihood of such incidents is moderate, particularly if sanitization practices are not consistently applied or if weaker sanitization methods are used. The impact could be severe, resulting in unauthorized access to sensitive information, legal consequences, and damage to the organization's reputation. Implementing and enforcing thorough sanitization or destruction of media containing CUI before disposal or reuse mitigates this risk by reducing the likelihood of unauthorized access and minimizing the potential impact of such incidents.

### Control Identifier: MP-7

Control Description: Media Use. This control requires organizations to restrict or prohibit the use of specific types of system media on defined systems or system components, using designated controls. Additionally, it prohibits the use of portable storage devices in organizational systems if such devices have no identifiable owner. The control applies to both digital media (e.g., flash drives, CDs, removable hard drives) and non-digital media (e.g., paper, microfilm), as well as mobile devices with information storage capabilities. The purpose is to mitigate risks associated with unauthorized use, data breaches, and malware introduction via removable media.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there remains a significant risk that removable media could be used inappropriately, leading to data modification, destruction, corruption, unauthorized data transfer, malware introduction, or data loss. While the organization has implemented controls to restrict or prohibit the use of certain types of media, there is a concern that these controls may not be consistently applied or monitored across all systems.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that removable media could be used inappropriately, leading to significant security incidents such as data breaches, introduction of malware, or loss of sensitive information. The likelihood of such incidents is moderate, particularly if the use of removable media is not tightly controlled or if unauthorized devices are used. The impact could be severe, resulting in unauthorized access to sensitive information, system compromise, and operational disruptions. Implementing and enforcing strict controls on the use of removable media, including ensuring that only authorized and identifiable devices are used, mitigates this risk by reducing the likelihood of unauthorized access and the potential impact of such incidents.

### Control Identifier: SI-4

Control Description: System Monitoring. This control requires organizations to monitor their systems to detect attacks, potential indicators of attacks, and unauthorized connections. It includes identifying unauthorized use of the system through defined techniques, deploying monitoring devices strategically and ad hoc within the system, analyzing detected events, adjusting monitoring levels based on risk, obtaining legal opinions regarding monitoring activities, and providing monitoring information to designated personnel. The control supports continuous monitoring and incident response efforts, with monitoring activities guided by organizational objectives.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there remains a risk of undetected attacks or malicious activities due to potential gaps in monitoring coverage or inefficiencies in analyzing and responding to detected events. The organization has implemented various tools and techniques for system monitoring, including intrusion detection systems and network monitoring software. Still, the effectiveness of these measures depends on continuous evaluation and improvement to address emerging threats.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that attacks or malicious activities could go undetected, allowing them to escalate and cause significant harm. The primary threat is the unauthorized modification, destruction, or corruption of data, which could result in data breaches, loss of system integrity, and operational disruptions. The likelihood of such incidents is moderate, particularly if monitoring activities are not sufficiently comprehensive or responsive to changing threat landscapes. The impact could be severe, leading to substantial operational, financial, and reputational damage. Implementing this control mitigates the risk by ensuring that systems are continuously monitored, so potential threats are detected early and can be responded to promptly, reducing both the likelihood and impact of security incidents.

### Control Identifier: SI-4

Control Description: System Monitoring. This control requires organizations to monitor their systems to detect attacks, potential indicators of attacks, and unauthorized connections. It includes identifying unauthorized use of the system through defined techniques, deploying monitoring devices strategically and ad hoc within the system, analyzing detected events, adjusting monitoring levels based on risk, obtaining legal opinions regarding monitoring activities, and providing monitoring information to designated personnel. The control supports continuous monitoring and incident response efforts, with monitoring activities guided by organizational objectives.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there remains a risk of undetected attacks or malicious activities due to potential gaps in monitoring coverage or inefficiencies in analyzing and responding to detected events. The organization has implemented various tools and techniques for system monitoring, including intrusion detection systems and network monitoring software. Still, the effectiveness of these measures depends on continuous evaluation and improvement to address emerging threats.

Assessment Status: Implemented

Associated Risk: The risk associated with this control is that attacks or malicious activities could go undetected, allowing them to escalate and cause significant harm. The primary threat is the unauthorized modification, destruction, or corruption of data, which could result in data breaches, loss of system integrity, and operational disruptions. The likelihood of such incidents is moderate, particularly if monitoring activities are not sufficiently comprehensive or responsive to changing threat landscapes. The impact could be severe, leading to substantial operational, financial, and reputational damage. Implementing this control mitigates the risk by ensuring that systems are continuously monitored, so potential threats are detected early and can be responded to promptly, reducing both the likelihood and impact of security incidents.

### Control Identifier: AC-7

Control Description: Unsuccessful Logon Attempts. This control requires organizations to enforce a limit on the number of consecutive invalid logon attempts by a user during a defined time period. It includes actions that are automatically triggered when the maximum number of unsuccessful attempts is exceeded, such as locking the account or node, delaying the next logon prompt, notifying system administrators, or other organization-defined actions. The purpose of this control is to mitigate the risk of brute-force attacks by limiting the number of attempts a user can make to log in unsuccessfully, thus reducing the likelihood of unauthorized access.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, there is still a threat of brute-force attacks if the control is not properly configured or enforced. The organization has implemented measures to lock accounts or apply delay algorithms after a certain number of unsuccessful attempts, but the effectiveness of these measures depends on the strictness of the configurations and monitoring to ensure compliance.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing or improperly configuring AC-7 is the increased likelihood of successful brute-force attacks, where attackers continuously attempt to guess passwords. This can lead to unauthorized access to user accounts, resulting in data breaches, system compromise, and further exploitation of the organization's systems. The likelihood of such incidents is moderate, particularly if account lockout thresholds are too high or delay mechanisms are not stringent enough. The impact could be severe, including operational disruptions, financial loss, and damage to the organization’s reputation. Implementing this control mitigates the risk by ensuring that unsuccessful logon attempts are limited and appropriately responded to, thereby reducing both the likelihood and impact of brute-force attacks.

### Control Identifier: AC-6(9)

Control Description: Least Privilege | Log Use of Privileged Functions. This control requires organizations to log the execution of privileged functions. Privileged functions include critical system operations that, if misused, can lead to unauthorized system changes, data corruption, or security breaches. Logging these functions is essential to detect and analyze misuse, whether intentional or unintentional by authorized users or by unauthorized external entities who have compromised system accounts. This control is particularly important for mitigating risks from insider threats and advanced persistent threats (APTs).

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. However, it is crucial to ensure that logging is comprehensive and that logs are regularly reviewed to identify any potential misuse of privileged functions. Failure to do so could result in unauthorized access to and misuse of these functions, leading to significant security incidents.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing or inadequately managing AC-6(9) is that non-privileged users or unauthorized individuals could gain access to privileged functions. If such access goes undetected due to a lack of logging or analysis, it could lead to unauthorized system changes, data corruption, or security breaches. The likelihood of such incidents is moderate, particularly in environments where privileged functions are numerous or complex. The impact could be severe, including operational disruptions, financial loss, legal penalties, and damage to the organization’s reputation. Implementing this control mitigates the risk by ensuring that all privileged functions are logged and that logs are regularly reviewed, thereby reducing both the likelihood and impact of unauthorized access and misuse.

### Control Identifier: IA-2(8)

Control Description: Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant. This control requires the implementation of replay-resistant authentication mechanisms for accessing either privileged or non-privileged accounts. Replay-resistant authentication mechanisms are designed to prevent attackers from successfully using previously captured authentication messages to gain unauthorized access. These mechanisms typically involve the use of nonces, challenges, or time-synchronous cryptographic authenticators to ensure that each authentication attempt is unique and cannot be reused.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. The organization has implemented mechanisms to ensure that authentication data cannot be reused in replay attacks. This includes protocols and technologies that make it impractical to achieve successful authentication by replaying previously intercepted credentials.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing IA-2(8) is the increased vulnerability to replay attacks, where attackers intercept and reuse authentication credentials to gain unauthorized access to the network. If authentication processes are not resistant to replay attacks, the likelihood of unauthorized access to sensitive systems and data increases significantly. The potential impact includes severe security incidents such as data breaches, system compromise, and unauthorized access to critical organizational assets. Implementing replay-resistant authentication mechanisms mitigates this risk by ensuring that intercepted authentication data cannot be reused, thereby reducing the likelihood and impact of replay attacks on the organization's network.

### Control Identifier: MP-7(1)

Control Description: Media Use | Prohibit Use Without Owner. This control was withdrawn and incorporated into MP-7. It originally aimed to prohibit the use of portable storage devices that do not have an identifiable owner within the organization. The control was intended to ensure that only authorized and identified devices are used within the organization's systems, reducing the risks associated with the use of unidentified and potentially harmful portable storage devices.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. The organization has implemented measures to ensure that only portable storage devices with an identifiable owner are permitted for use. This helps prevent the introduction of malicious software, unauthorized access, or data breaches by restricting the use of unapproved devices.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing MP-7(1) is the increased likelihood of unidentified portable storage devices being used within the organization. Such devices could introduce malicious software, enable unauthorized access, or cause data breaches. Without proper controls, these incidents could lead to data corruption, loss, or unauthorized disclosure of sensitive information, potentially resulting in severe operational, financial, and reputational damage. Implementing this control mitigates the risk by ensuring that only portable storage devices with an identifiable owner are allowed, thereby reducing the likelihood and impact of unauthorized or malicious use of such devices.

### Control Identifier: MA-3(3)

Control Description: Maintenance Tools | Prevent Unauthorized Removal. This control requires the prevention of the removal of maintenance equipment that may contain organizational information by implementing one or more of the following actions:

Verifying that the equipment contains no organizational information before removal.

Sanitizing or destroying the equipment.

Retaining the equipment within the facility.

Obtaining explicit authorization from designated personnel to remove the equipment from the facility.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. The organization has established protocols to ensure that maintenance tools and equipment containing organizational information are not removed without proper verification or sanitization. This reduces the risk of unauthorized information leakage or potential security threats.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing MA-3(3) is the potential introduction of malicious code into the organization's systems via uninspected diagnostic or test media. Without this control, there is a heightened risk that malicious code could be inadvertently introduced, leading to data modification, destruction, or corruption. This can result in severe security incidents, including system compromise and data breaches. Implementing this control mitigates the risk by ensuring that all maintenance media and equipment are thoroughly scanned and sanitized before being used or removed, thereby protecting the organization’s systems from potential malware and other security threats.

### Control Identifier: SC-4

Control Description: Information in Shared System Resources. This control requires the prevention of unauthorized and unintended information transfer via shared system resources. The objective is to ensure that information produced by the actions of prior users or roles (or processes acting on behalf of prior users or roles) is not made available to current users or roles (or processes acting on behalf of current users or roles) that gain access to shared system resources after those resources have been released back to the system.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. The organization has implemented mechanisms to prevent unauthorized access to sensitive information due to improper handling of shared resources. These measures ensure that shared system resources are securely managed and that data is not inadvertently transferred between users or processes.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing SC-4 is unauthorized access to sensitive information due to improper handling of shared system resources. Without this control, data could be inadvertently transferred between users or processes, leading to unauthorized access and data breaches. This can result in severe security incidents, including exposure of confidential information and potential regulatory non-compliance. Implementing this control mitigates the risk by ensuring that shared resources are managed properly so that only authorized processes can access the data intended for them, thereby reducing both the likelihood and impact of potential security incidents.

### Control Identifier: CM-7(5)

Control Description: Least Functionality | Authorized Software — Allow-by-exception. This control involves identifying organization-defined software programs authorized to execute on the system and implementing a deny-all, permit-by-exception policy to ensure that only these authorized programs are allowed to run. The organization should review and update the list of authorized software programs at a frequency defined by the organization.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. The organization has effectively implemented a policy that restricts software execution to only those programs that have been explicitly authorized. This helps to prevent unauthorized or malicious software from being executed on organizational systems.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing CM-7(5) is the unauthorized or malicious software being executed on organizational systems. Without this control, unauthorized or harmful software could be installed and executed, leading to significant security incidents such as malware infections, data breaches, and system compromises. Implementing a deny-by-exception or a deny-all, permit-by-exception policy mitigates this risk by preventing unauthorized software from running, thus reducing the likelihood of security breaches and limiting the potential impact of any unauthorized software that might otherwise be introduced into the environment.

### Control Identifier: RA-3

Control Description: Risk Assessment | Conduct a risk assessment, including identifying threats to and vulnerabilities in the system, determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information, and determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. The organization has implemented a risk assessment process that identifies threats and vulnerabilities, evaluates the likelihood and impact of these risks, and documents the results. This process is integrated into the overall risk management strategy and is reviewed and updated regularly as required.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing RA-3 is the possibility of unaddressed vulnerabilities and threats to organizational systems and CUI. If the organization fails to conduct thorough and regular risk assessments, critical vulnerabilities and threats may go unidentified and unmanaged, leading to significant security incidents. Regular risk assessments help the organization stay ahead of potential risks, enabling proactive management and mitigation. Implementing this control mitigates the risk by ensuring that the organization continually evaluates and responds to changes in the risk environment, thereby reducing the likelihood and impact of security breaches.

### Control Identifier: CM-3

Control Description: Configuration Change Control | Determine and document the types of changes to the system that are configuration-controlled. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses. Document configuration change decisions associated with the system, implement approved configuration-controlled changes, retain records of configuration-controlled changes, monitor and review activities associated with these changes, and coordinate and provide oversight for configuration change control activities through an organization-defined configuration change control element.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. The organization has implemented a formal configuration change control process that includes systematic proposal, justification, implementation, testing, review, and disposition of system changes. Configuration Control Boards (CCBs) are utilized to review and approve proposed changes, ensuring that all changes are properly documented and that security and privacy impacts are considered.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing CM-3 is the introduction of unauthorized, unapproved, or poorly managed changes to organizational systems. Without proper change control, the organization is exposed to significant security and operational risks. Unauthorized or poorly documented changes can introduce vulnerabilities, destabilize systems, and lead to data breaches or compliance failures. This control mitigates the risk by ensuring that all changes are tracked, approved, and implemented in a controlled manner, reducing the likelihood of unauthorized changes and their potential impact on the organization’s operations and assets.

### Control Identifier: PL-2

Control Description: System Security and Privacy Plans | Develop security and privacy plans for the system that:

Are consistent with the organization’s enterprise architecture;

Explicitly define the constituent system components;

Describe the operational context of the system in terms of mission and business processes;

Identify the individuals that fulfill system roles and responsibilities;

Identify the information types processed, stored, and transmitted by the system;

Provide the security categorization of the system, including supporting rationale;

Describe any specific threats to the system that are of concern to the organization;

Provide the results of a privacy risk assessment for systems processing personally identifiable information;

Describe the operational environment for the system and any dependencies on or connections to other systems or system components;

Provide an overview of the security and privacy requirements for the system;

Identify any relevant control baselines or overlays, if applicable;

Describe the controls in place or planned for meeting the security and privacy requirements, including a rationale for any tailoring decisions;

Include risk determinations for security and privacy architecture and design decisions;

Include security- and privacy-related activities affecting the system that require planning and coordination with organization-defined individuals or groups;

Are reviewed and approved by the authorizing official or designated representative prior to plan implementation.

The plan must be distributed, reviewed, updated, and protected from unauthorized disclosure or modification as outlined in the control requirements.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. The organization has developed comprehensive security and privacy plans that align with the organization’s enterprise architecture and operational context. These plans are reviewed regularly, updated to reflect any changes in the system environment, and are protected from unauthorized access. The organization’s security and privacy postures are clearly defined and understood across relevant stakeholders.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing PL-2 is the lack of a clear or outdated understanding of the organization's security posture. Without well-documented and current security and privacy plans, the organization may fail to accurately identify its system boundaries, security control implementations, and potential vulnerabilities. This could lead to significant security incidents, non-compliance with regulatory requirements, and overall operational risk. Implementing this control mitigates these risks by ensuring that the organization maintains up-to-date, well-structured security and privacy plans that are consistent with its operational and security objectives, thereby reducing the likelihood and impact of security breaches and policy violations.

### Control Identifier: AU-9

Control Description:

a. Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

b. Alert organization-defined personnel or roles upon detection of unauthorized access, modification, or deletion of audit information.

Audit information includes all information needed to successfully audit system activity, such as audit records, audit log settings, audit reports, and personally identifiable information. Audit logging tools are those programs and devices used to conduct system audit and logging activities. Protection of audit information focuses on technical protection and limits the ability to access and execute audit logging tools to authorized individuals. Physical protection of audit information is addressed by both media protection controls and physical and environmental protection controls.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. Audit logs and tools are adequately protected against unauthorized access, tampering, or deletion. Specific alerts are configured to notify designated personnel upon detection of unauthorized activities related to audit information. The implementation ensures the integrity and reliability of audit records, supporting effective incident detection and response.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing AU-9 is that audit logs and tools may be vulnerable to unauthorized access, tampering, or deletion. This vulnerability could enable attackers to conceal their activities, leading to undetected breaches, incomplete investigations, and a significant loss of accountability. Properly securing audit information and tools is crucial to maintain the integrity of audit records, ensuring they are reliable for detecting and responding to security incidents. This control mitigates these risks by ensuring that audit information and tools are protected and that any unauthorized access is promptly detected and addressed, reducing the likelihood and impact of such incidents.

### Control Identifier: SI-4(4)

Control Description:

(a) Determine criteria for unusual or unauthorized activities or conditions for inbound and outbound communications traffic;

(b) Monitor inbound and outbound communications traffic [Assignment: organization-defined frequency] for [Assignment: organization-defined unusual or unauthorized activities or conditions].

Unusual or unauthorized activities or conditions related to system inbound and outbound communications traffic include internal traffic that indicates the presence of malicious code or unauthorized use of legitimate code or credentials within organizational systems or propagating among system components, signaling to external systems, and the unauthorized exporting of information. Evidence of malicious code or unauthorized use of legitimate code or credentials is used to identify potentially compromised systems or system components.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. Criteria for unusual or unauthorized activities have been determined and are actively monitored within the organization’s inbound and outbound communications traffic. The monitoring helps to identify and respond to potential security incidents quickly, ensuring that unauthorized activities are promptly detected.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing SI-4(4) is that unauthorized access or misuse of systems could go undetected, leading to serious security incidents. Unauthorized activities, if left unnoticed, can escalate into major security breaches, resulting in data loss, unauthorized data transfers, or system compromise. Implementing this control mitigates the risk by ensuring continuous monitoring and detection of unusual or unauthorized communications traffic, thereby reducing both the likelihood and impact of security breaches.

### Control Identifier: AU-3

Control Description:

Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

Audit record content that may be necessary to support the auditing function includes event descriptions (item a), time stamps (item b), source and destination addresses (item c), user or process identifiers (items d and f), success or fail indications (item e), and filenames involved (items a, c, e, and f). Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred. Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. The audit records have been configured to capture all necessary information to establish the type, time, location, source, and outcome of events, as well as the identities of associated individuals or entities. This information is critical for ensuring that all user actions can be traced and accounted for, supporting the organization's auditing and incident response functions.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing AU-3 (Content of Audit Records) is a lack of user accountability, which can lead to difficulty in investigating and resolving security incidents. Without detailed audit records, the organization may struggle to hold users accountable for their actions, leading to unaddressed breaches, legal and regulatory issues, and a failure to enforce security policies. Implementing this control mitigates the risk by ensuring that all user actions are traceable, supporting accountability and effective incident response.

### Control Identifier: AC-17(3)

Control Description:

Route remote accesses through authorized and managed network access control points.

Organizations consider the Trusted Internet Connections (TIC) initiative DHS TIC requirements for external network connections since limiting the number of access control points for remote access reduces attack surfaces.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. Remote access is routed through authorized and managed network access control points, ensuring that all remote connections are monitored and controlled, which helps in mitigating unauthorized access attempts. By doing so, the organization has reduced the potential attack surface that could be exploited by external threats.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing AC-17(3) (Remote Access | Managed Access Control Points) is unauthorized remote access to the organization's systems. Remote access could occur through unmonitored and unsecured entry points, making it easier for attackers to gain unauthorized access. This can lead to data breaches, unauthorized system changes, and potentially catastrophic system compromises. Such incidents could result in significant operational disruptions, financial losses, and reputational damage, as well as increased vulnerability to further attacks.

### Control Identifier: SC-10

Control Description:

Terminate the network connection associated with a communications session at the end of the session or after [Assignment: organization-defined time period] of inactivity.

Network disconnect applies to internal and external networks. Terminating network connections associated with specific communications sessions includes de-allocating TCP/IP address or port pairs at the operating system level and de-allocating the networking assignments at the application level if multiple application sessions are using a single operating system-level network connection. Periods of inactivity may be established by organizations and include time periods by type of network access or for specific network accesses.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. The network connections associated with communications sessions are terminated at the end of the session or after a defined period of inactivity. This reduces the risk of unauthorized access by ensuring that inactive or forgotten sessions do not remain open, which could otherwise be exploited by malicious actors.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing SC-10 (Network Disconnect) is unauthorized access through inactive or forgotten sessions. If sessions remain active after the intended user has finished, they could be misused by unauthorized individuals, leading to data breaches or other forms of misuse. Implementing this control mitigates the risk by ensuring that all network connections are terminated when no longer needed, thereby reducing both the likelihood and impact of unauthorized access.

### Control Identifier: SC-28

Control Description:

Protect the [Selection (one or more): confidentiality; integrity] of the following information at rest: [Assignment: organization-defined information at rest].

Information at rest refers to the state of information when it is not in process or in transit and is located on system components. Such components include internal or external hard disk drives, storage area network devices, or databases. The focus of protecting information at rest is not on the type of storage device or frequency of access but rather on the state of the information. This control addresses the confidentiality and integrity of information, covering both user and system information. System-related information requiring protection includes configurations or rule sets for firewalls, intrusion detection and prevention systems, filtering routers, and authentication information. Organizations may employ different mechanisms to achieve confidentiality and integrity protections, including the use of cryptographic mechanisms and file share scanning.

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. Measures such as encryption, access controls, and other appropriate security mechanisms are implemented to protect Controlled Unclassified Information (CUI) at rest, ensuring its confidentiality and integrity.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing SC-28 (Protection of Information at Rest) is unauthorized access to or disclosure of CUI stored on organizational systems. If CUI at rest is not properly secured, unauthorized individuals could access or disclose sensitive information, leading to severe security incidents, including data breaches and compliance violations. Implementing this control mitigates the risk by ensuring that robust security measures, such as encryption and access controls, are in place to protect the confidentiality of CUI at rest, thereby reducing both the likelihood and impact of potential breaches.

### Control Identifier: CA-2

Control Description:

a. Select the appropriate assessor or assessment team for the type of assessment to be conducted;

b. Develop a control assessment plan that describes the scope of the assessment including:

Controls and control enhancements under assessment;

Assessment procedures to be used to determine control effectiveness; and

Assessment environment, assessment team, and assessment roles and responsibilities;

c. Ensure the control assessment plan is reviewed and approved by the authorizing official or designated representative prior to conducting the assessment;

d. Assess the controls in the system and its environment of operation [Assignment: organization-defined frequency] to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting established security and privacy requirements;

e. Produce a control assessment report that documents the results of the assessment; and

f. Provide the results of the control assessment to [Assignment: organization-defined individuals or roles].

Assessment Findings: The control is currently In Place within the JohnDoe&Co Information System. Assessments are conducted regularly to ensure that security controls are functioning as intended, weaknesses are identified, and improvements are made where necessary. The results of these assessments are documented and provided to the relevant personnel for further action.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing CA-2 (Control Assessments) is the presence of undetected weaknesses or ineffective security controls. Without regular assessments, security controls may become ineffective over time, leading to undetected vulnerabilities and a false sense of security. This can result in significant security incidents, including data breaches and system compromises. Implementing this control mitigates the risk by ensuring that security controls are regularly assessed for their effectiveness, allowing the organization to address any weaknesses or gaps before they can be exploited, thereby reducing the likelihood and impact of security breaches.

### Control Identifier: PE-8(1)

Control Description:

Maintain and review visitor access records using [Assignment: organization-defined automated mechanisms].

Assessment Findings: Visitor access records are currently maintained and reviewed using automated mechanisms within the JohnDoe&Co Information System. These records are stored in a database management system that is accessible by organizational personnel, facilitating regular reviews to ensure that access authorizations are current and still required to support organizational mission and business functions.

Assessment Status: Implemented

Associated Risk: The primary risk associated with not implementing PE-8(1) (Visitor Access Records | Automated Records Maintenance and Review) is the possibility of unauthorized physical access going undetected. Without proper logging and review of visitor access, unauthorized physical access to the facility may go unnoticed or unresolved, leading to serious security incidents, including theft, tampering, or data breaches. Implementing this control mitigates the risk by ensuring that all physical access is logged and can be reviewed, supporting both real-time security monitoring and post-incident investigations. This helps in reducing the likelihood and impact of unauthorized physical access.

### Control Identifier: CM-4

Control Description:

The control requires the analysis of changes to the system to determine potential security and privacy impacts prior to change implementation. Organizational personnel with security or privacy responsibilities must conduct these impact analyses, ensuring that individuals performing the analyses possess the necessary skills and technical expertise. The process involves reviewing relevant documentation and operational procedures to understand control requirements and implementation, assessing the impact of changes on organizational supply chain partners, and determining how potential changes could create new risks or affect the ability of implemented controls to mitigate those risks.

Assessment Findings:

The assessment found that while the process for conducting impact analyses is in place and generally followed, there are weaknesses in consistently reviewing all relevant documentation prior to implementation. Some instances were noted where changes were made without a thorough assessment, leading to the introduction of security vulnerabilities. Additionally, communication with supply chain partners regarding the impact of changes was found to be inconsistent, potentially leaving gaps in the understanding of how changes might affect external stakeholders.

Assessment Status: Implemented

Associated Risk:

The risk associated with the identified findings includes the potential for unauthorized changes to systems that could introduce security vulnerabilities or other issues. Without proper and consistent impact analyses, the organization is at risk of creating new attack vectors or destabilizing the system, which could lead to severe consequences such as data breaches, operational disruptions, and non-compliance with regulatory requirements. The overall risk to the organization is assessed as high, given the potential for significant impact if these vulnerabilities are exploited.

### Control Identifier: CM-5

Control Description:

This control requires the organization to define, document, approve, and enforce physical and logical access restrictions associated with changes to the system. Changes to hardware, software, or firmware components, as well as operational procedures related to the system, can have significant effects on security and privacy. Therefore, only qualified and authorized individuals are permitted to access systems for the purpose of initiating changes. Access restrictions include a variety of measures such as physical and logical access controls, software libraries, workflow automation, and controlled change windows to ensure changes are only made during specified times.

Assessment Findings:

The assessment found that access restrictions for changes are generally well implemented, with documented procedures in place to ensure that only authorized personnel can make changes to the system. However, there were a few instances where the enforcement of these restrictions was not as stringent as required, leading to potential vulnerabilities. For example, access logs indicated that in some cases, changes were made outside of the defined change windows without proper authorization. This indicates a need for stronger enforcement of the existing policies and better monitoring of access control mechanisms.

Assessment Status: Implemented

Associated Risk:

The risk associated with unauthorized changes to systems includes the potential introduction of vulnerabilities, system instability, or even data breaches. Without proper access controls, unauthorized individuals could make changes that compromise the security and integrity of the system. The likelihood of this occurring, given the current control weaknesses, is moderate to high, with a potentially severe impact on the organization's security posture. Therefore, while the control is implemented, there is a significant risk that needs to be mitigated through enhanced enforcement and monitoring.

### Control Identifier: CM-5(1)

Control Description:

This control requires the organization to enforce access restrictions for system changes using automated mechanisms and to automatically generate audit records of enforcement actions. The purpose is to ensure that configuration change control is rigorously applied and that any unauthorized changes can be detected and addressed promptly. This involves logging system access associated with applying configuration changes to support after-the-fact investigations and to maintain system integrity.

Assessment Findings:

The assessment revealed that automated mechanisms for enforcing access restrictions and generating audit records are in place and generally functioning as intended. However, there were some issues with the completeness and accuracy of the audit logs, where not all enforcement actions were recorded. This could potentially allow unauthorized changes to go undetected. Additionally, some of the automated enforcement mechanisms were found to be outdated, lacking the ability to fully integrate with newer systems, which may limit their effectiveness.

Assessment Status: Implemented

Associated Risk:

Without fully effective automated mechanisms to enforce access restrictions for changes, there is a heightened risk of unauthorized or unapproved changes being made to critical systems. Such changes could introduce security vulnerabilities, disrupt operations, and lead to significant security incidents, including data breaches and loss of system integrity. The risk is further amplified by the potential gaps in audit records, which could hinder the ability to investigate and respond to unauthorized activities. The overall risk is assessed as high, with potential substantial financial and reputational damage due to non-compliance with industry regulations or standards.

### Control Identifier: AC-11

Control Description:

The control requires the prevention of further access to the system by initiating a device lock after a defined period of inactivity or by requiring the user to initiate a device lock before leaving the system unattended. The lock remains in place until the user reestablishes access using established identification and authentication procedures. Device locks are temporary measures to prevent unauthorized access to organizational systems during short periods of user absence, and they can be implemented at either the operating system or application level. User-initiated locks require physical action from users, and proximity locks can also be utilized.

Assessment Findings:

The assessment determined that device locks are generally implemented as required, with policies in place to ensure that systems are secured during periods of inactivity. However, it was noted that not all users consistently follow the procedure for initiating device locks, particularly when leaving workstations unattended for brief periods. In some cases, device locks were not triggered after the organization-defined inactivity period, leading to potential exposure of sensitive information. Additionally, proximity locks, while available, were not widely adopted across the organization, limiting their effectiveness.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate device locking includes the possibility of unauthorized individuals accessing and viewing sensitive information during periods of user inactivity. An unattended device becomes vulnerable to anyone nearby, increasing the chances of data breaches, unauthorized changes, and the exposure of confidential information. This risk is significant, with potential for considerable operational, financial, and reputational damage to the organization if not properly managed.

### Control Identifier: SI-5

Control Description:

This control requires the organization to receive system security alerts, advisories, and directives from defined external organizations on an ongoing basis. Additionally, the organization must generate internal security alerts, advisories, and directives as necessary and disseminate them to the appropriate personnel, organizational elements, or external entities. The control also mandates the implementation of security directives within established time frames or, if not possible, notifying the issuing organization of the degree of noncompliance. The purpose is to maintain situational awareness and ensure timely responses to potential threats and vulnerabilities.

Assessment Findings:

The assessment found that the organization has established procedures for receiving and disseminating security alerts, advisories, and directives. However, there were instances where critical alerts were not communicated promptly to all relevant stakeholders, leading to delays in addressing emerging threats. Furthermore, while the system for generating internal alerts is in place, it was underutilized, resulting in some internal security concerns not being escalated as quickly as they should have been.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with deficiencies in this control is that the organization may miss critical information about new threats and vulnerabilities, leading to delayed responses and increased exposure to security incidents. If security alerts are not adequately monitored and acted upon, the likelihood of a security breach increases, which could result in significant damage to the organization's operations, assets, and reputation. Effective implementation of this control is essential to reduce both the likelihood and impact of potential security incidents.

### Control Identifier: SC-23

Control Description:

This control requires the protection of the authenticity of communication sessions. The focus is on communications protection at the session level, ensuring that both parties in a communication session can have confidence in each other's identity and the validity of the transmitted information. The control aims to protect against session hijacking, man-in-the-middle attacks, and the insertion of false information into sessions, thereby maintaining the integrity and authenticity of communications.

Assessment Findings:

The assessment confirmed that measures to protect the authenticity of communication sessions are in place and actively monitored. However, there were some gaps in the implementation, particularly regarding the robustness of the defenses against advanced session hijacking techniques. While basic protections like encryption and session timeouts are enforced, some systems were found to be vulnerable to sophisticated man-in-the-middle attacks due to outdated cryptographic protocols still in use in certain legacy systems.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate session authenticity controls includes the potential for communication sessions to be intercepted or hijacked, leading to unauthorized access and serious security incidents. If session authenticity is compromised, data modification, destruction, or corruption could occur, undermining the integrity and confidentiality of the information exchanged. The likelihood of such attacks increases if vulnerabilities in the session protection mechanisms are not addressed, posing a significant risk to the organization's security posture.

### Control Identifier: AC-12

Control Description:

The control mandates the automatic termination of user sessions after organization-defined conditions or trigger events that require session disconnect. This control specifically addresses the termination of user-initiated logical sessions, which are distinct from network connections. Logical sessions include local, network, and remote access sessions, and they are initiated whenever a user or a process acting on behalf of a user accesses an organizational system. Terminating these sessions is crucial to ensuring that unauthorized access to active sessions does not occur, thereby protecting the integrity and confidentiality of sensitive information.

Assessment Findings:

The assessment determined that the automatic termination of user sessions is generally implemented across the organization, with predefined conditions such as periods of user inactivity and time-of-day restrictions. However, there were instances where session termination did not occur as expected, particularly in systems that were not updated with the latest security patches. In some cases, user sessions remained open beyond the defined inactivity period, increasing the risk of unauthorized access.

Assessment Status: Implemented

Associated Risk:

The risk associated with unattended or inactive user sessions that are not automatically terminated includes the possibility that unauthorized individuals could exploit these open sessions to access sensitive information or perform unauthorized actions. This risk is significant, as it increases the likelihood of data breaches, unauthorized system modifications, and other security incidents. The consequences could be severe, leading to significant operational, financial, and reputational damage to the organization if these vulnerabilities are not properly addressed.

### Control Identifier: SI-3(2)

Control Description:

This control has been withdrawn and incorporated into SI-3. However, the original intent of this control was to ensure that systems automatically receive updates for malicious code protection mechanisms, such as antivirus definitions, to protect against the latest threats. This is crucial for maintaining the effectiveness of security measures in defending against new and evolving malware.

Assessment Findings:

Despite the withdrawal of SI-3(2) as a standalone control, the assessment found that the organization continues to implement automatic updates as part of its broader malicious code protection strategy. This ensures that systems are protected against the latest malware threats. However, there were some delays noted in the deployment of updates across all systems, particularly in isolated networks, which could increase the risk of exposure to new malware variants.

Assessment Status: Implemented

Associated Risk:

The risk associated with delayed or incomplete updates to malicious code protection mechanisms includes increased exposure to new and evolving malware. If the organization's systems are not adequately protected with the latest updates, they may become vulnerable to attacks that could result in data modification, destruction, or corruption. The potential impact of such vulnerabilities is significant, as it could lead to data breaches, system downtime, and compromised operational integrity.

### Control Identifier: AC-19

Control Description:

This control requires the establishment of configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices, particularly when these devices are outside of controlled areas. It also involves authorizing the connection of mobile devices to organizational systems. Mobile devices, such as smartphones and tablets, have computing capabilities comparable to desktop systems and require stringent control measures to prevent unauthorized access, data transfer, and potential malware introduction. The control emphasizes the need for users to take physical actions to protect and control these devices when they are outside controlled areas.

Assessment Findings:

The assessment found that configuration and connection requirements for mobile devices are well-defined and implemented. However, there were some gaps in the enforcement of these requirements, particularly in ensuring that all mobile devices are regularly updated with the latest security patches. Additionally, while authorization procedures are in place, some devices were found to have connected to the network without proper authorization, posing a potential security risk.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate control over mobile devices includes the possibility of unauthorized data transfer and the introduction of malware into the organization's network. These devices could be exploited to transfer sensitive data to unauthorized systems or introduce malicious software, leading to significant data breaches, operational disruptions, financial losses, and damage to the organization's reputation. Strict controls on the use of mobile devices are essential to mitigate these risks, ensuring that devices are only used in a secure and authorized manner.

### Control Identifier: CM-7

Control Description:

This control requires the configuration of systems to provide only mission-essential capabilities as defined by the organization. It also mandates the prohibition or restriction of unnecessary functions, ports, protocols, software, and services. The intent is to minimize the system's attack surface by eliminating unnecessary functionality, which could otherwise be exploited. The control suggests using tools like network scanners, intrusion detection/prevention systems, and endpoint protection technologies to enforce least functionality, thereby ensuring that systems are limited to the essential services needed to support organizational missions, functions, or operations.

Assessment Findings:

The assessment found that the organization has implemented the principle of least functionality by configuring systems to provide only essential capabilities. However, it was noted that some systems still had unnecessary services or applications enabled, which were not required for their intended purpose. This was particularly evident in legacy systems that had not been updated or reconfigured in line with current security policies. Additionally, while tools are in place to identify and prevent the use of prohibited functions, there were gaps in the continuous monitoring process, which could allow unauthorized services to remain active.

Assessment Status: Implemented

Associated Risk:

The risk associated with failing to enforce least functionality includes an expanded attack surface, making organizational systems more susceptible to exploitation through unnecessary or unused system capabilities. If these vulnerabilities are exploited, it could lead to data modification, destruction, or corruption, as well as unauthorized access to sensitive information. This increases the likelihood of significant security incidents that could harm the organization's operations, assets, and reputation. Implementing and enforcing this control mitigates the risk by ensuring systems are configured to perform only their intended functions, thereby reducing opportunities for attackers to exploit unnecessary functionality.

### Control Identifier: IR-6

Control Description:

This control requires that personnel report suspected incidents to the organizational incident response capability within a defined time period. Additionally, it mandates that incident information be reported to designated authorities as defined by the organization. The types of incidents, the content and timeliness of reports, and the reporting authorities are determined by applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Proper incident reporting is essential for informing risk assessments, evaluating control effectiveness, and guiding decisions related to technology acquisitions.

Assessment Findings:

The assessment found that procedures for incident reporting are in place, and personnel are generally aware of the requirement to report suspected incidents within the specified time frame. However, there were some gaps in the completeness and timeliness of incident documentation, with some incidents not being reported to the appropriate authorities as quickly as required. Additionally, the communication of incident information to external stakeholders was inconsistent, potentially leading to non-compliance with regulatory requirements.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with inadequate incident reporting includes the potential for security incidents to be improperly tracked, documented, or communicated. This can result in ineffective incident response, non-compliance with legal and regulatory requirements, and missed opportunities to enhance security practices through lessons learned. Incomplete or delayed reporting can lead to significant consequences, including operational disruptions, financial losses, and damage to the organization's reputation. Implementing and enforcing this control mitigates these risks by ensuring that all incidents are properly reported and documented, enabling a more effective and coordinated response.

### Control Identifier: AU-2

Control Description:

This control requires the identification of the types of events that the system is capable of logging to support the audit function. It also involves coordinating the event logging function with other organizational entities requiring audit-related information, specifying the types of events for logging within the system, and providing a rationale for why these event types are adequate for supporting after-the-fact investigations of incidents. Event logging includes capturing significant and relevant events related to system security and the privacy of individuals, such as password changes, failed logons, and administrative privilege usage. The control emphasizes the importance of reviewing and updating the event types selected for logging to ensure they remain relevant and continue to support the organization’s monitoring and auditing needs.

Assessment Findings:

The assessment found that the event logging capabilities are implemented and aligned with the organization's requirements. However, there were some issues with the consistency and completeness of logged events, particularly in high-volume environments where system performance concerns led to the deactivation of certain logging functions. Additionally, the review and update process for logged event types was found to be irregular, with some logs not being updated to reflect new security requirements or system changes.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate event logging includes the inability to detect, analyze, and respond to unauthorized or malicious activities within the system. This can lead to undetected security incidents, prolonged breaches, and non-compliance with regulatory requirements. If critical events are not logged, or if logs are not adequately maintained and reviewed, the organization may be unable to identify the root causes of problems or respond effectively to security threats. Properly creating and retaining audit logs mitigates this risk by enabling effective monitoring and investigation, ensuring that the organization can quickly identify and respond to security incidents.

### Control Identifier: CM-11

Control Description:

This control requires the organization to establish policies governing the installation of software by users, enforce these policies through defined methods, and monitor compliance on a regular basis. The intent is to control and manage the software that users install on organizational systems to prevent unauthorized, insecure, or potentially malicious software from being introduced. This includes defining what software users are permitted to install, such as updates to existing software or approved applications, and what is prohibited, such as software with unknown or suspicious origins.

Assessment Findings:

The assessment found that the organization has established clear policies regarding user-installed software, with enforcement mechanisms in place, including both procedural controls and automated monitoring tools. However, some gaps were identified in the enforcement process, particularly in scenarios where users with elevated privileges bypassed restrictions to install non-approved software. Additionally, the frequency of compliance monitoring was found to be insufficient in some departments, leading to delays in identifying and addressing unauthorized installations.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate control over user-installed software includes the potential for unauthorized, insecure, or malicious software to be installed by users, leading to significant security incidents. Such incidents could result in data breaches, system compromises, and operational disruptions. The likelihood of these events increases if users are able to install software without proper oversight or if monitoring is not conducted regularly. Implementing and enforcing this control mitigates the risk by ensuring that user-installed software is properly controlled and monitored, reducing the likelihood of unauthorized software being introduced and limiting the potential impact on the organization’s security posture.

### Control Identifier: AU-5

Control Description:

This control requires the organization to alert designated personnel or roles within a specified time period in the event of an audit logging process failure. Additionally, it mandates taking further actions as defined by the organization. Audit logging process failures may include software and hardware errors, failures in audit log capturing mechanisms, or reaching/exceeding audit log storage capacity. The control emphasizes the importance of defining actions based on the type, location, and severity of the failure, ensuring that audit logging issues are promptly identified and addressed to maintain the integrity and continuity of security monitoring.

Assessment Findings:

The assessment found that mechanisms for detecting and responding to audit logging process failures are in place and functioning as intended. Alerts are configured to notify the appropriate personnel within the defined time frame when failures occur. However, it was noted that some logging failures went undetected due to limitations in the monitoring tools, particularly in environments with complex logging architectures. Additionally, while basic responses like alerting and overwriting old logs are defined, there was a lack of clarity around more severe responses, such as shutting down systems or stopping the generation of audit records.

Assessment Status: Implemented

Associated Risk:

The risk associated with undetected audit logging failures includes the possibility of gaps in security monitoring, which could result in missing critical data needed to investigate security incidents. If audit logging failures go unnoticed, this could lead to undetected security breaches, prolonged exposure to threats, and an inability to respond effectively to security incidents. The potential impact is significant, as it could hinder the organization's ability to maintain a robust security posture. Implementing and properly configuring alerts for logging failures mitigates this risk by ensuring that issues are quickly identified and addressed, preserving the integrity and effectiveness of the audit logging process.

### Control Identifier: IA-6

Control Description:

This control requires the obscuring of feedback of authentication information during the authentication process to protect it from potential exploitation by unauthorized individuals. The purpose is to ensure that systems do not provide feedback that could be used to compromise authentication mechanisms. Obscuring methods may vary based on the type of device, with common techniques including displaying asterisks when passwords are typed or briefly displaying input before obscuring it. This control is particularly important in preventing shoulder surfing and other forms of unauthorized observation.

Assessment Findings:

The assessment found that the organization has implemented obscuring feedback mechanisms effectively across various systems, including desktops, notebooks, and mobile devices. The feedback obscuring methods, such as masking passwords with asterisks, are consistently applied, reducing the likelihood of authentication information being observed by unauthorized individuals. However, some legacy systems still lack proper feedback obscuring, which could expose authentication details in certain scenarios.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate authentication feedback obscuring includes the possibility that authentication information could be observed and captured by unauthorized individuals during the login process. This exposure could lead to unauthorized access and other security incidents. The impact of such a compromise could be significant, including unauthorized system access, data breaches, and operational disruptions. By implementing and enforcing proper feedback obscuring techniques, the organization mitigates these risks, ensuring that sensitive information remains protected during authentication processes and reducing the chances of it being captured by attackers.

### Control Identifier: IA-5(2)

Control Description:

This control mandates that for public key-based authentication, the organization must enforce authorized access to the corresponding private key and map the authenticated identity to the account of the individual or group. When public key infrastructure (PKI) is used, the organization must validate certificates by constructing and verifying a certification path to an accepted trust anchor and implement a local cache of revocation data to support path discovery and validation. Public key cryptography is an essential authentication mechanism that requires strict management of private keys and continuous verification of certificate validity to ensure secure authentication processes.

Assessment Findings:

The assessment determined that the organization has effectively implemented public key-based authentication, with controls in place to enforce authorized access to private keys and to map authenticated identities accurately. PKI certificates are validated by constructing and verifying certification paths to trusted anchors, and a local cache of revocation data is maintained to ensure availability even when network access to revocation information is disrupted. However, some gaps were identified in the frequency of updates to the revocation cache, which could delay the detection of revoked certificates.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate management of public key-based authentication includes the possibility of unauthorized access due to the continued use of compromised or outdated certificates. If temporary passwords or keys are not properly managed, they may be exploited beyond their intended purpose, increasing the likelihood of unauthorized access. This could result in significant security incidents, including unauthorized data access, system breaches, and compromised communications. By enforcing stringent controls on private key access and ensuring continuous validation of certificates, this control mitigates the risk, ensuring the integrity and security of the authentication process

### Control Identifier: IA-4(6)

Control Description:

This control requires coordination with external organizations for the cross-organization management of identifiers. Cross-organization identifier management involves the ability to identify individuals, groups, roles, or devices when conducting activities that involve the processing, storage, or transmission of information across different organizations. This coordination is crucial for ensuring that identifiers are properly managed, especially in collaborative environments where multiple organizations interact and share resources.

Assessment Findings:

The assessment found that the organization has established coordination mechanisms with relevant external organizations to manage identifiers across organizational boundaries. This coordination includes regular updates and synchronization of identifier status to prevent conflicts or unauthorized reuse. However, some challenges were noted in deactivating identifiers that are no longer in use, particularly when employees or devices transition between organizations. There were instances where inactive identifiers remained active longer than necessary, increasing the risk of unauthorized access.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate cross-organization identifier management includes the potential for unauthorized access or security incidents due to the reuse of identifiers that should have been deactivated. If inactive identifiers remain active, they could be exploited to gain unauthorized access to systems and data, leading to significant security incidents such as data breaches and system compromises. This risk is particularly high in collaborative environments where identifiers are shared across organizations. Implementing this control mitigates the risk by ensuring that inactive accounts are automatically disabled after a defined period, reducing the attack surface and enhancing overall security.

### Control Identifier: IA-5(1)

Control Description:

This control applies to password-based authentication and includes requirements for maintaining and updating a list of commonly-used, expected, or compromised passwords; verifying passwords against this list when users create or update them; transmitting passwords only over cryptographically-protected channels; storing passwords using an approved salted key derivation function; and enforcing immediate password changes upon account recovery. The control also encourages the use of long passwords or passphrases and the use of automated tools to assist users in selecting strong passwords. The goal is to prevent password reuse and ensure that users create strong, unique passwords that enhance the security of the organization's systems.

Assessment Findings:

The assessment found that the organization has implemented most of the required controls for password-based authentication, including the use of cryptographically-protected channels for transmitting passwords and the enforcement of password changes upon account recovery. However, there were some gaps in maintaining and updating the list of commonly-used, expected, or compromised passwords, which could allow weak or compromised passwords to be used. Additionally, while users are encouraged to select long passwords, the enforcement of composition and complexity rules was found to be inconsistent across different systems.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate password management includes the possibility of password reuse or the use of weak passwords, which could significantly weaken the security of the organization's systems. Reusing old passwords or selecting weak passwords can lead to easier password guessing or compromise, resulting in unauthorized access and potential data breaches. The impact of such incidents could be severe, including loss of sensitive data, unauthorized system access, and significant operational disruptions. Implementing this control mitigates the risk by enforcing policies that prohibit password reuse and ensure that users consistently create strong, unique passwords, thereby enhancing the overall security posture of the organization.

### Control Identifier: AT-2(2)

Control Description:

This control involves providing literacy training on recognizing and reporting potential indicators of insider threats. Indicators may include behaviors such as long-term job dissatisfaction, attempts to access unauthorized information, unexplained financial resources, bullying, harassment, workplace violence, and other serious policy violations. The training includes guidance on how to communicate concerns about insider threats through the organization’s established channels, following proper procedures. The control also suggests tailoring training content to specific roles within the organization to make it more relevant and effective.

Assessment Findings:

The assessment found that the organization has implemented literacy training on insider threats as required. The training programs cover a broad range of potential indicators and provide clear instructions on how to report suspicious activities. However, it was noted that while the training is comprehensive, participation rates in the training sessions were lower than expected in some departments. This could lead to gaps in awareness and potentially allow insider threats to go undetected.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate insider threat awareness training includes the possibility that potential indicators of insider threats may go unnoticed by employees or managers, allowing malicious activities to occur without timely intervention. If these threats are not detected early, they could lead to significant harm to the organization, including data breaches, financial losses, and reputational damage. By implementing and regularly updating this training, the organization mitigates these risks by ensuring that all personnel are equipped to recognize and report signs of insider threats, thereby enhancing the overall security posture and protecting the organization from internal harm.

### Control Identifier: AU-9(3)

Control Description:

This control requires the implementation of cryptographic mechanisms to protect the integrity of audit information and audit tools. Cryptographic mechanisms, such as signed hash functions using asymmetric cryptography, are used to ensure that the audit information has not been tampered with. These mechanisms allow the distribution of a public key to verify the hash while keeping the secret key confidential, which was used to generate the hash. This ensures that the integrity of the audit logs is maintained, and any unauthorized alterations can be detected.

Assessment Findings:

The assessment found that cryptographic mechanisms are in place to protect the integrity of audit logs and tools. The organization employs signed hash functions to verify the integrity of audit data, ensuring that any attempts to alter the logs can be identified. However, it was noted that the management of these cryptographic mechanisms was not consistently restricted to a subset of privileged users, which could increase the risk of unauthorized access to audit management functions.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate protection of audit information includes the possibility of unauthorized or inappropriate management of audit logging functionality. If users who should not have access to audit management functions are able to alter or disable logging, this could compromise the integrity and availability of critical audit information. This could result in tampering with logs, misconfiguring log settings, or disabling logging functions altogether. The potential impact is significant, as it could prevent the organization from detecting security incidents or investigating them properly. Limiting the management of audit logging to a subset of privileged users, along with the use of cryptographic protection, mitigates this risk by ensuring that only trusted, qualified individuals have the authority to manage these sensitive functions, thereby preserving the reliability and security of audit logs.

### Control Identifier: AU-6(3)

Control Description:

This control requires the organization to analyze and correlate audit records across different repositories to gain organization-wide situational awareness. This approach ensures that audit data from various sources are reviewed together, providing a comprehensive view of security events and supporting awareness across all levels of risk management, including the organizational level, mission/business process level, and information system level. The goal is to detect and respond to complex or distributed security incidents that might involve multiple systems or areas within the organization.

Assessment Findings:

The assessment found that the organization has implemented processes to correlate audit records from different systems, which has improved the ability to detect complex security incidents. However, some challenges remain in integrating data from older legacy systems that do not easily interface with newer logging and correlation tools. Additionally, while the correlation processes are in place, the frequency of analysis and the resources allocated to this task are sometimes insufficient to handle the volume of data, potentially leading to delays in detecting and responding to incidents.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate correlation of audit records includes the potential for missing or failing to detect complex or distributed security incidents. Without effective correlation, the organization might be unable to identify security events that span multiple systems, such as advanced persistent threats (APTs), insider threats, or coordinated attacks. This could result in severe security breaches, including data modification, destruction, corruption, and operational disruptions. The impact of such incidents could be significant, leading to data loss, compliance failures, and substantial harm to the organization’s operations and reputation. Implementing this control mitigates these risks by ensuring that audit logs are reviewed in a comprehensive and correlated manner, providing a more complete picture of the organization’s security posture.

### Control Identifier: AC-22

Control Description:

This control requires the organization to designate individuals authorized to make information publicly accessible and to ensure these individuals are properly trained. The control also mandates a review of content before it is posted publicly to ensure no nonpublic information, such as Controlled Unclassified Information (CUI), is included. Regular reviews of publicly accessible content are also required to identify and remove any nonpublic information that may have been posted inadvertently. This control is essential to prevent unauthorized disclosure of sensitive information, which could lead to significant data breaches and other security incidents.

Assessment Findings:

The assessment found that the organization has designated individuals responsible for managing publicly accessible content and has provided them with the necessary training. Procedures are in place to review content before it is posted publicly, ensuring that nonpublic information is not included. However, the frequency of reviews for content already posted on publicly accessible systems was found to be inconsistent, which could increase the risk of sensitive information being exposed for longer periods before it is detected and removed.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate management of publicly accessible content includes the potential for unauthorized disclosure of CUI and other sensitive information. If such information is exposed to the public, it could lead to significant data breaches, loss of trust from stakeholders, and potential legal repercussions. The impact could be severe, including damage to the organization's reputation, financial losses, and regulatory penalties. Implementing controls to manage how CUI is posted and processed on public systems is critical to preventing unauthorized disclosure and protecting the organization's sensitive information. Regular review and prompt removal of any nonpublic information discovered are essential to mitigating this risk.

### Control Identifier: SC-19

Control Description:

The control SC-19, related to Voice Over Internet Protocol (VoIP), has been withdrawn because it was deemed technology-specific. Instead, VoIP is addressed as any other technology or protocol within the organization's security framework. Despite being withdrawn, the associated security concerns around VoIP communications still require attention to ensure they are appropriately managed and secured, particularly against risks such as unauthorized access and interception.

Assessment Findings:

Although SC-19 has been officially withdrawn, the organization continues to implement security measures for VoIP communications. These measures include secure configuration, regular monitoring, and strict access controls to prevent unauthorized access and interception of VoIP traffic. The organization treats VoIP like any other technology, applying general security protocols and controls to ensure its secure operation. However, given that the control is withdrawn, there is no specific policy or control that directly addresses VoIP as a standalone concern, which could lead to potential gaps in the security posture.

Assessment Status: Implemented

Associated Risk:

The risk associated with VoIP communications, despite the withdrawal of SC-19, includes unauthorized access to or interception of sensitive communications. If VoIP communications are not adequately protected, they could be intercepted, disrupted, or otherwise compromised, leading to significant security incidents such as unauthorized disclosure of sensitive information, disruption of communication channels, and potential exploitation by attackers. The impact could be severe, particularly in environments where VoIP is used for critical communications. Implementing secure configurations, regular monitoring, and strict access controls for VoIP technologies mitigates this risk, reducing both the likelihood and impact of potential security breaches.

### Control Identifier: AU-6

Control Description:

This control requires the organization to review and analyze system audit records regularly for indications of inappropriate or unusual activity and assess the potential impact of such activities. Findings from the audit reviews must be reported to designated personnel or roles. Additionally, the organization should adjust the level of audit record review, analysis, and reporting based on changes in risk, such as new information from law enforcement or other credible sources. This control is critical for maintaining effective security monitoring and ensuring that any unauthorized or suspicious activities are promptly detected and addressed.

Assessment Findings:

The assessment found that the organization has established processes for the regular review and analysis of audit records. These processes include identifying unusual or inappropriate activities and reporting findings to the appropriate personnel, such as the incident response team or security office. However, some gaps were identified in the frequency and comprehensiveness of the audit reviews, particularly in response to evolving threats. There was also a noted need for more timely adjustments to the scope and depth of audit reviews when new risk information is received.

Assessment Status: Implemented

Associated Risk:

The risk associated with inadequate audit record review and analysis includes the possibility of missing or outdated log information, which can lead to undetected security incidents or an inability to respond effectively to evolving threats. If the organization does not regularly review and update its logging practices, critical security incidents may be missed, and the organization could be unable to respond promptly and effectively. The impact of such failures could be significant, resulting in data modification, destruction, or corruption, as well as potential operational disruptions and compliance failures. Regularly reviewing and updating logged events mitigates this risk by ensuring that logging practices remain relevant and comprehensive, enabling effective monitoring, detection, and response to security threats.

### Control Identifier: RA-5(2)

Control Description:

This control requires the organization to update the list of system vulnerabilities to be scanned on a regular basis, particularly when new vulnerabilities are identified and reported. Given the complexity of modern software and systems, new vulnerabilities are continuously discovered. It is essential to incorporate these newly discovered vulnerabilities into the scanning process to ensure that the organization can promptly identify and mitigate them, reducing the risk of exploitation.

Assessment Findings:

The assessment found that the organization has implemented a process for regularly updating the list of vulnerabilities to be scanned. This includes adding newly discovered vulnerabilities prior to each scan and as they are identified through threat intelligence or vendor reports. However, there were some instances where delays in updating the vulnerability list were noted, potentially leaving the organization exposed to known vulnerabilities for longer than necessary.

Assessment Status: Implemented

Associated Risk:

The risk associated with not promptly updating the list of vulnerabilities to be scanned includes the potential for known vulnerabilities to be exploited by attackers. If critical vulnerabilities are not addressed in a timely manner, attackers may exploit these weaknesses, leading to significant security incidents, including data modification, destruction, corruption, and system compromises. The impact of such incidents could be severe, resulting in data breaches, operational disruptions, and financial losses. Implementing this control mitigates the risk by ensuring that vulnerabilities are regularly updated and prioritized based on their assessed risk, allowing the organization to focus remediation efforts on the most critical vulnerabilities, thereby reducing the likelihood and impact of security breaches.

### Control Identifier: RA-5

Control Description:

The control RA-5 focuses on the continuous monitoring and scanning of system and application vulnerabilities. The organization is required to monitor and scan for vulnerabilities at a frequency determined by the organization, and additionally whenever new vulnerabilities that could affect the system are identified. The control mandates the use of tools that are capable of interoperability, automating parts of the vulnerability management process, and the capability to update the vulnerabilities to be scanned. Vulnerability scan reports and monitoring results should be analyzed, and legitimate vulnerabilities should be remediated within organization-defined response times based on an assessment of risk. Moreover, information obtained from the vulnerability monitoring process must be shared with designated personnel to prevent similar vulnerabilities in other systems.

Assessment Findings:

The assessment revealed that the organization has implemented a robust vulnerability monitoring and scanning process. This includes the regular updating of scanning tools and vulnerability lists, as well as the analysis of scan reports to ensure that vulnerabilities are identified and addressed promptly. The organization also utilizes various tools and techniques that facilitate interoperability and automate parts of the vulnerability management process, ensuring that vulnerabilities are not missed. However, the assessment identified a few areas where the frequency of scans could be increased, particularly in response to newly reported vulnerabilities. Additionally, while most vulnerabilities are remediated within the defined response times, there were a few instances where remediation was delayed due to resource constraints.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with inadequate vulnerability monitoring and scanning is that critical vulnerabilities in systems and applications may go undetected, allowing attackers to exploit these weaknesses. Unpatched vulnerabilities pose a significant risk of data modification, destruction, or corruption, leading to data breaches, system compromises, and potential operational disruptions. If vulnerabilities are not regularly identified and addressed, the organization faces an increased likelihood of security incidents, which can result in severe consequences, including financial losses, reputational damage, and non-compliance with regulatory requirements. Implementing this control mitigates the risk by ensuring that vulnerabilities are regularly monitored, identified, and addressed, reducing both the likelihood and impact of potential security breaches.

### Control Identifier: IA-4

Control Description:

The IA-4 control focuses on the management of system identifiers, which are used to uniquely identify individuals, groups, roles, services, or devices within the system. The control requires organizations to receive authorization from designated personnel to assign these identifiers, select appropriate identifiers for the intended entity, assign the identifiers, and prevent their reuse for a specified period. The identifiers can include common device identifiers such as Media Access Control (MAC) addresses, Internet Protocol (IP) addresses, or unique token identifiers. Preventing the reuse of identifiers ensures that previously used identifiers are not reassigned to different entities, which helps maintain system integrity and accountability.

Assessment Findings:

The assessment confirmed that the organization has implemented a systematic process for managing system identifiers. The organization has established protocols for receiving authorization before assigning identifiers, selecting appropriate identifiers, and ensuring that these identifiers are assigned correctly to the intended individual, group, role, service, or device. Moreover, the organization has implemented measures to prevent the reuse of identifiers for a designated period, reducing the risk of identifiers being recycled prematurely. However, the assessment did note that the enforcement of identifier reuse prevention could be improved in some instances, particularly regarding the assignment of device identifiers, to ensure that no overlap occurs.

Assessment Status: Implemented

Associated Risk:

The main risk associated with inadequate identifier management is the potential for unauthorized access or security incidents due to the inappropriate reuse of identifiers. If identifiers are reused without proper controls, there is a risk of unauthorized access, account misuse, and loss of accountability, which can lead to data breaches, system compromises, and other security incidents. Implementing controls to prevent the reuse of identifiers for a defined period mitigates this risk by ensuring that identifiers are not recycled too quickly, thereby protecting the integrity and security of the organization's systems and data.

### Control Identifier: AU-7

Control Description:

The AU-7 control mandates that organizations implement a capability for reducing audit records and generating reports without altering the original content or time ordering of the audit records. This capability must support on-demand audit record review, analysis, and reporting requirements, particularly for after-the-fact investigations of incidents. Audit record reduction involves processing collected audit log information into a summary format that is more meaningful to analysts. This includes using modern data mining techniques and advanced data filters to identify anomalous behavior in audit records. The system's report generation capability should provide customizable reports that assist in the timely detection and analysis of security incidents.

Assessment Findings:

The assessment found that the organization has successfully implemented a robust audit record reduction and report generation capability. This capability allows for on-demand review, analysis, and reporting of audit records, which is crucial for both real-time monitoring and post-incident investigations. The system effectively processes large volumes of audit data, reducing it to a manageable and actionable format without altering the original content or the chronological order of the records. However, the assessment noted that as the volume of audit data continues to grow, there may be a need for additional resources or more advanced tools to prevent analysts from being overwhelmed by the data, thereby ensuring continued effectiveness in incident detection and response.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with insufficient audit record reduction and report generation is that the organization may become overwhelmed by large volumes of audit data, making it difficult to detect, analyze, and respond to security incidents in a timely manner. This could result in delayed detection of breaches, incomplete investigations, and greater damage from security incidents. By implementing this control, the organization mitigates the risk by enabling efficient reduction, filtering, and reporting of audit records, thus supporting effective on-demand analysis and timely incident response.

### Control Identifier: MP-3

Control Description:

The MP-3 control requires organizations to mark system media to indicate distribution limitations, handling caveats, and applicable security markings of the information contained on the media. This includes both digital media, such as diskettes, magnetic tapes, external hard drives, flash drives, and optical discs, as well as non-digital media, such as paper and microfilm. The control also allows for the exemption of certain types of media from marking requirements if the media remains within designated controlled areas as defined by the organization. The markings reflect applicable laws, executive orders, policies, and regulations, particularly for Controlled Unclassified Information (CUI) as defined by the National Archives and Records Administration.

Assessment Findings:

The assessment found that the organization has implemented the required media marking procedures for both digital and non-digital media containing CUI. These procedures ensure that all media is appropriately marked with security labels that indicate the necessary handling precautions and distribution limitations. The organization has also defined and documented specific types of media that are exempt from marking when they remain within controlled areas, in compliance with organizational policies. This practice ensures that CUI is adequately protected from unauthorized access or distribution.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with inadequate media marking is the mishandling or unauthorized distribution of media containing CUI, which could lead to unauthorized access or disclosure of sensitive information. Such incidents can result in significant security breaches and regulatory non-compliance. By marking all media containing CUI with appropriate labels and distribution limitations, the organization mitigates the risk of mishandling and reduces the potential impact of any security incidents.

### Control Identifier: SI-2

Control Description:

The SI-2 control focuses on the identification, reporting, and remediation of system flaws. It requires organizations to:

Identify, report, and correct system flaws in a timely manner.

Test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

Install security-relevant software and firmware updates within organization-defined time periods.

Incorporate flaw remediation activities into the organizational configuration management process.

This control applies to all types of software and firmware, requiring organizations to identify systems affected by software flaws, report vulnerabilities, and ensure that updates, such as patches and service packs, are applied promptly. By integrating flaw remediation into configuration management, organizations can track and verify remediation actions, ensuring that updates are applied effectively without introducing new risks.

Assessment Findings:

The assessment found that the organization has implemented robust processes for identifying, reporting, and correcting system flaws. Security-relevant updates, including patches and firmware upgrades, are regularly tested for effectiveness and potential side effects before deployment. The organization has defined time periods for applying updates, which vary based on the severity of the vulnerability and the criticality of the system involved. Flaw remediation has been successfully integrated into the organization's configuration management process, allowing for effective tracking and verification of remediation efforts. This ensures that all identified vulnerabilities are addressed promptly, thereby maintaining the security and integrity of the organization's systems.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with unaddressed system flaws is the potential for attackers to exploit these vulnerabilities, leading to system compromises. Unpatched flaws can provide an entry point for malicious actors, resulting in data breaches, system corruption, or unauthorized access.

### Control Identifier: PE-3

Control Description:

The PE-3 control focuses on enforcing physical access controls at entry and exit points to the facility where the system resides. Key aspects of this control include:

Enforcing physical access authorizations by verifying individual access before granting entry and controlling ingress and egress to the facility using organization-defined physical access control systems or devices, or guards.

Maintaining physical access audit logs for defined entry or exit points.

Implementing controls for publicly accessible areas within the facility.

Escorting and controlling visitor activity under organization-defined circumstances.

Securing keys, combinations, and other physical access devices.

Conducting regular inventories of physical access devices and changing combinations and keys according to a defined schedule or when necessary due to loss or compromise.

Physical access control is critical to safeguarding the physical environment where the organization's systems and data reside, ensuring that only authorized individuals have access to sensitive areas. This control also applies to monitoring and auditing physical access to detect and respond to any unauthorized activities.

Assessment Findings:

The assessment determined that the organization has implemented physical access controls effectively across its facilities. Physical access is tightly controlled at all entry and exit points, with strict verification procedures in place. The organization employs a combination of automated physical access control systems and guards to manage ingress and egress. Physical access audit logs are maintained diligently, and the facility includes designated publicly accessible areas with appropriate access controls to prevent unauthorized movement to non-public areas. Visitor activity is monitored and controlled through established procedures, including escort requirements under specific circumstances. Additionally, keys, combinations, and other physical access devices are secured, regularly inventoried, and changed according to the organization’s policies.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with inadequate physical access control is the potential for undetected physical breaches or environmental threats to the organization’s systems and infrastructure. This could lead to unauthorized access, data breaches, or damage to critical systems, thereby compromising the organization’s security posture.

### Control Identifier: PE-8

Control Description:

The PE-8 control requires organizations to maintain and manage visitor access records for facilities where critical systems reside. This control includes:

Maintaining visitor access records: Organizations must keep records of all visitors for a defined period. These records typically include names, organizations, visitor signatures, identification types, dates of access, entry and departure times, the purpose of the visit, and the individuals visited.

Reviewing visitor access records: The records should be reviewed regularly to ensure that access authorizations are up to date and continue to support the organization’s mission and business functions.

Reporting anomalies: Any irregularities or anomalies discovered during the review process must be reported to designated personnel for further investigation.

Proper management of visitor access records is essential for preventing unauthorized access to sensitive areas within the facility and for maintaining a detailed log of who accessed the facility and when.

Assessment Findings:

The assessment determined that the organization has implemented the control effectively. Visitor access records are meticulously maintained, including detailed information about each visitor, such as identification, entry and departure times, and the purpose of the visit. These records are reviewed regularly as per the organization's defined schedule. Any anomalies identified during the review are promptly reported to the appropriate personnel for further action. This systematic approach ensures that any potential unauthorized access or malicious activities by visitors can be detected and addressed quickly.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with inadequate visitor access record management is the potential for unauthorized access or malicious activity by visitors. If visitor records are not properly maintained, reviewed, and anomalies reported, visitors could exploit this weakness to gain unauthorized access to sensitive areas or engage in harmful activities, leading to security incidents, including data breaches or physical damage.

### Control Identifier: PE-2

Control Description:

The PE-2 control is designed to ensure that only authorized individuals have physical access to facilities where critical systems reside. This control includes:

Developing, approving, and maintaining a list of authorized individuals: Organizations must maintain an up-to-date list of all individuals authorized to access the facility. This list should be regularly reviewed to ensure its accuracy.

Issuing authorization credentials: Physical access is controlled through the issuance of credentials such as ID badges, identification cards, or smart cards, which must be presented for entry.

Reviewing the access list: The access list must be reviewed at an organization-defined frequency to ensure that only those who need access have it.

Removing access when no longer required: Individuals must be promptly removed from the access list when they no longer require access to the facility.

Proper implementation of this control helps prevent unauthorized physical access to systems and equipment, reducing the risk of security incidents such as theft, tampering, or data breaches.

Assessment Findings:

The assessment revealed that the organization has effectively implemented the PE-2 control. The access list of authorized individuals is current and maintained rigorously. Credentials are issued and managed according to defined procedures, ensuring that only those with a legitimate need can access the facility. The access list is reviewed regularly to identify and remove individuals who no longer require access. This approach helps maintain strict control over who can enter sensitive areas, thereby protecting critical systems and data.

Assessment Status: Implemented

Associated Risk:

The main risk addressed by this control is the potential for unauthorized physical access to systems and equipment. Without proper physical access controls, unauthorized individuals could enter secure areas, leading to serious security incidents, such as theft, tampering with equipment, or data breaches.

### Control Identifier: AC-8

Control Description:

The AC-8 control is designed to ensure that users are informed of their responsibilities and the legal conditions associated with accessing an organization's systems. This control includes:

Displaying a system use notification message or banner: The message informs users that they are accessing a U.S. Government system, that usage may be monitored, recorded, and audited, that unauthorized use is prohibited and subject to penalties, and that use of the system implies consent to such monitoring and recording.

Retaining the notification until acknowledgment: The system use notification must remain visible until users acknowledge the conditions and explicitly take action to log on or further access the system.

Publicly accessible systems: Additional conditions apply, including displaying system use information consistent with privacy accommodations, references to monitoring, and descriptions of authorized uses of the system.

This control ensures that users are aware of their obligations and the potential consequences of unauthorized actions, thereby helping to prevent the mishandling of Controlled Unclassified Information (CUI) and other sensitive data.

Assessment Findings:

The assessment confirmed that the organization has effectively implemented the AC-8 control. The system use notification is prominently displayed before users can log into the system, and it contains the required information. Users must acknowledge the notification before proceeding, which ensures that they are informed of their responsibilities and the legal implications of accessing the system. This process is consistent across all access points, including publicly accessible systems where additional notifications are provided as required.

Assessment Status: Implemented

Associated Risk:

The primary risk addressed by this control is that users may be unaware of their obligations and responsibilities regarding the handling of Controlled Unclassified Information (CUI) and other sensitive data. Without clear notification, users might unknowingly engage in activities that could lead to data breaches, non-compliance with legal and regulatory requirements, and damage to the organization's reputation.

### Control Identifier: CM-1

Control Description:

The CM-1 control requires organizations to develop, document, and disseminate configuration management policies and procedures at the organization, mission/business process, or system level. The policy must address key areas such as purpose, scope, roles, responsibilities, management commitment, and compliance with applicable laws and regulations. Additionally, procedures must be established to facilitate the implementation of the configuration management policy and associated controls. The organization must designate an official responsible for managing the development, documentation, and dissemination of these policies and procedures. Regular reviews and updates of the policy and procedures are necessary, particularly following significant events such as audits, security incidents, or changes in regulations.

Assessment Findings:

The assessment found that the organization has established comprehensive configuration management policies and procedures that align with organizational goals and regulatory requirements. These policies and procedures are regularly reviewed and updated to address any changes in the operational environment or applicable laws. The designated official effectively manages the development and dissemination of these documents, ensuring that all relevant personnel are informed and compliant with the policies. The procedures are detailed, providing clear guidance on how to implement the configuration management controls, which helps maintain system integrity and security.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with inadequate configuration management policies and procedures is the potential for unauthorized or unmanaged changes to system configurations. This can lead to configuration drift, unmanaged changes, and inconsistencies, which in turn create security vulnerabilities and increase the likelihood of system breaches. Such issues can compromise system integrity, cause operational disruptions, and make it challenging to maintain compliance with security standards.

### Control Identifier: SA-8

Control Description:

The SA-8 control requires organizations to apply defined security and privacy engineering principles throughout the system development life cycle. This includes the specification, design, development, implementation, and modification of systems and system components. The principles aim to ensure that security and privacy are integrated into the system from the outset, thereby reducing vulnerabilities, mitigating risks, and enhancing the overall security posture of the system. Examples of these principles include developing layered protections, incorporating security and privacy requirements into the system design, ensuring secure software development practices, and performing threat modeling to identify and mitigate potential risks.

Assessment Findings:

The assessment determined that the organization has effectively integrated security and privacy engineering principles into its system development life cycle. These principles are consistently applied to new systems under development as well as to upgrades and modifications of existing systems. The organization has established a robust framework that includes layered protections, comprehensive security and privacy policies, and rigorous controls that are tailored to meet specific organizational needs. Additionally, developers receive training on secure software development, which further strengthens the security posture of the systems being developed. The organization also employs threat modeling to proactively identify and address potential vulnerabilities.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with inadequate application of security and privacy engineering principles is the potential for inherent vulnerabilities in organizational systems due to poor design, insecure development practices, or inadequate systems engineering. Systems developed without a strong focus on security and privacy are more susceptible to attacks, leading to data loss, information disclosure, or other significant security incidents.

### Control Identifier: AT-3

Control Description:

The AT-3 control requires organizations to provide role-based security and privacy training to personnel with specific roles and responsibilities. This training should be provided before individuals are authorized to access the system, information, or perform their assigned duties, and should be refreshed at an organization-defined frequency. The training must also be updated whenever there are significant system changes or when lessons learned from internal or external security incidents or breaches become available. The content of the training is tailored to the specific roles and responsibilities of the personnel, ensuring that they are adequately prepared to handle their information security responsibilities.

Assessment Findings:

The assessment determined that the organization has effectively implemented role-based security and privacy training. The training is provided to personnel before they begin their duties and is regularly updated to reflect new threats, system changes, and lessons learned from security incidents. The organization has identified the roles that require specific training, including system administrators, security officers, and others with access to sensitive information. Training content is reviewed and updated regularly to ensure it remains relevant and effective, with updates prompted by changes in systems, regulations, or after security incidents. The organization also incorporates lessons learned from both internal and external breaches, which helps to improve the training's effectiveness.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with inadequate role-based training is that personnel may be ill-prepared to handle their information security responsibilities, leading to increased vulnerabilities and a higher likelihood of security incidents. Without proper training, employees might not recognize or respond appropriately to security threats, resulting in data breaches, system compromises, and other security incidents that could cause significant harm to the organization.

### Control Identifier: MA-2

Control Description:

The MA-2 control requires organizations to schedule, document, and review records of maintenance, repair, and replacement on system components according to manufacturer or vendor specifications and/or organizational requirements. This includes approving and monitoring all maintenance activities, whether performed on-site or remotely, and requiring explicit approval for the removal of system components for off-site maintenance. The control also mandates the sanitization of equipment to remove sensitive information before off-site maintenance, and the verification of potentially impacted controls after maintenance activities. The information recorded in maintenance logs includes details such as the date and time of maintenance, descriptions of work performed, names of individuals involved, and the components or equipment serviced.

Assessment Findings:

The assessment determined that the organization has effectively implemented the MA-2 control. Maintenance activities are scheduled and documented in accordance with organizational requirements, and all activities are approved and monitored by designated personnel. The organization ensures that system components are sanitized before they are sent off-site for maintenance, and thorough checks are performed to verify the proper functioning of controls after maintenance actions. The maintenance records include all necessary details, including the description of maintenance performed, the identities of personnel involved, and the equipment serviced or replaced.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with inadequate controlled maintenance is that organizational systems may degrade over time, leading to increased security vulnerabilities, system failures, and operational disruptions. Without regular and well-documented maintenance, systems are more likely to become outdated, susceptible to attacks, or prone to failures that could disrupt operations and compromise security.

### Control Identifier: AT-2

Control Description:

The AT-2 control requires organizations to provide security and privacy literacy training to system users, including managers, senior executives, and contractors. The training must be delivered as part of initial training for new users and at an organization-defined frequency thereafter. Additionally, training should be provided when required by system changes or after significant security events. Organizations are also required to employ various techniques to increase security and privacy awareness, update training content regularly, and incorporate lessons learned from internal or external security incidents or breaches into the training program.

Assessment Findings:

The assessment confirmed that the organization has effectively implemented the AT-2 control. Security and privacy literacy training is provided to all system users during onboarding and is refreshed periodically as required by organizational policy. The training content is regularly updated to reflect changes in systems, policies, and lessons learned from security incidents. The organization uses a variety of awareness techniques, such as email advisories, posters, and logon screen messages, to reinforce key security concepts and ensure ongoing awareness among all personnel.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with inadequate literacy training and awareness is that personnel may inadvertently compromise the security of the organization’s systems due to a lack of knowledge and understanding of security risks and policies. This can lead to increased vulnerabilities, security breaches, and other incidents that could have serious consequences for the organization.

### Control Identifier: MA-3

Control Description:

The MA-3 control requires organizations to approve, control, and monitor the use of system maintenance tools. Additionally, it mandates the periodic review of previously approved maintenance tools to ensure they remain relevant, secure, and supported. This control addresses the security-related risks associated with maintenance tools that are used specifically for diagnostic and repair actions on organizational systems but are not within the system authorization boundaries. Maintenance tools can include hardware, software, and firmware items and may be pre-installed, brought in with maintenance personnel, cloud-based, or downloaded from a website.

Assessment Findings:

The assessment confirmed that the organization has effectively implemented the MA-3 control. Maintenance tools are approved, controlled, and monitored according to organizational policy. Periodic reviews are conducted to ensure that outdated or unsupported tools are withdrawn from use. Only authorized personnel are allowed to use these tools, and they are vetted to ensure they do not introduce security risks into the organization's environment.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with improper management of maintenance tools is unauthorized access or compromise during maintenance activities. Unauthorized individuals could gain access to sensitive systems, or insecure tools and techniques could be used, leading to a compromise of the system.

### Control Identifier: CM-6

Control Description:

The CM-6 control requires organizations to establish, document, and enforce configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements. This includes:

Establishing and documenting configuration settings.

Implementing the configuration settings.

Identifying, documenting, and approving any deviations from established configuration settings.

Monitoring and controlling changes to the configuration settings.

Configuration settings refer to the parameters that can be changed in the hardware, software, or firmware components of the system that affect the security and privacy posture or functionality of the system. Common secure configurations, such as Security Content Automation Protocol (SCAP) standards, provide recognized benchmarks for secure configuration settings.

Assessment Findings:

The assessment confirmed that the organization has effectively implemented the CM-6 control. Configuration settings across all IT products are enforced and maintained according to the organization's secure configuration guidelines. Deviations from these settings are documented and require approval based on operational requirements. The organization continuously monitors and controls any changes to the configuration settings to ensure the security posture is not compromised.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with improper configuration settings is security incidents caused by misconfigurations or insecure settings. This could lead to vulnerabilities being introduced into the system.

### Control Identifier: AU-8

Control Description:

The AU-8 control requires organizations to use internal system clocks to generate time stamps for audit records and to ensure that time stamps:

Are recorded with a granularity of time measurement defined by the organization.

Use Coordinated Universal Time (UTC), have a fixed local time offset from UTC, or include the local time offset as part of the time stamp.

Time stamps generated by the system include both date and time, and accurate time stamps are critical for correlating events, investigating incidents, and supporting security capabilities such as access control and identification and authentication. The granularity of time measurements refers to the degree of synchronization between system clocks and reference clocks, which is essential for maintaining consistent and accurate time records across the organization.

Assessment Findings:

The assessment confirmed that the organization has effectively implemented the AU-8 control. Internal system clocks are used to generate time stamps for audit records, and these time stamps meet the organization-defined granularity of time measurement. The time stamps are recorded in UTC or with a fixed local time offset, ensuring consistency across all systems.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with improper time stamp management is the presence of inaccurate or inconsistent time stamps on audit records. This could lead to difficulties in correlating events, investigating incidents, and responding effectively to security threats.

### Control Identifier: PS-4

Control Description:

The PS-4 control requires that, upon the termination of an individual's employment, the organization must:

Disable system access within a defined time period.

Terminate or revoke any authenticators and credentials associated with the individual.

Conduct exit interviews that include a discussion of specified information security topics.

Retrieve all security-related organizational system-related property.

Retain access to organizational information and systems formerly controlled by the terminated individual.

System property includes hardware authentication tokens, system administration technical manuals, keys, identification cards, and building passes. Exit interviews are crucial to ensure that terminated individuals understand the security constraints imposed upon them as former employees and that all system-related property is properly accounted for. The timely execution of termination actions is essential, especially for individuals terminated for cause.

Assessment Findings:

The assessment confirmed that the organization has effectively implemented the PS-4 control. Upon termination, the organization promptly disables system access, revokes all credentials, conducts comprehensive exit interviews covering critical security topics, and retrieves all relevant security-related organizational property. Additionally, the organization retains access to information and systems previously controlled by the terminated individual.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with personnel termination is unauthorized access to Controlled Unclassified Information (CUI) by former or transferred employees.

### Control Identifier: IR-4

Control Description:

The IR-4 control requires that the organization implement an incident handling capability that:

Is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.

Coordinates incident handling activities with contingency planning activities.

Incorporates lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implements the resulting changes accordingly.

Ensures that the rigor, intensity, scope, and results of incident handling activities are comparable and predictable across the organization.

Incident handling capabilities are essential for managing and mitigating security incidents. Organizations must consider incident response during the definition, design, and development of mission and business processes and systems. Incident-related information can come from various sources, including audit monitoring, physical access monitoring, network monitoring, user or administrator reports, and reported supply chain events. Effective incident handling requires coordination among various organizational entities, such as system owners, human resources, physical security offices, and legal departments.

Assessment Findings:

The assessment confirmed that the organization has effectively implemented the IR-4 control. The organization has a comprehensive incident handling capability that is well-coordinated with contingency planning activities. The organization regularly updates incident response procedures based on lessons learned from incidents, ensuring continuous improvement in its incident handling practices.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with incident handling is the inability to effectively respond to security incidents.

### Control Identifier: SC-12

Control Description:

The SC-12 control requires that the organization establish and manage cryptographic keys whenever cryptography is employed within the system, in accordance with the organization-defined key management requirements. These requirements include key generation, distribution, storage, access, and destruction. Cryptographic key management and establishment can be performed using either manual procedures or automated mechanisms, supported by manual procedures. The organization defines these key management requirements to comply with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines. Additionally, the organization must manage trust stores to ensure that only approved trust anchors are part of these trust stores, which include both externally visible certificates and those related to internal system operations. NIST’s Cryptographic Module Validation Program (CMVP) and Cryptographic Algorithm Validation Program (CAVP) provide further guidance on validated cryptographic modules and algorithms suitable for key management and establishment.

Assessment Findings:

The assessment confirmed that the organization has implemented the SC-12 control effectively. The organization has established and manages cryptographic keys according to its defined requirements, which align with the necessary legal and regulatory standards. Trust stores are managed to include only approved and validated trust anchors, ensuring the secure handling of cryptographic keys throughout their lifecycle.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with cryptographic key establishment and management is unauthorized access due to compromised or poorly managed cryptographic keys.

### Control Identifier: AC-2

Control Description:

The AC-2 control requires the organization to define and document the types of accounts allowed and specifically prohibited for use within the system. The control mandates the assignment of account managers, the specification of prerequisites and criteria for group and role membership, the authorization of system users, and the management of access authorizations for each account. Additionally, it requires organizations to monitor account usage, notify account managers of any changes, authorize access based on valid authorization, review accounts for compliance, and establish processes for changing shared or group account authenticators when necessary. The account management processes must be aligned with personnel termination and transfer processes to ensure security and proper management.

Assessment Findings:

The assessment confirmed that the organization has implemented the AC-2 control effectively. The organization has documented and defined account types, established clear processes for account creation, modification, and termination, and aligned these processes with personnel changes. Access privileges are regularly reviewed, and any necessary changes are implemented promptly. The organization also monitors account usage to ensure compliance with established policies and procedures.

Assessment Status: Implemented

Associated Risk:

Without proper account management, unauthorized users, processes, or devices could gain access to the system. Specific risks include:

Orphaned Accounts: Accounts of former employees or contractors not being disabled, allowing continued access to sensitive systems.

Weak or Default Credentials: Lack of enforcement for strong password policies, allowing attackers to exploit weak or default passwords.

Unmonitored Accounts: Inactive accounts not regularly monitored or removed, potentially being hijacked by malicious actors.

Privilege Escalation: Users having more access than necessary, increasing the risk of privilege escalation attacks.

### Control Identifier: AC-3

Control Description:

The AC-3 control requires the enforcement of approved authorizations for logical access to information and system resources in accordance with applicable access control policies. Access control policies regulate access between active entities (e.g., users or processes acting on behalf of users) and passive entities (e.g., devices, files, records) within organizational systems. This control encompasses the enforcement of authorized access at the system level and, where applicable, at the application and service level to enhance information security and privacy. While this control focuses on logical access, it is distinct from physical access controls, which are covered under the Physical and Environmental Protection (PE) family.

Assessment Findings:

The assessment confirmed that the organization has implemented the AC-3 control effectively. The organization enforces approved access authorizations for system resources in line with its access control policies. Access control mechanisms are applied at both the system and application levels, ensuring that only authorized users can access sensitive data and systems. The organization has established robust mechanisms to prevent unauthorized access, thereby enhancing the security of its information systems.

Assessment Status: Implemented

Associated Risk:

The primary and most severe threat addressed by this control is unauthorized access. Specific risks include:

Unauthorized Users: Individuals or processes could gain access to sensitive systems and data without proper authorization, potentially leading to data breaches, unauthorized data manipulation, or system compromise.

Internal Threats: Even authorized users could exceed their access rights, leading to unintentional or malicious data alteration.

External Attacks: Unauthorized external entities could exploit vulnerabilities to access the system and compromise data integrity or confidentiality.

### Control Identifier: AC-14

Control Description:

The AC-14 control requires organizations to identify specific user actions that can be performed on the system without identification or authentication, consistent with organizational mission and business functions. These actions should be documented with supporting rationale in the system's security plan. The intent is to allow certain limited actions, such as accessing public websites or receiving calls on mobile devices, without requiring identification or authentication when such actions do not pose a security risk. This control does not apply to situations where identification and authentication have already occurred but rather to scenarios where these steps are bypassed for specified actions.

Assessment Findings:

The assessment confirmed that the organization has implemented the AC-14 control effectively. The organization has identified and documented actions that can be performed without identification or authentication in the system’s security plan, consistent with mission requirements. These actions are limited to non-sensitive activities where the risk of bypassing identification or authentication is minimal. The control is in place, ensuring that privileged credentials are not unnecessarily exposed.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with this control is the unnecessary exposure of privileged accounts during routine, non-security-related tasks. Specific risks include:

Exposure of Privileged Accounts: Performing nonsecurity functions with privileged accounts may expose high-value credentials to potential compromise.

Unauthorized Access: If privileged accounts are compromised, attackers could gain unauthorized access to sensitive systems, escalate privileges, and cause significant damage.

Data Breaches: Compromised privileged accounts could lead to unauthorized data access, resulting in data breaches, operational disruptions, and financial losses.

### Control Identifier: AC-17(1)

Control Description:

The AC-17(1) control requires organizations to employ automated mechanisms to monitor and control remote access methods. The purpose is to detect attacks and ensure compliance with remote access policies by auditing the connection activities of remote users across various system components, including servers, notebook computers, workstations, smartphones, and tablets. Audit logging for remote access is enforced by AU-2, with audit events defined in AU-2a.

Assessment Findings:

The assessment confirmed that the organization has implemented the AC-17(1) control effectively. Automated mechanisms are in place to monitor and control remote access methods, ensuring that all remote access activities are logged and analyzed for compliance with organizational policies. These mechanisms are designed to detect unauthorized access attempts and to ensure that only authorized users can access the system remotely.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with this control is the unauthorized remote execution of privileged commands and access to security-relevant information. Specific risks include:

Unauthorized Access: Unauthorized individuals could gain remote access to execute privileged commands or view sensitive information, leading to potential security incidents.

Data Breaches: Unauthorized access could result in data breaches, unauthorized data manipulation, or the compromise of critical systems.

Operational Disruption: Unauthorized changes to critical systems could cause operational disruptions, resulting in financial and reputational damage to the organization.

### Control Identifier: AC-17

Control Description:

The AC-17 control requires organizations to establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed. Additionally, each type of remote access must be authorized before any connection is permitted. Remote access refers to accessing organizational systems through external networks such as the Internet. This includes methods like dial-up, broadband, and wireless. Organizations typically use encrypted Virtual Private Networks (VPNs) to ensure the confidentiality and integrity of remote connections. However, while VPNs secure data in transit, they do not inherently improve the availability of connections and may limit the monitoring of network traffic for malicious activity.

Assessment Findings:

The assessment verified that the AC-17 control has been fully implemented. The organization has established comprehensive usage restrictions and configuration requirements for all forms of remote access, which are well-documented. Additionally, all types of remote access connections require authorization before they are established, ensuring that only approved users can connect remotely to the system.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with this control is unauthorized access and the potential compromise of the system via remote access sessions. Specific risks include:

Unauthorized Access: Unauthorized users could gain remote access to the organization's systems through unmonitored or poorly controlled sessions.

Data Breaches: Unauthorized access could result in data breaches, unauthorized data manipulation, or system compromise.

Operational Disruption: Unauthorized changes to critical systems could lead to operational disruptions, resulting in financial and reputational damage to the organization.

### Control Identifier: AC-6

Control Description:

The AC-6 control requires organizations to employ the principle of least privilege, which limits access for users (or processes acting on behalf of users) to only those resources necessary to accomplish their assigned tasks. This principle applies not only to individual users but also to system processes, ensuring that they operate with the minimum privileges necessary to perform their functions. The principle of least privilege is implemented during the development, implementation, and operation of organizational systems. Organizations consider creating additional processes, roles, and accounts as needed to enforce this principle effectively.

Assessment Findings:

The assessment confirmed that the AC-6 control is fully implemented within the organization. The principle of least privilege is consistently applied across all levels of the organization, including specific duties and system processes. Access rights are carefully managed and regularly reviewed to ensure that users and processes do not have more access than is necessary for their assigned tasks. This minimizes the risk of unauthorized access to sensitive systems and data.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with this control is excessive or unnecessary access to systems and data. Specific risks include:

Excessive Access Rights: Users or processes may have more access rights than necessary, increasing the likelihood of unauthorized access to sensitive data and systems.

Data Breaches: Excessive privileges could lead to data breaches if unauthorized users access or misuse critical systems.

Privilege Escalation: Malicious actors could exploit unnecessary access rights to escalate privileges, gaining control over more sensitive parts of the system.

### Control Identifier: AC-5

Control Description:

The AC-5 control requires organizations to identify and document duties that must be separated to mitigate the risk of fraud or misuse of privileges. This involves defining system access authorizations that enforce the separation of duties. The goal is to prevent a single individual from having control over all aspects of a critical process, which could lead to unauthorized actions. Separation of duties ensures that tasks and responsibilities are divided among different individuals or roles, reducing the risk of malevolent activity without collusion.

Assessment Findings:

The assessment confirmed that the AC-5 control is implemented and functioning as intended. Duties requiring separation have been identified and documented, and system access authorizations have been defined accordingly to enforce these separations. The organization has effectively divided mission-critical functions and support functions among different individuals or roles, ensuring that no single individual has excessive control over any critical process.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with this control is the potential for fraud or malicious activity if duties are not adequately separated. Specific risks include:

Fraud and Malicious Activity: A single individual with excessive control could manipulate processes or data without detection.

Errors and Oversights: Lack of separation may lead to unintentional errors that could go unchecked, resulting in significant operational or financial impacts.

Lack of Oversight: Without proper oversight, unauthorized transactions or data manipulations could occur, leading to significant damage.

### Control Identifier: AC-20

Control Description:

The AC-20 control requires organizations to establish and enforce terms and conditions for the use of external systems that access organizational systems or process, store, or transmit organizational data. External systems include any systems not under the direct control of the organization, such as personally-owned devices, contractor-managed systems, or systems operated by other organizations. Organizations may choose to prohibit the use of certain external systems or apply specific restrictions to ensure the security of their network and data.

Assessment Findings:

The assessment confirmed that the AC-20 control is implemented and functioning as intended. The organization has established clear terms and conditions for the use of external systems, ensuring that only authorized and secure external systems can connect to the organizational network. These terms are consistent with trust relationships and ensure that external systems comply with organizational security policies.

Assessment Status: Implemented

Associated Risk:

The primary risk associated with this control is the potential for unauthorized or insecure external systems to connect to the organization's network. Specific risks include:

Unauthorized Access: External systems may not be subject to the same security controls, leading to potential unauthorized access to organizational systems and data.

Introduction of Vulnerabilities: Insecure external systems could introduce malware or other security vulnerabilities into the organizational network.

Data Breaches: External systems processing or storing organizational data may not have adequate protections, increasing the risk of data breaches.

**3.3 Residual Risks**

After implementing the required security controls, some residual risks remain due to the nature of the environment, the complexity of the systems, and operational needs. These risks are documented below along with the rationale for their acceptance and any compensating controls or planned mitigations.

Risk of Unauthorized Access via External Systems

Residual Risk: Despite the implementation of AC-20 (Use of External Systems) and associated controls, there remains a low residual risk that authorized external systems could be compromised and subsequently used to gain unauthorized access to the organization's internal network.

Rationale for Acceptance: The organization has implemented stringent controls and monitoring mechanisms to manage and control external access. The remaining risk is considered acceptable due to the high level of trust in the external systems and the compensating controls in place, such as encrypted VPN connections and continuous monitoring of external access.

Compensating Controls:

Regular review and updating of external system access policies.

Enhanced monitoring and logging of external connections to detect anomalies.

Planned Mitigations:

Periodic audits of external system security configurations.

Further integration of multi-factor authentication (MFA) for all external access points.

Risk of Inadequate Time Synchronization (AU-8 Time Stamps)

Residual Risk: While time synchronization controls have been implemented, there remains a moderate risk that minor discrepancies in time stamps could impact the correlation of audit records across systems, especially during incident investigations.

Rationale for Acceptance: The risk is minimized by the use of authoritative time sources and frequent synchronization checks. The likelihood of significant discrepancies is low, and the potential impact is limited to forensic activities where exact time correlation is critical.

Compensating Controls:

Use of multiple synchronized time sources to ensure consistency.

Regular validation of time settings across critical systems.

Planned Mitigations:

Implementation of tighter synchronization intervals for systems handling sensitive data.

Automated alerts for any detected time discrepancies beyond acceptable thresholds.

Risk of Insider Threats due to Separation of Duties (AC-5)

Residual Risk: Although separation of duties (AC-5) is enforced, there is a low residual risk that collusion between individuals could bypass these controls, leading to potential fraud or unauthorized actions.

Rationale for Acceptance: The likelihood of collusion is mitigated by strict access controls, regular audits, and the organizational culture of accountability. The risk is accepted due to the high cost and operational complexity of implementing additional controls beyond those already in place.

Compensating Controls:

Continuous monitoring and logging of high-risk activities.

Regular rotation of duties among personnel to minimize the opportunity for collusion.

Planned Mitigations:

Enhanced auditing procedures focusing on high-risk transactions and activities.

Implementation of behavioral analysis tools to detect potential insider threats.

Risk of Unauthorized Privileged Access (AC-6 Least Privilege)

Residual Risk: Despite the enforcement of least privilege (AC-6), there remains a low to moderate risk that users may have more access rights than necessary, potentially leading to unauthorized access to sensitive data.

Rationale for Acceptance: The residual risk is deemed acceptable due to the existing access controls and the low likelihood of privilege misuse. The organization has implemented role-based access controls (RBAC) and regular reviews of access rights, which significantly reduce the risk.

Compensating Controls:

Regular access reviews and recertification processes.

Immediate revocation of access rights upon role changes or termination.

Planned Mitigations:

Implementation of automated tools to enforce least privilege dynamically.

More frequent audits of high-privilege accounts and their activities.

**4. Recommendations**

**4.1 Remediation Actions**

To address the identified vulnerabilities and reduce the residual risks in the environment, the following remediation actions are recommended. These actions include implementing additional controls, strengthening existing controls, and modifying system configurations to enhance the overall security posture.

Enhancing External System Controls (Related to AC-20 Use of External Systems)

Recommendation: Implement a more rigorous vetting process for external systems that connect to the organization's network. This includes requiring detailed security assessments for any third-party systems before they are granted access and mandating compliance with organizational security standards.

Action Steps:

Develop and enforce stricter terms and conditions for external system access.

Conduct security assessments and penetration testing on all external systems before approval.

Increase the frequency of audits on connections established through external systems.

Expected Outcome: Reduced risk of unauthorized or insecure external systems connecting to the internal network, thereby minimizing the potential for data breaches or system compromise.

Improving Time Synchronization Accuracy (Related to AU-8 Time Stamps)

Recommendation: Tighten the time synchronization process by reducing the intervals between synchronization events and ensuring that all systems use multiple redundant time sources to avoid discrepancies.

Action Steps:

Implement tighter synchronization intervals for systems that handle critical and sensitive data.

Deploy additional time servers to create redundancy and improve accuracy.

Configure automated alerts for any time discrepancies beyond a set threshold.

Expected Outcome: Enhanced accuracy and consistency of time stamps across systems, improving the reliability of audit records and incident investigations.

Strengthening Separation of Duties (Related to AC-5 Separation of Duties)

Recommendation: Strengthen the enforcement of separation of duties by implementing automated checks and balances within the system to detect and prevent any violations of established duties.

Action Steps:

Deploy automated systems that can monitor and enforce separation of duties in real-time.

Increase the frequency of internal audits specifically targeting potential separation of duty violations.

Implement stricter controls around high-risk roles, including enhanced background checks and continuous monitoring.

Expected Outcome: Reduced likelihood of fraud or malicious activities by ensuring that no single individual has excessive control over critical processes.

Tightening Access Privileges (Related to AC-6 Least Privilege)

Recommendation: Implement more granular control over access privileges by utilizing advanced role-based access control (RBAC) systems and automated privilege management tools.

Action Steps:

Implement automated privilege management tools that dynamically adjust access rights based on current roles and responsibilities.

Conduct more frequent access reviews, particularly for high-privilege accounts, to ensure compliance with the principle of least privilege.

Provide additional training for administrators and users on the importance of least privilege and the proper handling of privileged accounts.

Expected Outcome: Minimized risk of unauthorized access or privilege escalation, leading to better protection of sensitive data and critical systems.

Enhanced Monitoring and Control of Remote Access (Related to AC-17 Remote Access)

Recommendation: Improve the monitoring and control of remote access by implementing advanced security measures such as multi-factor authentication (MFA) for all remote access points and continuous monitoring of remote sessions.

Action Steps:

Mandate the use of MFA for all remote access connections to the organization's network.

Deploy continuous monitoring tools that can detect and respond to suspicious remote access activities in real-time.

Review and update remote access policies to reflect current threats and best practices.

Expected Outcome: Improved security of remote access connections, reducing the risk of unauthorized access and the potential compromise of sensitive information.

Enhancing Cryptographic Key Management (Related to SC-12 Cryptographic Key Establishment and Management)

Recommendation: Strengthen cryptographic key management practices by ensuring that all keys are managed in accordance with best practices and that automated tools are used to manage key lifecycle activities.

Action Steps:

Deploy automated key management solutions that enforce best practices for key generation, distribution, storage, and destruction.

Regularly audit cryptographic key management processes to identify and address any weaknesses.

Train personnel involved in key management on the latest best practices and threats related to cryptographic keys.

Expected Outcome: Reduced risk of key compromise or mismanagement, leading to enhanced protection of encrypted data and overall system security.

Updating System Configuration Management (Related to CM-6 Configuration Settings)

Recommendation: Regularly review and update system configuration settings to ensure they remain aligned with the latest security standards and operational requirements.

Action Steps:

Implement automated tools that continuously monitor and enforce secure configuration settings across all systems.

Conduct regular audits to ensure that all system configurations comply with the organization's security policies.

Update configuration baselines to reflect any changes in the threat environment or operational needs.

Expected Outcome: Enhanced system security through consistent enforcement of secure configuration settings, reducing the likelihood of misconfigurations leading to security incidents.

**4.2 Prioritization of Actions**

To effectively address the vulnerabilities and mitigate the associated risks, the remediation actions should be prioritized based on the severity and potential impact of the risks. The following prioritization is suggested to guide the implementation of the recommended remediation actions:

Immediate Actions (High Priority)

These actions address the most critical vulnerabilities that pose an immediate threat to the organization's security. They should be implemented as soon as possible to prevent potential security breaches.

Enhancing External System Controls (Related to AC-20 Use of External Systems)

Rationale: Unauthorized or insecure external systems connecting to the network present a significant risk of data breaches and system compromise. Addressing this issue immediately will reduce the likelihood of external threats gaining access to internal systems.

Action: Implement a rigorous vetting process and enforce stricter terms and conditions for external system access.

Tightening Access Privileges (Related to AC-6 Least Privilege)

Rationale: Excessive or unnecessary access rights significantly increase the risk of unauthorized access to sensitive data and systems. Reducing privileges to the minimum necessary for job functions is critical to minimizing the potential for data breaches and misuse.

Action: Implement advanced role-based access control (RBAC) systems and conduct immediate access reviews.

Enhanced Monitoring and Control of Remote Access (Related to AC-17 Remote Access)

Rationale: Unauthorized remote access can lead to severe security incidents, including unauthorized command execution and data breaches. Strengthening remote access controls, particularly through the use of multi-factor authentication (MFA), is vital.

Action: Mandate MFA for all remote access connections and deploy continuous monitoring tools.

Near-Term Actions (Medium Priority)

These actions should be completed in the near term (within the next few months) to continue improving the organization's security posture after the most critical risks are addressed.

Improving Time Synchronization Accuracy (Related to AU-8 Time Stamps)

Rationale: Accurate and consistent time stamps are essential for reliable audit records and incident investigations. Improving time synchronization reduces the risk of errors in incident response and auditing.

Action: Tighten synchronization intervals and deploy additional time servers for redundancy.

Updating System Configuration Management (Related to CM-6 Configuration Settings)

Rationale: Misconfigurations can lead to security incidents and vulnerabilities. Regularly updating and enforcing secure configuration settings will help maintain a strong security posture.

Action: Implement automated monitoring tools for configuration settings and conduct regular audits.

Enhancing Cryptographic Key Management (Related to SC-12 Cryptographic Key Establishment and Management)

Rationale: Poorly managed cryptographic keys can lead to unauthorized access and data breaches. Strengthening key management practices ensures the integrity and confidentiality of encrypted data.

Action: Deploy automated key management solutions and conduct regular audits of key management processes.

Long-Term Actions (Low Priority)

These actions, while still important, address less immediate risks and can be planned for implementation over the long term (within the next year).

Strengthening Separation of Duties (Related to AC-5 Separation of Duties)

Rationale: Separation of duties is crucial for preventing fraud and ensuring accountability. However, since it primarily addresses internal risks, it can be implemented over a longer time frame as part of a broader internal controls enhancement initiative.

Action: Deploy automated systems to monitor separation of duties and increase the frequency of internal audits.

This prioritization allows the organization to focus on addressing the most severe risks first, ensuring that critical vulnerabilities are mitigated promptly while planning for longer-term improvements to the overall security posture.

**5. Conclusion**

The security assessment of the system has revealed a generally robust security posture, with most controls effectively implemented and in place. The organization has demonstrated a commitment to maintaining a secure environment, with many critical controls fully operational and continuously monitored. However, several vulnerabilities have been identified that could pose significant risks if not addressed promptly.

**Overall Security Posture:** The system's security posture is strong in several areas, including access control, audit logging, and configuration management. These controls provide a solid foundation for the system's security framework. The consistent application of security controls, along with regular monitoring and auditing, has helped mitigate many common threats.

However, some areas require immediate attention to prevent potential exploitation. Notably, risks associated with external system access, least privilege enforcement, and remote access controls need to be addressed to ensure the ongoing security of the system. While these vulnerabilities are currently mitigated to some extent by existing controls, their presence indicates potential gaps that could be exploited by determined adversaries.

**Importance of Addressing Identified Vulnerabilities:** Addressing the identified vulnerabilities is crucial to maintaining the integrity, confidentiality, and availability of the system. Unaddressed, these vulnerabilities could lead to unauthorized access, data breaches, and potential system compromises, resulting in severe operational, financial, and reputational damage.

The organization must prioritize remediation efforts based on the severity of the risks. Immediate actions should focus on enhancing controls over external systems, tightening access privileges, and improving remote access security. Near-term and long-term actions should continue to build on these efforts, ensuring that all vulnerabilities are fully addressed.

**Steps to Maintain System Security:** To maintain and strengthen the system’s security, the following steps will be taken:

* **Immediate Remediation:** The organization will promptly implement the highest-priority actions, particularly those related to external systems and access controls, to close the most critical security gaps.
* **Ongoing Monitoring:** Continuous monitoring will be enhanced, particularly for remote access and privileged account usage, to detect and respond to potential security incidents in real-time.
* **Regular Audits and Assessments:** The organization will conduct regular security audits and risk assessments to ensure that new vulnerabilities are identified and addressed in a timely manner.
* **Policy and Procedure Updates:** Security policies and procedures will be reviewed and updated regularly to reflect the latest best practices and regulatory requirements, ensuring that the organization’s security posture evolves with the threat landscape.
* **Training and Awareness:** Ongoing security training and awareness programs will be strengthened to ensure that all personnel understand their roles and responsibilities in maintaining system security.

By taking these steps, the organization will continue to protect its assets, data, and operations from evolving threats, ensuring that the system remains secure and resilient in the face of potential challenges.