|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Control | Weaknesses | Responsible  Office/ Organization | Resource Estimate  (funded/ unfunded/ reallocation) | Scheduled Completion Date | Milestones with Interim Completion Dates | Changes to Milestones | How was the weakness identified? | Status *(Ongoing or Complete)* |
| AC-4 | **The organization lacks mechanisms for enforcing approved authorizations for controlling the flow of information within the system and between connected systems based on predefined policies. This can lead to unauthorized data transfers or breaches of security/privacy policies.** | **The Information Security Office (ISO) or a specific team responsible for security controls implementation.** | **Funded. Resources required include software and hardware for boundary protection, packet filtering, and potentially advanced cross-domain solutions if required by the organization’s architecture.** | **Final Completion Date: November 29, 2024** | **Assessment and Gap Analysis:**  **Completion Date: September 15, 2024**  **Description: Identify gaps in current information flow control mechanisms and assess the need for new hardware/software.**  **Policy Development and Approval:**  **Completion Date: September 30, 2024**  **Description: Develop organization-specific information flow control policies. Obtain necessary approvals from stakeholders.**  **Procurement of Tools/Devices:**  **Completion Date: October 15, 2024**  **Description: Purchase required boundary protection devices and filtering mechanisms.**  **Implementation of Enforcement Mechanisms:**  **Completion Date: October 30, 2024**  **Description: Install and configure boundary protection devices and filtering mechanisms to enforce information flow control policies.**  **Testing and Verification:**  **Completion Date: November 14, 2024**  **Description: Conduct testing to verify that information flow control is effectively enforced and that no unauthorized flows occur.**  **Final Review and Policy Enforcement:**  **Completion Date: November 29, 2024**  **Description: Conduct a final review of the implemented controls, update policies as necessary, and ensure full enforcement.** | **Document any delays or accelerations in the timeline. Adjustments might be necessary if, for example, procurement is delayed or testing uncovers additional needs.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AC-6 (9) | **Inadequate logging of privileged function executions.**  **Lack of analysis tools to detect misuse of privileged functions.**  **Potential risk of insider threats or advanced persistent threats due to unmonitored privileged function usage.** | **Information Security Office (ISO)**    **IT Department** | **Reallocation: Existing logging infrastructure and resources will be leveraged**  **Funded: Purchase of advanced logging and analysis tools**  **Estimated Cost: $80,000 for software acquisition and integration** | **Final Completion Date: November 29, 2024** | **Assessment of current logging capabilities will be completed by September 15, 2024, evaluating the current logging infrastructure to identify gaps in privileged function logging.**  **Procurement of logging and analysis tools is scheduled to be completed by September 30, 2024, where the necessary tools capable of logging and analyzing privileged functions will be acquired and configured.**  **Implementation of logging mechanisms will be finalized by October 15, 2024, with the deployment of mechanisms that capture all privileged function executions across the system.**  **Configuration of analysis and alerting mechanisms will be done by October 30, 2024, ensuring the setup of mechanisms to detect potential misuse of privileged functions.**  **Testing and verification will be conducted by November 14, 2024, to ensure that logging and analysis tools are accurately capturing and reporting privileged function usage.**  **The project will conclude with a final review and policy enforcement by November 29, 2024, ensuring that the implemented controls are fully effective.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AC-7 | **No current enforcement of limits on unsuccessful logon attempts**  **Lack of automated actions when the maximum number of unsuccessful logon attempts is exceeded**  **Potential vulnerability to brute force attacks due to lack of protective measures** | **Information Security Office (ISO)**    **IT Department** | **Reallocation: Utilize existing IT resources for implementation and configuration**  **Funded: Purchase of additional security software, if needed, for enhanced logon attempt management**  **Estimated Cost: $50,000 for software upgrades and implementation** | **Final Completion Date: November 29, 2024** | **Enforcement of a limit on unsuccessful logon attempts will be established by September 15, 2024. This will include defining the number of allowed attempts and the time period within which they must occur.**  **Automated actions, such as locking accounts or notifying administrators after unsuccessful attempts, will be configured by September 30, 2024.**  **Implementation of additional security measures, such as delay algorithms or secret questions, will be completed by October 15, 2024, to prevent brute force attacks.**  **Testing and verification of the implemented controls will be conducted by October 30, 2024, ensuring that the system responds appropriately to unsuccessful logon attempts.**  **Final review and enforcement of the logon attempt policies will be completed by November 29, 2024, making sure that all protective measures are fully operational.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AC-8 | **No existing system use notification message or banner displayed before system access**  **Lack of user acknowledgment of system usage conditions before logging on**  **Non-compliance with privacy and security notice requirements for publicly accessible systems** | **Information Security Office (ISO)**    **IT Department** | **Reallocation: Utilize current resources for implementing notification banners**  **Funded: Potential costs for customization and legal review of the notification content**  **Estimated Cost: $20,000 for customization and integration** | **Final Completion Date: November 29, 2024** | **Development and approval of the system use notification message or banner will be completed by September 15, 2024, ensuring it aligns with applicable laws, directives, and privacy guidelines.**  **Implementation of the notification banner across all user access points will be finalized by September 30, 2024, requiring users to acknowledge the conditions before system access.**  **Testing and verification of the notification system will be conducted by October 15, 2024, ensuring that it functions correctly and remains on screen until acknowledgment is received.**  **For publicly accessible systems, additional configurations to display system use information and references to monitoring will be implemented by October 30, 2024.**  **Final review and enforcement of the system use notification will be completed by November 29, 2024, ensuring compliance and effective user notification.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AC-11 | **Lack of automatic device lock after a defined period of inactivity**  **No requirement for users to manually lock devices before leaving them unattended**  **Insufficient implementation of identification and authentication procedures to reestablish access after a device lock** | **Information Security Office (ISO)**    **IT Department** | **Reallocation: Use existing IT infrastructure to implement device lock policies**  **Funded: Purchase and configure proximity-based locking devices (e.g., Bluetooth dongles)**  **Estimated Cost: $30,000 for procurement and deployment of proximity lock devices and software configuration** | **Final Completion Date: November 29, 2024** | **Configuration of the operating system to initiate an automatic device lock after 15 minutes of inactivity will be completed by September 15, 2024. This includes setting group policies across all devices to enforce the lockout time period.**  **Implementation of proximity-based locking mechanisms, such as Bluetooth dongles or similar devices, to automatically lock the system when the user moves away from the workstation will be done by September 30, 2024. This will involve integrating the proximity locks with existing security systems and ensuring compatibility.**  **Deployment of user training and policy updates to require manual device locking before leaving systems unattended will be finalized by October 15, 2024. This will ensure users are aware of and comply with the requirement to lock their devices.**  **Testing and verification of the implemented device lock mechanisms, including proximity locks and manual lock enforcement, will be conducted by October 30, 2024. This will ensure that all devices comply with the new security measures and that the device lock remains engaged until proper identification and authentication are provided.**  **Final review and enforcement of the device lock policy, including automatic and manual locking mechanisms, will be completed by November 29, 2024, ensuring full compliance and effective implementation across the organization.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AC-12 | **No existing mechanism to automatically terminate user sessions after a defined period of inactivity**  **Lack of enforcement of session termination following certain trigger events or conditions**  **Potential security risks due to sessions remaining active beyond the necessary timeframe** | **Information Security Office (ISO)**    **IT Department** | **Reallocation: Utilize existing system management tools to configure automatic session termination**  **Funded: Purchase of additional software if necessary to enforce specific trigger events**  **Estimated Cost: $25,000 for software procurement and implementation** | **Final Completion Date: November 29, 2024** | **Configuration of the system to automatically terminate user sessions after 30 minutes of inactivity will be completed by September 15, 2024. This will involve setting appropriate group policies and adjusting system configurations.**  **Implementation of session termination triggers, such as time-of-day restrictions or response to specific incidents, will be configured by September 30, 2024. This includes integrating the termination rules with existing incident response systems.**  **Testing and verification of the session termination mechanisms will be conducted by October 15, 2024, ensuring that sessions are correctly terminated under the defined conditions and that no unintended disruptions occur.**  **User training and policy updates will be deployed by October 30, 2024, ensuring that all users are aware of the new session termination rules and the implications for their workflow.**  **Final review and enforcement of the session termination policies will be completed by November 29, 2024, ensuring that the system is fully compliant with the AC-12 control requirements.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AC-17 | **No documented usage restrictions, configuration requirements, or implementation guidance for remote access**  **Lack of a formal authorization process for each type of remote access prior to allowing connections**  **Potential security vulnerabilities due to inadequate control and monitoring of remote access** | **Information Security Office (ISO)**    **IT Department** | **Reallocation: Leverage existing VPN infrastructure and security policies for implementation**  **Funded: Purchase of advanced monitoring tools to ensure secure and authorized remote access**  **Estimated Cost: $40,000 for additional monitoring and auditing software** | **Final Completion Date: November 29, 2024** | **Establishment and documentation of usage restrictions, configuration requirements, and implementation guidance for each type of remote access will be completed by September 15, 2024. This will include defining policies for VPN, broadband, wireless, and other remote connections, ensuring they align with organizational security standards.**  **Implementation of an encrypted Virtual Private Network (VPN) solution for all remote access types, ensuring confidentiality and integrity of remote connections, will be finalized by September 30, 2024. This step will also involve ensuring compliance with applicable laws and regulations.**  **Authorization processes for each type of remote access, including dial-up, broadband, wireless, and VPN, will be defined and enforced by October 15, 2024. This will involve establishing clear protocols for approving remote access and documenting all authorizations.**  **Deployment of monitoring and auditing tools to oversee all remote access connections and detect any unauthorized or suspicious activity will be completed by October 30, 2024. These tools will provide real-time insights into remote access activities.**  **Final review and enforcement of remote access policies and configurations will be completed by November 29, 2024, ensuring that all remote connections are secure, authorized, and compliant with the AC-17 control requirements.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AC-17(2) | **No implementation of cryptographic mechanisms to ensure confidentiality and integrity of remote access sessions**  **Potential vulnerability to unauthorized access or data interception during remote sessions**  **Lack of secure communication channels for remote access, leading to possible breaches of sensitive information** | **Information Security Office (ISO)**  **IT Department** | **Reallocation: Leverage existing infrastructure where possible, including current VPN solutions**  **Funded: Acquisition and deployment of advanced cryptographic tools such as Transport Layer Security (TLS) for remote sessions**  **Estimated Cost: $35,000 for additional cryptographic software and its implementation** | **Final Completion Date: November 29, 2024** | **Implementation of a Virtual Private Network (VPN) with strong encryption protocols, such as TLS, to protect the confidentiality and integrity of all remote access sessions will be completed by September 15, 2024. This step includes configuring existing VPNs to use robust cryptographic mechanisms.**  **Deployment of Transport Layer Security (TLS) across all remote access channels will be finalized by September 30, 2024. TLS will be configured to secure end-to-end communication for remote sessions, ensuring encryption of all transmitted data.**  **Testing and verification of the encryption mechanisms, including VPN and TLS configurations, will be conducted by October 15, 2024. This will ensure that all remote access sessions are encrypted and secure, with no vulnerabilities or weak points in the encryption protocols.**  **User training and policy updates on the new encryption protocols will be completed by October 30, 2024. This will involve educating users on the importance of encrypted remote sessions and ensuring compliance with the new protocols.**  **Final review and enforcement of the cryptographic controls for remote access will be completed by November 29, 2024, ensuring all remote sessions are secured and compliant with the AC-17(2) control requirements.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AC-17(3) | **Lack of a centralized approach to managing remote access through authorized network access control points**  **Potential vulnerabilities due to remote access connections bypassing managed control points**  **Increased attack surface due to multiple unmanaged access points** | **Information Security Office (ISO)**  **IT Department** | **Reallocation: Utilize existing network infrastructure to centralize access control points**  **Funded: Purchase of advanced access control systems and Trusted Internet Connections (TIC) compliance tools**  **Estimated Cost: $50,000 for procurement, deployment, and configuration of access control systems** | **Final Completion Date: November 29, 2024** | **Assessment of the current remote access infrastructure to identify unmanaged access points will be completed by September 15, 2024. This will involve mapping all existing remote access connections and determining where improvements are needed.**  **Implementation of a centralized approach to route all remote access through authorized and managed network access control points will be finalized by September 30, 2024. This will include integrating the existing network with a centralized access management system, ensuring compliance with the Trusted Internet Connections (TIC) initiative.**  **Configuration and deployment of advanced access control systems, including setting up Trusted Internet Connections (TIC) compliant tools, will be completed by October 15, 2024. This step will ensure that all remote access is routed through secure and managed points, reducing potential attack surfaces.**  **Testing and verification of the centralized remote access routing will be conducted by October 30, 2024, ensuring that all remote connections are properly routed and that no unauthorized access points are being used.**  **Final review and enforcement of the managed access control policy, including ongoing monitoring and auditing of access points, will be completed by November 29, 2024, ensuring compliance with AC-17(3) requirements and security best practices.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AC-18 | **No established configuration and connection requirements for wireless access**  **Lack of formal authorization process for wireless access types before connections are allowed**  **Potential security risks from unauthorized or improperly configured wireless connections** | **Information Security Office (ISO)**  **IT Department** | **Reallocation: Use existing network management tools and resources to implement wireless access controls**  **Funded: Purchase of advanced wireless access management and monitoring tools, if necessary**  **Estimated Cost: $45,000 for software procurement and configuration of wireless access controls** | **Final Completion Date: November 29, 2024** | **Development of configuration and connection requirements for each type of wireless access, including 802.11x, Bluetooth, and other wireless technologies, will be completed by September 15, 2024. This will involve setting secure parameters for wireless networks and establishing mutual authentication protocols.**  **Implementation of an authorization process for all wireless access types will be finalized by September 30, 2024. This process will ensure that no wireless connection is allowed without proper approval and configuration, reducing the risk of unauthorized access.**  **Deployment of wireless access management tools to enforce configuration and connection requirements will be completed by October 15, 2024. These tools will provide real-time monitoring and control over all wireless connections within the organization.**  **Testing and verification of wireless access controls, including the enforcement of authentication protocols and connection restrictions, will be conducted by October 30, 2024. This will ensure that all wireless access points comply with the established security requirements.**  **Final review and enforcement of the wireless access policy, including ongoing monitoring and regular audits of wireless connections, will be completed by November 29, 2024, ensuring full compliance with AC-18 requirements.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AC-19 | **No established configuration and connection requirements for organization-controlled mobile devices, particularly when they are outside of controlled areas**  **Lack of a formal authorization process for the connection of mobile devices to organizational systems**  **Potential security risks from unauthorized or improperly configured mobile device connections** | **Information Security Office (ISO)**  **IT Department** | **Reallocation: Use existing mobile device management (MDM) tools and resources for implementation**  **Funded: Purchase of additional security and management software, if necessary, for mobile devices**  **Estimated Cost: $60,000 for software procurement and enhanced mobile device management** | **Final Completion Date: November 29, 2024** | **Development of configuration and connection requirements for organization-controlled mobile devices, including security measures for when such devices are outside of controlled areas, will be completed by September 15, 2024. This includes setting policies for device encryption, authentication, and remote wipe capabilities.**  **Implementation of a formal authorization process for connecting mobile devices to organizational systems will be finalized by September 30, 2024. This process will involve ensuring that no mobile device is connected without proper approval and security configuration.**  **Deployment of a Mobile Device Management (MDM) solution to enforce configuration and connection requirements, as well as to monitor and manage mobile devices remotely, will be completed by October 15, 2024. The MDM solution will ensure that all mobile devices comply with the established security policies, even when they are outside of controlled areas.**  **Testing and verification of mobile device controls, including security configurations and connection authorizations, will be conducted by October 30, 2024. This will ensure that all mobile devices are secure and properly managed.**  **Final review and enforcement of the mobile device access control policy, including ongoing monitoring and regular audits of mobile device connections, will be completed by November 29, 2024, ensuring full compliance with AC-19 requirements.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AC-22 | **No designated individuals authorized to make information publicly accessible**  **Lack of training for individuals on ensuring that publicly accessible information does not contain nonpublic information**  **Insufficient review processes to prevent nonpublic information from being posted to publicly accessible systems**  **No regular review of publicly accessible content to ensure nonpublic information is not included** | **Public Affairs Office (PAO)**  **Information Security Office (ISO)** | **Reallocation: Use existing resources for training, review processes, and content management**  **Funded: Possible funding for additional content review tools or training programs**  **Estimated Cost: $20,000 for training programs and content management tools** | **Final Completion Date: November 29, 2024** | **Designation of individuals authorized to make information publicly accessible will be completed by September 15, 2024. This step includes identifying personnel across departments who will have the responsibility for managing publicly accessible content.**  **Training programs for authorized individuals to ensure they understand how to review and manage publicly accessible information without including nonpublic information will be established and completed by September 30, 2024.**  **Development and implementation of a content review process that requires all proposed content to be reviewed before posting to ensure it does not contain nonpublic information will be finalized by October 15, 2024. This will include setting up guidelines and procedures for content approval.**  **Implementation of regular reviews of publicly accessible content to ensure that no nonpublic information has been mistakenly included will be conducted by October 30, 2024. The frequency of these reviews will be determined by organizational needs and risks.**  **Final review and enforcement of the publicly accessible content management policy will be completed by November 29, 2024, ensuring all content posted is compliant with AC-22 requirements and that regular audits are in place.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AT-2(2) | **No existing literacy training program on recognizing and reporting potential indicators of insider threat**  **Increased risk of insider threats going undetected due to lack of awareness and reporting mechanisms** | **Human Resources (HR) Department**  **Information Security Office (ISO)** | **Reallocation: Utilize existing training resources and materials**  **Funded: Development and implementation of specialized training modules on insider threat detection**  **Estimated Cost: $30,000 for training development and delivery** | **Final Completion Date: November 29, 2024** | **Development of a comprehensive insider threat literacy training program, tailored to different roles within the organization (e.g., managers, general employees), will be completed by September 15, 2024. This program will include modules on recognizing behavioral indicators and reporting procedures.**  **Implementation of the insider threat training program across the organization will be finalized by September 30, 2024. Training sessions will be conducted both in-person and online, ensuring that all employees, including remote workers, receive the necessary training.**  **Creation of clear communication channels for employees and management to report potential indicators of insider threats will be established by October 15, 2024. This will include the development of reporting policies and procedures that are accessible to all staff.**  **Deployment of a training evaluation process, where the effectiveness of the insider threat training is assessed and improvements are made based on feedback, will be completed by October 30, 2024. This will ensure that the training remains relevant and effective.**  **Final review and integration of the insider threat awareness program into the organization's ongoing training schedule will be completed by November 29, 2024, ensuring that all employees regularly receive updated training on insider threat detection.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AU-2 | **No identification of the specific event types that the system is capable of logging**  **Lack of coordination with other organizational entities to guide event logging criteria**  **No specified event types or logging frequencies for the system**  **Inadequate rationale provided for the selected event types to support after-the-fact investigations**  **No established process for regularly reviewing and updating the event types being logged** | **Information Security Office (ISO)**  **Audit and Compliance Department** | **Reallocation: Utilize existing system logging tools and audit resources**  **Funded: Potential funding for advanced logging tools or enhancements if required**  **Estimated Cost: $40,000 for logging enhancements and audit integrations** | **Final Completion Date: November 29, 2024** | **Identification of the specific event types that the system is capable of logging will be completed by September 15, 2024. This will involve analyzing the current system's logging capabilities and mapping them to organizational security needs.**  **Coordination with other organizational entities, such as the audit and compliance departments, to establish criteria for event logging will be finalized by September 30, 2024. This step ensures that the event types selected for logging align with overall organizational objectives and compliance requirements.**  **Specification of event types for logging, including the frequency or specific situations requiring logging, will be completed by October 15, 2024. This will involve selecting critical events such as failed logons, security attribute changes, and data access that are crucial for security and audit purposes.**  **Development of a rationale for the selected event types, explaining why they are sufficient for supporting after-the-fact investigations, will be finalized by October 30, 2024. This rationale will be documented and reviewed by the audit and compliance team.**  **Implementation of a review process for regularly updating the event types being logged, based on organizational needs and changes in system usage, will be completed by November 29, 2024. This process will ensure that the event logging remains relevant and effective.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AU-3 | **Audit records do not consistently contain all required information, such as event type, time, location, source, outcome, and identity of involved individuals or entities**  **Potential privacy risks due to incomplete or improperly managed audit records**  **Lack of a standardized format for audit records across different systems** | **Information Security Office (ISO)**  **Audit and Compliance Department** | **Reallocation: Use existing audit tools and resources to enhance record content**  **Funded: Potential need for additional tools or updates to existing audit logging systems**  **Estimated Cost: $30,000 for software updates and training** | **Final Completion Date: November 29, 2024** | **Assessment of current audit records to identify gaps in the required information, such as event type, timestamp, source, outcome, and identities of individuals/entities, will be completed by September 15, 2024. This will involve a review of existing logs and audit trails.**  **Development and implementation of a standardized format for audit records that ensures all required information is captured consistently across systems will be finalized by September 30, 2024. This format will include mandatory fields for each required element.**  **Enhancement of audit logging systems to automatically capture and populate all necessary information in audit records will be completed by October 15, 2024. This may involve configuring or updating existing logging tools.**  **Deployment of training sessions for relevant staff on the importance of comprehensive audit records and the use of the standardized format will be conducted by October 30, 2024. This training will ensure that all personnel understand the requirements and procedures for audit logging.**  **Regular review and update of the audit record content, based on system changes or new requirements, will be established by November 29, 2024. This will include periodic audits to ensure compliance with AU-3 requirements and to identify any necessary adjustments.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AU-5 | **No established process to alert designated personnel in the event of an audit logging process failure**  **Lack of predefined actions to take when audit logging process failures occur, such as log storage capacity being exceeded**  **Potential for undetected failures in the audit logging process, leading to gaps in audit records** | **Information Security Office (ISO)**  **IT Department** | **Reallocation: Use existing monitoring and alerting tools within the IT infrastructure**  **Funded: Possible need for additional storage solutions or enhanced logging tools**  **Estimated Cost: $25,000 for additional storage solutions and software enhancements** | **Final Completion Date: November 29, 2024** | **Development and implementation of a process to automatically alert designated personnel, such as IT administrators and audit officers, within 15 minutes of an audit logging process failure, will be completed by September 15, 2024. This includes configuring existing monitoring systems to trigger alerts.**  **Establishment of predefined actions to be taken in response to specific types of audit logging process failures, such as storage capacity being exceeded or hardware errors, will be finalized by September 30, 2024. These actions may include overwriting the oldest logs, temporarily shutting down non-essential services, or initiating emergency log exports.**  **Testing and validation of the alerting process and predefined actions will be conducted by October 15, 2024, ensuring that all processes work as expected and that personnel receive alerts in a timely manner.**  **Deployment of additional storage solutions, if required, to prevent audit log storage capacity issues, will be completed by October 30, 2024. This will involve assessing current storage capacity and implementing scalable storage options.**  **Final review and integration of the audit logging failure response plan into the organization's overall incident response framework will be completed by November 29, 2024, ensuring comprehensive coverage of potential logging issues.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AU-6 | **No established process for regular review and analysis of system audit records for indications of inappropriate or unusual activity**  **Lack of a defined reporting structure for findings related to unusual or inappropriate activities**  **No process to adjust the frequency and scope of audit record reviews based on changes in risk or new information** | **Information Security Office (ISO)**  **Audit and Compliance Department** | **Reallocation: Use existing audit tools and monitoring systems**  **Funded: Potential need for advanced analysis tools or updates to audit review processes**  **Estimated Cost: $35,000 for software enhancements and training** | **Final Completion Date: November 29, 2024** | **Development and implementation of a process to regularly review and analyze system audit records, focusing on identifying organization-defined inappropriate or unusual activities, will be completed by September 15, 2024. The frequency of reviews will be determined based on organizational risk and system sensitivity.**  **Establishment of a clear reporting structure for findings from audit reviews, ensuring that they are promptly communicated to designated personnel, such as the incident response team or security officers, will be finalized by September 30, 2024.**  **Creation of a protocol to adjust the level of audit record review and analysis based on changes in risk, informed by law enforcement, intelligence, or other credible sources, will be completed by October 15, 2024. This protocol will ensure that audit reviews remain relevant and effective as new threats or vulnerabilities are identified.**  **Testing and validation of the audit record review and reporting processes will be conducted by October 30, 2024, to ensure that they function correctly and that any unusual activity is promptly detected and reported.**  **Final review and integration of the audit record review, analysis, and reporting processes into the organization's overall security and compliance framework will be completed by November 29, 2024, ensuring comprehensive coverage and responsiveness to potential risks.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AU-6(3) | **No process in place to analyze and correlate audit records across different repositories**  **Lack of organization-wide situational awareness due to isolated audit record repositories**  **Potential security risks due to incomplete understanding of events across the organization** | **Information Security Office (ISO)**  **Audit and Compliance Department** | **Reallocation: Use existing audit and monitoring tools to integrate audit records across repositories**  **Funded: Acquisition of centralized log management and correlation tools, if needed**  **Estimated Cost: $50,000 for centralized log management tools and integration services** | **Final Completion Date: November 29, 2024** | **Assessment of current audit record repositories to identify silos and integration opportunities will be completed by September 15, 2024. This will involve mapping all existing audit logs across different systems and identifying gaps in correlation.**  **Implementation of a centralized log management solution to aggregate and correlate audit records from different repositories across the organization will be finalized by September 30, 2024. This will enable organization-wide situational awareness by providing a comprehensive view of audit data.**  **Development of processes and protocols for continuous analysis and correlation of audit records to gain situational awareness at the organizational, mission/business process, and information system levels will be completed by October 15, 2024. This step will ensure that audit data is used effectively to identify and respond to risks.**  **Training and deployment of the centralized log management tools to relevant staff, including analysts and IT administrators, will be conducted by October 30, 2024. This training will focus on the use of the tools for real-time correlation and analysis of audit records.**  **Final review and integration of the audit correlation processes into the organization's security operations will be completed by November 29, 2024, ensuring that situational awareness is maintained across all levels of risk management.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AU-7 | **No existing capability for audit record reduction and report generation that supports on-demand review, analysis, and incident investigation**  **Potential issues with maintaining the original content and time ordering of audit records during reduction and reporting processes**  **Lack of a standardized approach to summarizing and reporting audit data for meaningful analysis** | **Information Security Office (ISO)**  **Audit and Compliance Department** | **Reallocation: Use existing audit tools and data analysis resources**  **Funded: Acquisition of advanced audit reduction and reporting tools, if necessary**  **Estimated Cost: $40,000 for software acquisition, implementation, and training** | **Final Completion Date: November 29, 2024** | **Assessment of current audit record capabilities to identify gaps in reduction and reporting will be completed by September 15, 2024. This will include evaluating existing tools and processes to determine their effectiveness in supporting audit reviews and incident investigations.**  **Implementation of an audit record reduction capability that organizes collected audit log information into a summary format, without altering the original content or time ordering of records, will be finalized by September 30, 2024. This capability will include data mining techniques and advanced filters to highlight anomalous behaviors.**  **Deployment of a report generation capability that allows for customizable, on-demand reports to support audit record review, analysis, and after-the-fact investigations will be completed by October 15, 2024. This step ensures that reports can be tailored to meet specific audit and compliance needs.**  **Training for relevant staff on using the audit reduction and report generation tools will be conducted by October 30, 2024. This training will focus on ensuring that users can effectively generate and analyze reports without compromising the integrity of the original audit data.**  **Final review and integration of the audit record reduction and report generation capabilities into the organization's overall audit and compliance framework will be completed by November 29, 2024, ensuring that these processes support comprehensive and meaningful analysis.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AU-8 | **No standardized use of internal system clocks to generate time stamps for audit records**  **Lack of consistency in recording time stamps that meet organization-defined granularity of time measurement**  **Potential discrepancies in time stamps due to variation in local time offsets or lack of synchronization with Coordinated Universal Time (UTC)** | **Information Security Office (ISO)**  **IT Department** | **Reallocation: Use existing system clock and time synchronization tools**  **Funded: Potential need for enhanced time synchronization tools or updates to current systems**  **Estimated Cost: $20,000 for system updates and time synchronization tools** | **Final Completion Date: November 29, 2024** | **Assessment of current systems to identify inconsistencies in time stamping, including variations in time synchronization and time offset handling, will be completed by September 15, 2024. This step involves reviewing how current systems generate and record time stamps.**  **Implementation of a standardized process for using internal system clocks to generate time stamps across all audit records will be finalized by September 30, 2024. This will ensure that all systems consistently use synchronized internal clocks for time stamping.**  **Configuration of systems to record time stamps that meet organization-defined granularity of time measurement, using Coordinated Universal Time (UTC) or a fixed local time offset, will be completed by October 15, 2024. This configuration will be applied uniformly across all relevant systems.**  **Testing and validation of the new time stamp configurations to ensure accuracy and consistency across systems, particularly in the context of audit records, will be conducted by October 30, 2024. This will include verifying that all time stamps are correctly synchronized and reflect the intended granularity.**  **Final review and integration of the time stamp generation and recording processes into the organization's audit and compliance framework will be completed by November 29, 2024, ensuring full compliance with AU-8 requirements.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AU-9 | **No established process to protect audit information and logging tools from unauthorized access, modification, or deletion**  **Lack of alerting mechanisms to notify personnel of unauthorized access or changes to audit information**  **Potential security risks due to the vulnerability of audit records and logging tools** | **Information Security Office (ISO)**  **IT Department** | **Reallocation: Use existing security tools and access control systems**  **Funded: Potential need for additional security tools or enhanced access controls for audit information**  **Estimated Cost: $30,000 for security enhancements and alerting mechanisms** | **Final Completion Date: November 29, 2024** | **Assessment of current audit information protection measures to identify gaps in access control, modification prevention, and deletion safeguards will be completed by September 15, 2024. This step involves evaluating existing security controls around audit logs and tools.**  **Implementation of enhanced access controls to protect audit information and logging tools from unauthorized access, modification, or deletion will be finalized by September 30, 2024. This will involve configuring role-based access controls (RBAC) and encryption measures to ensure only authorized personnel can interact with audit data.**  **Deployment of an alerting mechanism that notifies designated personnel immediately upon detection of unauthorized access, modification, or deletion of audit information will be completed by October 15, 2024. This alert system will integrate with existing security incident and event management (SIEM) tools.**  **Testing and validation of the new security controls and alerting mechanisms will be conducted by October 30, 2024, ensuring that the system effectively protects audit information and responds to unauthorized activities.**  **Final review and integration of the audit information protection measures into the organization's overall security and compliance framework will be completed by November 29, 2024, ensuring full compliance with AU-9 requirements.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| AU-9(3) | **No cryptographic mechanisms currently in place to protect the integrity of audit information and audit tools**  **Potential risk of audit information being tampered with or compromised without detection**  **Lack of assurance that audit data remains authentic and unaltered during storage and transmission** | **Information Security Office (ISO)**  **IT Department** | **Reallocation: Utilize existing cryptographic tools and technologies, if available**  **Funded: Acquisition of cryptographic solutions and tools if needed to ensure audit integrity**  **Estimated Cost: $40,000 for cryptographic tool implementation and configuration** | **Final Completion Date: November 29, 2024** | **Assessment of current audit information protection measures to identify the absence of cryptographic mechanisms and potential vulnerabilities will be completed by September 15, 2024. This step involves evaluating the current state of audit data protection and identifying areas where cryptography is needed.**  **Implementation of cryptographic mechanisms, such as signed hash functions using asymmetric cryptography, to protect the integrity of audit information and tools will be finalized by September 30, 2024. This ensures that all audit data is cryptographically secured against tampering.**  **Configuration and deployment of cryptographic keys and signed hash functions to ensure that the integrity of audit information can be verified at all times will be completed by October 15, 2024. This process includes setting up key management and distribution systems.**  **Testing and validation of the cryptographic protection mechanisms to ensure that they work as intended, preserving the integrity of audit data and tools, will be conducted by October 30, 2024. This will involve running scenarios to test the effectiveness of cryptographic protections.**  **Final review and integration of cryptographic protection measures into the organization's audit and compliance framework will be completed by November 29, 2024, ensuring full compliance with AU-9(3) requirements.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| CA-2 | **No standardized process for selecting appropriate assessors or developing control assessment plans**  **Lack of regular assessments to determine if controls are implemented correctly, operating as intended, and producing the desired outcomes**  **Inadequate documentation and reporting of control assessment results** | **Information Security Office (ISO)**  **Audit and Compliance Department** | **Reallocation: Utilize existing resources for assessor training and assessment planning**  **Funded: Potential need for external assessment tools or third-party assessors if internal resources are insufficient**  **Estimated Cost: $50,000 for external assessment resources and tool acquisition** | **Final Completion Date: November 29, 2024** | **Selection of appropriate assessors or assessment teams based on the type of assessment to be conducted, ensuring they possess the required skills and expertise, will be completed by September 15, 2024. This includes internal and potentially external personnel who are qualified to conduct control assessments.**  **Development of a comprehensive control assessment plan that includes the scope of the assessment, controls and control enhancements under assessment, assessment procedures, and roles and responsibilities, will be finalized by September 30, 2024. This plan will be reviewed and approved by the authorizing official or designated representative.**  **Execution of control assessments according to the plan, evaluating the system and its environment of operation to determine if controls are correctly implemented and achieving the desired outcomes, will be conducted by October 15, 2024. This step will include a thorough analysis and documentation of the assessment results.**  **Production of a detailed control assessment report that documents the results and findings of the assessment will be completed by October 30, 2024. This report will be reviewed by relevant stakeholders to ensure accuracy and completeness.**  **Distribution of the control assessment results to organization-defined individuals or roles, ensuring that all relevant parties are informed of the outcomes and any identified weaknesses, will be finalized by November 29, 2024.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| CA-5 | **No established process for developing and updating a Plan of Action and Milestones (POA&M) to track remediation actions**  **Lack of documentation for planned remediation actions following control assessments, audits, or continuous monitoring activities**  **Potential failure to address known vulnerabilities and weaknesses in a timely and organized manner** | **Information Security Office (ISO)**  **Project Management Office (PMO)** | **Reallocation: Utilize existing project management tools and resources**  **Funded: Potential need for dedicated resources to manage and update POA&Ms**  **Estimated Cost: $30,000 for POA&M management tools and training** | **Final Completion Date: November 29, 2024** | **Development of an initial Plan of Action and Milestones (POA&M) for the system that documents all planned remediation actions to correct weaknesses or deficiencies identified during control assessments will be completed by September 15, 2024. This includes detailing the actions needed to reduce or eliminate known vulnerabilities.**  **Implementation of a process to regularly update the POA&M based on findings from subsequent control assessments, independent audits, or continuous monitoring activities will be finalized by September 30, 2024. This process will ensure that the POA&M remains current and accurately reflects the state of the system's security posture.**  **Integration of the POA&M into the organization's overall project management and risk management frameworks to ensure that remediation actions are tracked and completed according to schedule will be completed by October 15, 2024. This step ensures that the POA&M is not just a document, but an active part of the remediation process.**  **Training for relevant personnel on how to develop, update, and manage the POA&M effectively will be conducted by October 30, 2024. This training will focus on using the POA&M as a tool for continuous improvement and risk management.**  **Final review and approval of the POA&M process by senior management, ensuring that it meets organizational and federal requirements, will be completed by November 29, 2024.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| CA-7 | **Lack of a formalized continuous monitoring strategy at the system level**  **Inadequate frequency of monitoring and control assessments leading to potential delays in identifying and addressing vulnerabilities**  **Insufficient correlation and analysis of information from monitoring and control assessments** | **Information Security Office (ISO)**  **Risk Management Office (RMO)** | **Reallocation: Utilize existing monitoring tools and resources**  **Funded: Potential need for additional automation tools and technologies for continuous monitoring**  **Estimated Cost: $75,000 for enhanced monitoring tools and integration services** | **Final Completion Date: November 29, 2024** | **Development of a system-level continuous monitoring strategy, aligned with the organization-level strategy, to monitor system security and privacy posture will be completed by September 15, 2024. This strategy will outline specific metrics to be monitored, the frequency of monitoring, and the process for assessing control effectiveness.**  **Establishment of organization-defined frequencies for monitoring and assessment of control effectiveness in accordance with the continuous monitoring strategy will be finalized by September 30, 2024. This includes setting up schedules for regular monitoring and control assessments.**  **Implementation of ongoing control assessments and monitoring of system and organization-defined metrics, ensuring that the system's security and privacy status is continually evaluated, will be conducted by October 15, 2024. This will involve deploying tools and processes to automatically collect and analyze relevant data.**  **Correlation and analysis of information generated by control assessments and monitoring activities, identifying potential issues and triggering appropriate response actions, will be completed by October 30, 2024. This step will focus on ensuring that all relevant data is analyzed in a timely manner to support decision-making.**  **Reporting the security and privacy status of the system to organization-defined personnel or roles at specified intervals will be fully integrated into the continuous monitoring process by November 29, 2024. This reporting will ensure that all stakeholders are informed of the system's status and any emerging risks.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| CM-3 | **Inconsistent documentation and review processes for configuration changes to the system**  **Lack of formal oversight for configuration change control activities**  **Inadequate monitoring and review of configuration-controlled changes after implementation** | **Configuration Management Office (CMO)**  **Change Advisory Board (CAB** | **Reallocation: Existing resources for Configuration Management**  **Funded: Potential need for additional tools to support automated configuration tracking and documentation**  **Estimated Cost: $50,000 for tool acquisition and training** | **Final Completion Date: November 15, 2024** | **Determine and document the types of changes to the system that are configuration-controlled by September 30, 2024. This will involve defining a clear scope of changes that require formal review and approval before implementation.**  **Establish a formal review process for proposed configuration-controlled changes, ensuring that each change is assessed for security and privacy impact. This process will be in place by October 15, 2024.**  **Document configuration change decisions and ensure that all approved changes are properly recorded. This documentation process will be completed by October 31, 2024.**  **Implement a system for retaining records of configuration-controlled changes for a defined period, ensuring compliance with organizational policies. This retention system will be operational by November 7, 2024.**  **Monitor and review activities associated with configuration-controlled changes to the system, ensuring ongoing compliance and identifying any issues post-implementation. This monitoring framework will be established by November 15, 2024.**  **Coordinate oversight of configuration change control activities through a formal Configuration Control Board (CCB) that meets regularly to review proposed changes and approve/disapprove them. This board will be fully operational by November 15, 2024.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| CM-4 | **Lack of formal procedures for conducting impact analyses prior to implementing system changes**  **Inconsistent documentation of potential security and privacy impacts related to changes**  **Limited involvement of personnel with security or privacy responsibilities in the change process** | **Security Office**  **Privacy Office**  **Configuration Management Office (CMO)** | **Reallocation: Utilize existing security and privacy personnel for impact analysis tasks**  **Funded: Potential need for additional training on conducting effective impact analyses**  **Estimated Cost: $30,000 for training and process enhancement** | **Final Completion Date: December 15, 2024** | **Develop and implement formal procedures for conducting impact analyses on system changes by September 30, 2024. These procedures will ensure that all potential security and privacy impacts are identified and documented before changes are approved.**  **Train organizational personnel with security and privacy responsibilities on the new impact analysis procedures by October 31, 2024. Training will focus on understanding control requirements, system design, and how changes might affect the security and privacy controls.**  **Conduct a pilot impact analysis on a proposed system change by November 15, 2024. This pilot will test the effectiveness of the new procedures and provide feedback for any necessary adjustments.**  **Review and update the impact analysis process based on feedback from the pilot by November 30, 2024. Adjustments will be made to ensure the process is effective and efficient.**  **Fully integrate the impact analysis process into the configuration management and change control processes by December 15, 2024.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| CM-5 | **Inadequate definition and documentation of access restrictions associated with system changes**  **Lack of enforced physical and logical access controls for system change processes**  **Insufficient controls over who can initiate and implement changes to system hardware, software, or firmware** | **Security Office**  **Configuration Management Office (CMO)**  **IT Operations** | **Funded: Implementation of enhanced access control mechanisms, including training and system upgrades**  **Estimated Cost: $45,000 for system upgrades and access control software, $15,000 for training** | **Final Completion Date: November 29, 2024** | **Define and document physical and logical access restrictions for all system changes by October 31, 2024. This will include specifying the roles and responsibilities of personnel authorized to make changes.**  **Approve the new access restriction protocols through the Configuration Control Board (CCB) and ensure they are in line with security and privacy policies by November 15, 2024.**  **Upgrade and configure access control systems to enforce the newly defined access restrictions by December 15, 2024. This will involve integrating with existing access control mechanisms and software.**  **Train authorized personnel on the new access restrictions and enforcement mechanisms by January 15, 2025. Training will focus on how to comply with the new protocols and how to use the updated access control systems.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| CM-5(1) | **Lack of automated mechanisms to enforce access restrictions for configuration changes**  **Absence of automatic generation of audit records for configuration change enforcement actions**  **Insufficient tracking and monitoring of unauthorized configuration changes** | **IT Security Office**  **Configuration Management Office (CMO)**  **IT Operations** | **Funded: Acquisition and integration of automated access control tools, including training and system configuration**  **Estimated Cost: $60,000 for software acquisition and integration, $10,000 for training** | **Final Completion Date: November 29, 2024** | **Select and approve automated tools for enforcing access restrictions and generating audit records by November 15, 2024. This will involve evaluating and selecting tools that meet security requirements.**  **Integrate and configure the selected tools with existing systems to ensure automated enforcement of access controls by January 15, 2025. This step includes ensuring that audit records are automatically generated.**  **Conduct thorough testing and validation of the automated mechanisms to confirm proper functionality by February 15, 2025. This will involve verifying that the tools enforce access restrictions and generate accurate audit logs.**  **Train IT and security staff on the use of the new tools and the interpretation of audit logs by February 28, 2025. Training will ensure that staff are proficient in using the automated controls and understanding the audit records.**  **Review and adjust the automated enforcement and audit processes based on initial implementation feedback by March 15, 2025. This milestone includes making any necessary refinements to the system.**  **Fully implement the automated access controls and audit record generation across all applicable systems by March 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| CM-7 | **Failure to configure systems to restrict non-essential functions, ports, protocols, software, and services**  **Lack of mechanisms to enforce the use of only mission-essential capabilities**  **Exposure to increased risk due to unnecessary functions and services running on system components** | **IT Security Office**  **Configuration Management Office (CMO)**  **Network Operations** | **Funded: Acquisition and deployment of network scanning tools, firewalls, and endpoint protection systems**  **Estimated Cost: $50,000 for tools and software acquisition, $20,000 for system configuration and training** | **Final Completion Date: January 31, 2025** | **Identify and document mission-essential capabilities by conducting a thorough review to determine only the capabilities required by the organization by September 30, 2024.**  **Restrict and disable non-essential functions, ports, and protocols by reconfiguring systems to ensure only required services are enabled, coordinating with relevant stakeholders to complete this task by October 31, 2024.**  **Deploy network scanning and endpoint protection tools to monitor and prevent the use of prohibited functions and services, ensuring implementation by November 30, 2024.**  **Test and validate system configurations to confirm alignment with least functionality requirements, addressing any identified gaps by December 15, 2024.**  **Train IT staff and users on the new configurations and protocols, focusing on maintaining least functionality, with training completed by January 15, 2025.**  **Conduct a final review of system configurations and update relevant policies and documentation to reflect the changes, with completion by January 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| CM-7(5) | **Lack of a defined process for identifying and managing authorized software programs on systems**  **Inadequate enforcement of deny-all, permit-by-exception policies for software execution**  **Insufficient review and updating of the list of authorized software programs, leading to potential vulnerabilities** | **IT Security Office**  **Configuration Management Office (CMO)**  **Software Asset Management Team** | **Funded: Implementation of software management tools and enforcement mechanisms**  **Estimated Cost: $40,000 for software tools and $10,000 for policy development and staff training** | **Final Completion Date: January 31, 2025** | **Identify and document all software programs authorized to execute on the system, ensuring alignment with organizational security policies by September 30, 2024.**  **Implement a deny-all, permit-by-exception policy for software execution, configuring systems to enforce this policy across all relevant environments by October 31, 2024.**  **Deploy software management tools to monitor and enforce the execution of authorized software, completing deployment by November 30, 2024.**  **Review and update the list of authorized software programs based on the latest organizational needs and threat assessments, with the first update completed by December 15, 2024.**  **Train IT staff on the new software management and enforcement processes, ensuring they can effectively manage and monitor authorized software by January 15, 2025.**  **Conduct a final review of the software management processes and enforcement mechanisms, making necessary adjustments by January 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| CM-11 | **Inadequate policies governing user-installed software, leading to potential security vulnerabilities**  **Lack of enforcement mechanisms for controlling software installation by users**  **Insufficient monitoring of compliance with software installation policies** | **IT Security Office**  **Configuration Management Office (CMO)**  **Compliance Office** | **Funded: Development and implementation of software installation policies and monitoring tools**  **Estimated Cost: $30,000 for policy development and $20,000 for monitoring tools** | **Final Completion Date: January 31, 2025** | **Establish and document policies governing the installation of software by users, specifying permitted and prohibited actions by September 30, 2024.**  **Develop and deploy enforcement mechanisms, such as automated tools and procedural guidelines, to ensure adherence to the software installation policies by October 31, 2024.**  **Configure monitoring systems to track and report compliance with the software installation policies, completing setup by November 30, 2024.**  **Conduct training sessions for IT staff and end-users on the new software installation policies and enforcement mechanisms by December 15, 2024.**  **Perform an initial review of compliance with the software installation policies, identifying any gaps or areas for improvement by January 15, 2025.**  **Implement necessary adjustments to the policies or enforcement mechanisms based on the review by January 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| IA-1 | **Absence of documented identification and authentication policies at the organization level**  **Lack of designated personnel responsible for managing identification and authentication policies and procedures**  **Inadequate procedures for the regular review and update of identification and authentication policies** | **IT Security Office**  **Compliance Office**  **Policy Management Office** | **Funded: Development and dissemination of identification and authentication policies, including training sessions and regular updates**  **Estimated Cost: $35,000 for policy development and $10,000 annually for updates and training** | **Final Completion Date: February 28, 2025** | **Develop and document organization-level identification and authentication policies, ensuring they align with applicable laws, directives, and standards by October 31, 2024.**  **Designate an official or team responsible for managing the identification and authentication policies and ensuring their proper dissemination by November 15, 2024.**  **Establish and document procedures to support the implementation of the identification and authentication policies, including assigning roles and responsibilities, by December 15, 2024.**  **Conduct training sessions for relevant personnel on the new policies and procedures by January 15, 2025.**  **Implement a schedule for regular review and updates of the policies and procedures, taking into account any relevant events such as audits, security incidents, or changes in regulations by January 31, 2025.**  **Perform an initial review of the implemented policies and procedures, making any necessary adjustments, and documenting the process by February 15, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| IA-2 | **Lack of unique identification and authentication for all organizational users and processes**  **Inadequate procedures for handling local and network access, including remote access, to organizational systems**  **Insufficient use of multi-factor authentication and encrypted virtual private networks for securing network connections** | **IT Security Office**  **Identity and Access Management Office**  **Network Operations Center** | **Funded: Implementation of unique identification, multi-factor authentication, and VPN solutions, including associated training and software upgrades**  **Estimated Cost: $75,000 for authentication systems, $20,000 for network upgrades, $10,000 for training** | **Final Completion Date: March 31, 2025** | **Implement unique identification and authentication mechanisms for all organizational users, including contractors and guest researchers, by October 31, 2024. This includes updating authentication protocols to comply with HSPD 12 requirements.**  **Establish and document procedures for local and network access, including remote access, ensuring compliance with security policies by November 30, 2024.**  **Integrate multi-factor authentication systems for critical access points and ensure the deployment of encrypted virtual private networks for secure network connections by December 15, 2024.**  **Conduct training sessions for relevant personnel on the new identification and authentication procedures, focusing on the use of multi-factor authentication and VPNs, by January 31, 2025.**  **Review and assess the effectiveness of the implemented identification and authentication controls, making necessary adjustments based on feedback and monitoring by February 28, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| IA-2 (1) | **Lack of multi-factor authentication (MFA) for access to privileged accounts**  **Inadequate security measures for high-risk accounts, relying solely on single-factor authentication**  **Insufficient enforcement of MFA solutions for privileged accounts, leading to potential unauthorized access** | **IT Security Office**  **Identity and Access Management Office** | **Funded: Implementation of multi-factor authentication mechanisms, including hardware tokens and software integration**  **Estimated Cost: $60,000 for MFA systems and tokens, $10,000 for integration and configuration, $5,000 for user training** | **Final Completion Date: December 31, 2024** | **Identify and document all privileged accounts within the organization that require multi-factor authentication by September 30, 2024.**  **Select and procure multi-factor authentication solutions, including hardware tokens and software, by October 15, 2024.**  **Integrate and configure the MFA solutions for all identified privileged accounts, ensuring compatibility with existing systems, by November 15, 2024.**  **Train privileged account holders and relevant IT personnel on the use of the new MFA systems and procedures by December 1, 2024.**  **Review the effectiveness of the implemented MFA solutions, making adjustments as needed, and finalize the implementation by December 31, 2024.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| IA-2(8) | **Absence of replay-resistant authentication mechanisms for privileged accounts**  **Vulnerability to replay attacks due to reliance on static authentication methods**  **Lack of cryptographic authentication protocols for enhanced security in account access** | **IT Security Office**  **Identity and Access Management Office** | **Funded: Deployment of replay-resistant authentication mechanisms, including cryptographic authenticators and software upgrades**  **Estimated Cost: $70,000 for authentication system upgrades, $15,000 for cryptographic tokens, $10,000 for training and integration** | **Final Completion Date: January 31, 2025** | **Identify accounts requiring replay-resistant authentication, focusing on privileged accounts by September 30, 2024.**  **Select and procure cryptographic authentication solutions and supporting software by October 15, 2024.**  **Implement the replay-resistant authentication mechanisms across all identified accounts, ensuring integration with existing systems by November 15, 2024.**  **Train system administrators and privileged account holders on the new authentication protocols and security procedures by December 1, 2024.**  **Conduct a review and assessment of the effectiveness of the replay-resistant mechanisms and adjust configurations as necessary by January 15, 2025.**  **Finalize the deployment and conduct a final review to ensure all security gaps are addressed by January 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| IA-4 | **Lack of comprehensive management for system identifiers**  **Inadequate authorization process for assigning identifiers to individuals, groups, and devices**  **Reuse of identifiers without a defined time period, increasing security risks** | **Identity and Access Management Office**  **IT Security Office** | **Funded: Implementation of enhanced identifier management protocols, including authorization processes and system upgrades**  **Estimated Cost: $50,000 for system enhancements and policy development, $10,000 for training and integration** | **Final Completion Date: February 28, 2025** | **Develop and document an authorization process for assigning identifiers, ensuring only authorized personnel can assign identifiers by September 30, 2024.**  **Select and implement a system for managing identifiers, including tools for assigning and tracking individual, group, role, service, and device identifiers by October 31, 2024.**  **Establish and enforce a policy to prevent the reuse of identifiers for a defined time period, integrating this into the system management protocols by November 30, 2024.**  **Train relevant personnel on the new identifier management processes and tools, focusing on the proper assignment and tracking of identifiers by December 15, 2024.**  **Conduct a review of the identifier management processes, ensuring compliance with the new policies and making adjustments as necessary by February 15, 2025.**  **Finalize the identifier management system and conduct a final assessment to ensure all weaknesses have been addressed by February 28, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| IA-5 | **Inadequate verification of identity during the distribution of authenticators**  **Default authenticators not changed prior to first use, leading to potential security risks**  **Lack of procedures for managing lost, compromised, or damaged authenticators** | **Identity and Access Management Office**  **IT Security Office** | **Funded: Implementation of enhanced authenticator management protocols, including identity verification and system upgrades**  **Estimated Cost: $60,000 for system enhancements and policy development, $15,000 for training and integration** | **Final Completion Date: March 31, 2025** | **Develop and document a process for verifying the identity of individuals, groups, roles, and devices during the initial distribution of authenticators by September 30, 2024.**  **Establish procedures for changing default authenticators prior to their first use, ensuring all defaults are updated immediately upon system installation by October 31, 2024.**  **Implement and enforce administrative procedures for managing lost, compromised, or damaged authenticators, including the revocation and reissuance of credentials by November 30, 2024.**  **Enhance the security of authenticator content, ensuring protection from unauthorized disclosure and modification through encryption and secure storage solutions by December 15, 2024.**  **Train relevant personnel on the new authenticator management processes and tools, focusing on secure handling, distribution, and revocation of authenticators by January 15, 2025.**  **Conduct a review of the authenticator management processes, ensuring compliance with the new policies and making necessary adjustments by March 15, 2025.**  **Finalize the authenticator management system and conduct a final assessment to ensure all weaknesses have been addressed by March 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| IA-5 (1) | **Lack of enforcement of strong password composition and complexity rules**  **Inadequate protection of passwords during transmission and storage**  **Insufficient mechanisms to prevent the use of commonly-used, expected, or compromised passwords** | **Identity and Access Management Office**  **Cybersecurity Office** | **Funded: Implementation of enhanced password management protocols, including list maintenance and password security tools**  **Estimated Cost: $35,000 for software upgrades, $10,000 for training and integration** | **Final Completion Date: April 30, 2025** | **Develop and maintain a list of commonly-used, expected, or compromised passwords, ensuring regular updates and inclusion of passwords from recent security breaches by September 30, 2024.**  **Implement verification mechanisms that ensure newly created or updated passwords are checked against the list of disallowed passwords by October 31, 2024.**  **Ensure all passwords are transmitted only over cryptographically-protected channels by November 15, 2024. This will involve upgrading existing systems to enforce encryption standards.**  **Store all passwords using an approved salted key derivation function by December 15, 2024. This includes migrating existing password data to the new storage mechanism.**  **Establish procedures requiring immediate password changes upon account recovery, enforcing new password rules by January 31, 2025.**  **Allow users to create long passwords and passphrases, and enforce strong password composition and complexity rules through automated tools by February 28, 2025.**  **Train relevant personnel on new password policies and the use of automated tools for password creation by March 31, 2025.**  **Conduct a review of password management policies and procedures, making adjustments as necessary to ensure compliance with the new requirements by April 15, 2025.**  **Finalize the password management system and conduct a final assessment to ensure all weaknesses have been addressed by April 30, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| IA-5 (2) | **Lack of enforcement for access control to private keys associated with public key-based authentication**  **Inadequate mapping of authenticated identities to corresponding user accounts**  **Insufficient validation of certificates, including lack of local cache for revocation data to support path discovery and validation** | **Public Key Infrastructure (PKI) Office**  **Cybersecurity Office** | **Funded: Implementation of enhanced PKI protocols, including key management and certificate validation processes**  **Estimated Cost: $40,000 for software upgrades and key management systems, $12,000 for training on PKI and certificate management** | **Final Completion Date: May 31, 2025** | **Enforce access controls for private keys used in public key-based authentication by September 30, 2024. This will involve reviewing and updating existing access control mechanisms to ensure only authorized personnel can access private keys.**  **Map authenticated identities to corresponding user accounts by October 31, 2024. This will require integrating identity management systems with PKI solutions to ensure proper account mapping.**  **Implement certificate validation processes, including constructing and verifying certification paths to an accepted trust anchor by November 30, 2024. This includes validating certificate status information through certificate revocation lists (CRLs) or certificate status protocol (OCSP) responses.**  **Develop and implement a local cache for revocation data by January 31, 2025. This will support certificate path discovery and validation, particularly in environments with limited network access to revocation information.**  **Train relevant personnel on enhanced PKI protocols, key management, and certificate validation processes by February 28, 2025.**  **Conduct a review of PKI systems and make necessary adjustments based on feedback and monitoring by April 30, 2025.**  **Finalize PKI processes and conduct a final assessment to ensure all weaknesses have been addressed by May 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| IA-5(6) | **Inadequate protection of authenticators relative to the security category of information they access**  **Lack of consistent enforcement for protecting authenticators in systems containing multiple security categories** | **Information Security Office**  **Risk Management Office** | **Funded: Implementation of enhanced security measures for authenticator management and protection**  **Estimated Cost: $35,000 for system enhancements and training, $10,000 for risk assessment and categorization updates** | **Final Completion Date: June 30, 2025** | **Review and categorize all systems to determine the highest security category of information by September 30, 2024. This will involve a thorough assessment of information security categories across all systems.**  **Develop and implement a strategy to protect authenticators in line with the highest security category by November 30, 2024. This will include updating policies and procedures for authenticator management.**  **Ensure that all systems containing multiple security categories have reliable physical or logical separation between categories, or protect authenticators commensurate with the highest security category by January 31, 2025.**  **Conduct training sessions for relevant personnel on the updated authenticator protection measures by March 31, 2025. Training will focus on how to handle and protect authenticators according to the security category of information.**  **Conduct a review of the protection measures in place and make necessary adjustments based on feedback and monitoring by May 31, 2025.**  **Finalize and validate the implementation of enhanced authenticator protection across all systems by June 30, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| IA-6 | **Inadequate obscuring of authentication feedback, increasing the risk of unauthorized access**  **Failure to implement consistent feedback obscuring mechanisms across all devices and platforms** | **Information Security Office**  **User Interface/Experience (UI/UX) Design Team** | **Funded: Implementation of feedback obscuring mechanisms across all systems and devices**  **Estimated Cost: $25,000 for software updates and user interface improvements, $10,000 for testing and quality assurance** | **Final Completion Date: May 31, 2025** | **Assess current authentication feedback mechanisms and identify gaps by September 30, 2024. This will involve evaluating systems and devices to determine where feedback obscuring is insufficient.**  **Develop and implement obscuring mechanisms such as asterisks or limited-time displays across all platforms by November 30, 2024. This includes ensuring consistency in how feedback is presented on both large displays and mobile devices.**  **Test and validate the effectiveness of the implemented obscuring mechanisms by January 31, 2025. This phase will involve user testing to ensure that the solutions do not hinder usability while providing adequate protection.**  **Train relevant personnel on the new authentication feedback procedures by February 28, 2025. Training will focus on the importance of feedback obscuring and how to manage these settings on different devices.**  **Conduct a final review and make any necessary adjustments based on feedback from the testing phase by April 30, 2025.**  **Complete final validation and ensure full implementation across the organization by May 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| IR-4 | **Inconsistent implementation of incident handling procedures across the organization**  **Lack of coordination between incident handling and contingency planning activities**  **Insufficient incorporation of lessons learned into incident response procedures and training** | **Incident Response Team**  **Contingency Planning Office**  **Training and Development Office** | **Funded: Enhancing incident response capabilities, coordination efforts, and training programs**  **Estimated Cost: $50,000 for improved incident response tools and systems, $20,000 for training development and delivery** | **Final Completion Date: February 28, 2025** | **Review and update the incident handling procedures to align with the incident response plan and integrate with contingency planning by October 15, 2024. This will include refining processes for preparation, detection, analysis, containment, eradication, and recovery.**  **Develop a comprehensive incident handling training program and schedule training sessions for all relevant personnel by November 30, 2024. The training will cover updated procedures, tools, and coordination efforts.**  **Conduct an organization-wide incident handling exercise by January 15, 2025, to test the updated procedures and coordination between incident handling and contingency planning teams. This exercise will be designed to simulate a real-world incident.**  **Analyze the results of the exercise and incorporate lessons learned into the incident response procedures, making necessary adjustments by February 15, 2025.**  **Complete final implementation of the updated incident handling procedures and ensure all personnel are trained and ready by February 28, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| IR-6 | **Delayed reporting of suspected incidents to the incident response team**  **Inconsistent reporting formats and lack of clarity in the content of incident reports**  **Failure to report incidents to appropriate authorities as required by organizational policies** | **Incident Response Team**  **IT Security Office**  **Legal and Compliance Office** | **Funded: Improvement of incident reporting processes, development of standardized reporting templates, and training on timely and accurate incident reporting**  **Estimated Cost: $30,000 for process improvement and training, $10,000 for development and implementation of reporting tools** | **Final Completion Date: February 29, 2025** | **Review and revise the incident reporting procedures to ensure timely reporting to the incident response team within organization-defined time periods by September 30, 2024. This will include updating the reporting timelines and responsibilities for all personnel.**  **Develop and implement standardized incident reporting templates to be used by all personnel when reporting incidents by October 31, 2024. Templates will include sections for required information such as incident type, timeline, and affected systems.**  **Conduct training sessions for all relevant personnel on the updated incident reporting procedures and the use of the standardized templates by November 30, 2024.**  **Establish and implement a process for reporting incidents to organization-defined authorities, ensuring compliance with applicable laws and regulations by January 31, 2025.**  **Perform a review of the incident reporting process, ensuring it meets the organization's requirements and make any necessary adjustments by February 29, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| MA-3(3) | **Failure to adequately verify the presence of organizational information on maintenance equipment before removal**  **Lack of consistent sanitization or destruction processes for equipment containing organizational data**  **Inadequate retention policies or enforcement for maintenance equipment within the facility** | **IT Maintenance Department**  **Data Security Office**  **Facilities Management** | **Funded: Implementation of stricter equipment verification, sanitization, and retention protocols; training for personnel on these updated processes**  **Estimated Cost: $25,000 for process implementation and training, $15,000 for equipment sanitization tools and facilities** | **Final Completion Date: February 28, 2025** | **Develop and implement verification protocols to ensure no organizational information remains on maintenance equipment prior to removal by September 30, 2024.**  **Establish and enforce sanitization or destruction processes for equipment that may contain organizational data by October 31, 2024. This will include the acquisition of necessary sanitization tools.**  **Implement a policy to retain all maintenance equipment within the facility unless an exemption is explicitly authorized by November 30, 2024.**  **Conduct training sessions for maintenance and security personnel on the updated verification, sanitization, and retention protocols by December 31, 2024.**  **Review and audit the effectiveness of the new protocols and adjust as necessary by February 28, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| MA-4 | **Insufficient approval and monitoring processes for nonlocal maintenance and diagnostic activities**  **Lack of strong authentication measures during the establishment of nonlocal maintenance sessions**  **Inadequate documentation and record-keeping for nonlocal maintenance activities** | **IT Security Office**  **System Administration Team**  **Configuration Management Office** | **Funded: Implementation of enhanced approval, authentication, and record-keeping processes for nonlocal maintenance activities**  **Estimated Cost: $30,000 for authentication systems and record-keeping tools, $20,000 for personnel training and process implementation** | **Final Completion Date: March 31, 2025** | **Develop and implement policies for the approval and monitoring of nonlocal maintenance activities, ensuring alignment with organizational security plans by October 31, 2024.**  **Integrate strong authentication measures, such as multi-factor authentication and PKI, into the nonlocal maintenance process by November 30, 2024.**  **Enhance the documentation process to maintain comprehensive records of all nonlocal maintenance sessions by December 31, 2024.**  **Train IT and maintenance personnel on the updated nonlocal maintenance protocols and the use of authentication systems by January 31, 2025.**  **Conduct a review and audit of nonlocal maintenance procedures and records to ensure compliance and effectiveness by March 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| MP-3 | **Inconsistent marking of system media, leading to potential mishandling or unauthorized distribution of sensitive information.**  **Lack of clear guidelines for exempting certain types of system media from marking when they remain within controlled areas.** | **Information Security Office**  **Records Management Office**  **Configuration Management Office** | **Funded: Implementation of standardized media marking protocols and exemption procedures.**  **Estimated Cost: $25,000 for training staff and updating marking tools, $10,000 for developing and disseminating updated guidelines.** | **Final Completion Date: February 28, 2025** | **Develop and distribute clear guidelines on media marking, including marking requirements for different types of media and exemptions for media within controlled areas by September 30, 2024.**  **Train relevant staff on the updated media marking protocols and exemption procedures by October 31, 2024.**  **Implement new media marking tools and processes across all departments by November 30, 2024.**  **Conduct an audit to ensure compliance with the new media marking guidelines and exemption protocols by January 31, 2025.**  **Review and adjust marking and exemption procedures based on audit findings by February 28, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| MP-4 | **Lack of consistent physical control and secure storage protocols for various types of digital and non-digital media.**  **Inadequate protection of stored media until proper destruction or sanitization is completed.** | **Information Security Office**  **Records Management Office**  **Facilities Management** | **Funded: Implementation of secure storage solutions and training for proper media handling and storage.**  **Estimated Cost: $35,000 for secure storage equipment and upgrades, $10,000 for staff training and procedure development.** | **Final Completion Date: March 31, 2025** | **Assess current media storage practices and identify gaps in physical control and secure storage by September 30, 2024.**  **Develop and implement updated secure storage protocols, including the classification of media and corresponding storage requirements, by October 31, 2024.**  **Purchase and install secure storage equipment, such as locked cabinets and controlled media libraries, by November 30, 2024.**  **Train relevant staff on new media storage protocols and procedures by December 15, 2024.**  **Begin monitoring and enforcing compliance with the updated storage protocols by January 31, 2025.**  **Conduct a review of the effectiveness of the new media storage controls and make adjustments as necessary by March 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| MP-5 | **Inadequate protection and control of system media during transport outside of controlled areas.**  **Lack of proper documentation and accountability for media transport activities.**  **Insufficient restrictions on personnel authorized to handle media during transport.** | **Information Security Office**  **Logistics and Transport Office**  **Records Management Office** | **Funded: Implementation of enhanced media transport controls, including cryptographic protection and secure containers, and development of tracking systems.**  **Estimated Cost: $40,000 for cryptographic solutions and secure containers, $10,000 for developing and implementing a media transport tracking system.** | **Final Completion Date: April 30, 2025** | **Review and identify organization-defined types of system media requiring protection during transport by September 30, 2024.**  **Develop and implement organization-defined controls, such as cryptography and secure containers, for protecting media during transport by October 31, 2024.**  **Establish accountability procedures for tracking and documenting media transport activities, ensuring media is handled only by authorized personnel, by November 30, 2024.**  **Train authorized transport personnel on new procedures and controls, including the use of cryptography and secure containers, by December 31, 2024.**  **Deploy and test the media transport tracking system to ensure accurate record-keeping and detect potential losses or tampering by January 31, 2025.**  **Conduct an internal audit to evaluate the effectiveness of the new media transport controls and tracking system by March 31, 2025.**  **Make necessary adjustments based on audit findings and complete final implementation by April 30, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| MP-5 (4) | **No cryptographic protection applied during the transport of sensitive system media.**  **Absence of integrated controls ensuring the confidentiality and integrity of media in transit.**  **Lack of alignment with updated cryptographic requirements as incorporated into SC-28(1).** | **Information Security Office**  **Compliance Office** | **Funded: Implementation of cryptographic protection for media transport, including necessary updates to existing infrastructure and training.**  **Estimated Cost: $35,000 for cryptographic software upgrades and $5,000 for training personnel on new protocols.** | **Final Completion Date: March 31, 2025** | **Conduct a gap analysis to identify where cryptographic protection is currently lacking in media transport procedures by September 30, 2024.**  **Develop and implement cryptographic solutions to protect the confidentiality and integrity of media during transport, aligning with SC-28(1) by October 31, 2024.**  **Update security policies and procedures to reflect the integration of cryptographic protection into media transport processes by November 30, 2024.**  **Train staff responsible for media transport on the new cryptographic protection methods, ensuring they understand how to implement these controls effectively by December 31, 2024.**  **Test the effectiveness of cryptographic protections during media transport through a series of controlled transport scenarios by February 28, 2025.**  **Complete final review and adjust the cryptographic protections based on test outcomes, ensuring full compliance with SC-28(1) by March 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| MP-6 | **Inadequate sanitization of system media before disposal or release from organizational control.**  **Lack of defined sanitization techniques that align with the security category or classification of information.**  **Risk of unauthorized retrieval of sensitive information from improperly sanitized media.** | **Information Security Office**  **Records Management Office** | **Funded: Implementation of enhanced media sanitization techniques, including new equipment and procedures.**  **Estimated Cost: $50,000 for sanitization equipment and $10,000 for staff training on new procedures.** | **Final Completion Date: April 30, 2025** | **Conduct a review of current media sanitization practices to identify gaps and deficiencies by September 30, 2024.**  **Define and document organization-specific media sanitization techniques that correspond to the security category of the information, ensuring compliance with applicable standards by October 31, 2024.**  **Procure and install new sanitization equipment necessary to support the defined techniques, including cryptographic erasure tools, by December 15, 2024.**  **Update media handling and disposal policies to incorporate the new sanitization requirements, ensuring alignment with NSA and NARA guidelines by January 15, 2025.**  **Train relevant personnel on the new sanitization procedures and equipment by February 28, 2025.**  **Perform a pilot sanitization project to test the new procedures and equipment, making adjustments as needed based on feedback and results by March 31, 2025.**  **Complete full implementation and review of media sanitization processes, ensuring compliance and effectiveness by April 30, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| MP-7 | **Lack of controls for restricting or prohibiting the use of certain types of system media.**  **Absence of clear policies regarding the use of portable storage devices with no identifiable owner.**  **Risk of unauthorized data access and potential data breaches due to unregulated use of portable storage media.** | **Information Security Office**  **IT Operations** | **Funded: Implementation of media use restrictions, including policy development, technical controls, and user training.**  **Estimated Cost: $35,000 for technical controls and $10,000 for training.** | **Final Completion Date: March 31, 2025** | **Review and assess current media use practices and identify gaps or risks by September 30, 2024.**  **Develop and document specific policies for restricting or prohibiting the use of organization-defined types of system media by October 31, 2024. This includes defining which media types are restricted and under what conditions.**  **Implement technical controls, such as disabling or restricting USB ports and external drive access on organization-defined systems, by December 15, 2024.**  **Establish a process to identify and assign ownership for portable storage devices to ensure accountability, to be completed by January 15, 2025.**  **Conduct training sessions for all relevant personnel on the new media use policies and technical controls by February 15, 2025.**  **Perform an internal audit to ensure compliance with the new media use restrictions and make adjustments based on audit findings by March 15, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| MP-7 (1) | **No established policy to prohibit the use of media devices without an identifiable owner.**  **Inconsistent enforcement of media ownership requirements, leading to potential security vulnerabilities.**  **Risk of unauthorized use of unclaimed media devices within the organization.** | **Information Security Office**  **IT Operations** | **Funded: Development and enforcement of media ownership policies, including the implementation of tracking systems and staff training.**  **Estimated Cost: $20,000 for system upgrades and policy enforcement tools, $5,000 for training programs.** | **Final Completion Date: February 28, 2025** | **Evaluate existing media use and ownership practices to identify gaps by September 30, 2024.**  **Develop and document policies to ensure that all media used within the organization has a clearly identifiable owner by October 31, 2024.**  **Implement a tracking system to monitor the ownership of media devices within the organization by November 30, 2024.**  **Conduct training sessions for staff on the importance of media ownership and the new policy requirements by December 31, 2024.**  **Perform a compliance audit to ensure all media devices in use have identifiable owners and make adjustments as needed by January 31, 2025.**  **Review and refine the policy based on audit results and finalize the implementation by February 28, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| PE-8 (1) | **Lack of automated mechanisms for maintaining and reviewing visitor access records.**  **Manual processes currently in place are prone to errors and inefficiencies, increasing the risk of unauthorized access.**  **No centralized database management system for visitor records, leading to potential gaps in monitoring and security.** | **Security Office**  **Facilities Management**  **IT Operations** | **Funded: Implementation of an automated database management system for visitor records, including system integration and staff training.**  **Estimated Cost: $30,000 for system acquisition and deployment, $10,000 for training and integration.** | **Final Completion Date: April 30, 2025** | **Evaluate current visitor access record maintenance processes and identify automation requirements by September 30, 2024.**  **Select and procure a suitable automated database management system for maintaining visitor access records by October 31, 2024.**  **Deploy and configure the automated system, ensuring it integrates with existing security and access control systems by January 15, 2025.**  **Train security and facilities management personnel on the use of the new system, focusing on maintaining and reviewing visitor records by February 28, 2025.**  **Conduct a pilot run of the automated system and gather feedback for final adjustments by March 31, 2025.**  **Finalize system deployment and begin regular reviews of visitor access records using the automated system by April 30, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| PL-2 | **Inadequate development and documentation of comprehensive system security and privacy plans.**  **Lack of coordination between system security plans and organizational enterprise architecture, leading to inconsistencies.**  **Insufficient regular reviews and updates to security and privacy plans, potentially leaving the system vulnerable to evolving threats.** | **Information Security Office**  **Privacy Office**  **System Owners** | **Funded: Development and integration of security and privacy plans, including training and system updates.**  **Estimated Cost: $40,000 for plan development and integration, $10,000 for training and continuous updates.** | **Final Completion Date: June 30, 2025** | **Develop and document security and privacy plans consistent with the organization’s enterprise architecture by October 31, 2024. This includes defining system components and operational context.**  **Identify and assign roles and responsibilities related to security and privacy plan implementation by November 30, 2024.**  **Conduct a privacy risk assessment for systems processing personally identifiable information by December 31, 2024.**  **Establish and describe the operational environment for systems and dependencies on other systems by January 31, 2025.**  **Provide an overview of the security and privacy requirements and identify relevant control baselines by February 28, 2025.**  **Review and approve the security and privacy plans by the authorizing official by March 31, 2025.**  **Distribute copies of the plans and ensure all changes are communicated to relevant personnel by April 30, 2025.**  **Set up a regular review process to update the plans in response to system changes or control assessments by June 30, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| PS-3 | **Inadequate or inconsistent screening of individuals prior to granting system access.**  **Lack of a formalized process for rescreening personnel based on organization-defined conditions, leading to potential security risks.**  **Failure to adhere to laws, executive orders, and directives related to personnel screening and rescreening activities.** | **Human Resources (HR) Department**  **Security Office**  **Information Assurance Office** | **Funded: Implementation of a comprehensive personnel screening and rescreening program.**  **Estimated Cost: $25,000 for background check services and system integration, $5,000 for policy updates and training.** | **Final Completion Date: April 30, 2025** | **Develop and document comprehensive screening procedures that align with applicable laws, directives, and standards by October 31, 2024.**  **Define organization-specific conditions and frequencies for rescreening personnel based on the sensitivity of information and roles by November 30, 2024.**  **Implement a system for tracking and managing personnel screening and rescreening activities by January 15, 2025.**  **Provide training for HR and security staff on the updated screening procedures and rescreening protocols by February 28, 2025.**  **Conduct an initial round of screenings and screenings for all personnel with system access by March 31, 2025.**  **Review and adjust the screening and rescreening processes based on feedback and lessons learned by April 15, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| PS-4 | **Lack of a standardized procedure for disabling system access and revoking credentials upon employee termination.**  **Inconsistent execution of exit interviews, leading to gaps in understanding security constraints and accountability for system-related property.**  **Failure to retrieve all security-related organizational property from terminated employees, increasing security risks.** | **Human Resources (HR) Department**  **Information Security Office**  **IT Department** | **Funded: Implementation of automated account termination and property retrieval system.**  **Estimated Cost: $30,000 for system development and integration, $7,500 for staff training and process refinement.** | **Final Completion Date: June 30, 2025** | **Develop and document standardized procedures for system access termination, credential revocation, and property retrieval by November 30, 2024.**  **Integrate the new procedures into the HR and IT systems, including automated triggers for account and credential termination by January 31, 2025.**  **Implement a mandatory exit interview process, including information security topics and property return verification, by March 15, 2025.**  **Conduct training for HR, IT, and security staff on the updated procedures and automated system by April 30, 2025.**  **Perform a pilot run of the new termination procedures with a selected group of upcoming terminations to identify potential issues and areas for improvement by May 31, 2025.**  **Review and finalize the termination procedures and make necessary adjustments based on pilot feedback by June 15, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| RA-3 | **Lack of a comprehensive risk assessment process that includes regular updates and integration of results across organizational levels.**  **Inadequate documentation and dissemination of risk assessment results, leading to insufficient risk management decisions.**  **Failure to update risk assessments in response to significant changes in the system or its environment.** | **Risk Management Office (RMO)**  **Information Security Office (ISO)** | **Funded: Development and implementation of a comprehensive risk assessment framework.**  **Estimated Cost: $50,000 for development of the framework, $15,000 for training, and $10,000 for ongoing updates and reviews.** | **Final Completion Date: July 31, 2025** | **Conduct initial identification of threats, vulnerabilities, and potential impacts by December 15, 2024.**  **Develop and integrate a risk assessment framework that aligns with organizational, mission, and system-level requirements by February 28, 2025.**  **Document risk assessment results in the security and privacy plans or a risk assessment report by March 31, 2025.**  **Establish a review cycle for risk assessments, with the first review to be completed by May 15, 2025.**  **Disseminate risk assessment results to relevant personnel and roles, ensuring proper communication channels are in place by June 15, 2025.**  **Update the risk assessment framework to include triggers for updates in response to system changes by July 15, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| RA-5 | **Inadequate monitoring and scanning for vulnerabilities in the system and hosted applications.**  **Lack of automated tools and processes for vulnerability management, resulting in potential delays in vulnerability identification and remediation.**  **Insufficient sharing of vulnerability information across the organization, leading to repeated vulnerabilities in different systems.** | **Information Security Office (ISO)**  **Vulnerability Management Team (VMT)** | **Funded: Implementation of automated vulnerability management tools and processes.**  **Estimated Cost: $75,000 for procurement and deployment of vulnerability management tools, $25,000 for staff training, and $15,000 for ongoing maintenance and updates.** | **Final Completion Date: December 31, 2025** | **Procure and deploy automated vulnerability monitoring tools that support interoperability and compliance with industry standards by March 31, 2025.**  **Develop and implement standardized procedures for vulnerability monitoring, including enumeration, formatting, and measuring impact, by May 15, 2025.**  **Establish a process for analyzing vulnerability scan reports and documenting results by July 1, 2025.**  **Set up a centralized repository for sharing vulnerability information across relevant organizational roles by August 31, 2025.**  **Develop and integrate a response plan for remediation of vulnerabilities within organization-defined response times by October 31, 2025.**  **Finalize and fully integrate the vulnerability management process, including regular updates of scanning tools, by December 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| RA-5 (2) | **The system's vulnerability scanning process does not include frequent updates to reflect newly discovered vulnerabilities, resulting in potential security gaps.** | **Information Security Office (ISO)**  **Vulnerability Management Team (VMT)** | **Funded: Implementation of automated processes for updating vulnerability databases.**  **Estimated Cost: $20,000 for automation tools, $10,000 for staff training, and $5,000 for ongoing maintenance.** | **Final Completion Date: November 30, 2025** | **Develop and implement a policy for updating the list of vulnerabilities to be scanned based on new discoveries, organizational-defined frequency, and prior to new scans by February 28, 2025.**  **Procure and deploy automated tools that enable real-time updates to the system’s vulnerability scanning list by March 31, 2025.**  **Integrate the new tools with existing vulnerability management systems by April 30, 2025.**  **Conduct staff training on new procedures and tools, ensuring all relevant personnel understand the process for updating vulnerabilities before each scan by June 30, 2025.**  **Test and validate the updated vulnerability scanning process in a controlled environment by September 30, 2025.**  **Fully operationalize the updated scanning process across the organization by November 30, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-4 | **The current system does not adequately prevent unauthorized and unintended information transfer via shared system resources, potentially leading to exposure of sensitive information.** | **Information Security Office (ISO)**  **System Administration Team** | **Funded: Implementation of access control mechanisms, data sanitization tools, and system upgrades.**  **Estimated Cost: $30,000 for tools, $15,000 for staff training, and $10,000 for system integration.** | **Final Completion Date: December 31, 2025** | **Conduct a system audit to identify areas where shared system resources may lead to unintended information transfer by February 28, 2025.**  **Develop and implement policies for data sanitization and residual information protection in shared system resources by March 31, 2025.**  **Upgrade system resources to include mechanisms that prevent unauthorized access to previously used resources by April 30, 2025.**  **Integrate access control features to enforce proper release and reallocation of system resources by June 30, 2025.**  **Train system administrators and users on new procedures and mechanisms by September 30, 2025.**  **Perform testing and validation to ensure that shared resources are appropriately managed and do not retain sensitive information after use by November 30, 2025.**  **Fully operationalize the new processes and controls by December 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-7 | **The organization lacks comprehensive boundary protection mechanisms, which may lead to vulnerabilities at external and internal interfaces, increasing the risk of unauthorized access and data breaches.** | **Information Technology (IT) Department**  **Network Security Team** | **Funded: Implementation of firewalls, gateways, and other boundary protection devices, including staff training and system upgrades.**  **Estimated Cost: $75,000 for hardware and software, $20,000 for staff training, and $15,000 for system integration and testing.** | **Final Completion Date: March 31, 2025** | **Conduct a comprehensive network audit to identify vulnerabilities at managed interfaces by October 15, 2024.**  **Design and implement subnetworks for publicly accessible system components, ensuring logical separation from internal networks by December 31, 2024.**  **Procure and configure boundary protection devices, including firewalls, routers, and intrusion detection systems, by January 31, 2025.**  **Integrate monitoring tools to control and monitor communications at key internal and external interfaces by February 28, 2025.**  **Conduct staff training sessions on new boundary protection measures and monitoring tools by March 15, 2025.**  **Test and validate the new boundary protection measures to ensure they are functioning as intended by March 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-7 (3) | **The system does not effectively limit the number of external network connections, which can lead to increased risk of unauthorized access and reduced efficiency in monitoring inbound and outbound communications traffic.** | **Information Security Office (ISO)**  **Network Security Team** | **Funded: Implementation of network access control mechanisms and configuration adjustments.**  **Estimated Cost: $30,000 for network reconfiguration, $10,000 for staff training, and $5,000 for ongoing monitoring.** | **Final Completion Date: March 31, 2025** | **Assess current external network connections and identify unnecessary access points by October 15, 2024.**  **Develop and implement a plan to limit external connections, including transitioning from IPv4 to IPv6, while maintaining network integrity by December 31, 2024.**  **Reconfigure network access points and implement necessary monitoring tools by January 31, 2025.**  **Conduct training sessions for the network security team on new access control configurations and monitoring procedures by February 28, 2025.**  **Test and validate the reconfigured network connections to ensure security and performance by March 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-7 (5) | **The system currently allows all network communications traffic by default, increasing the risk of unauthorized access. There is no implemented policy to deny traffic by default and allow only approved traffic by exception.** | **Information Security Office (ISO)**  **Network Security Team** | **Funded: Implementation of a deny-by-default, allow-by-exception policy at network interfaces.**  **Estimated Cost: $25,000 for policy development and implementation, $15,000 for network configuration tools, and $10,000 for staff training.** | **Final Completion Date: April 30, 2026** | **Assess current network traffic policies and identify areas where deny-by-default can be implemented by October 31, 2024.**  **Develop and document a policy for denying network communications traffic by default and allowing traffic by exception, including defining necessary exceptions by December 31, 2024.**  **Configure managed network interfaces to enforce the new deny-by-default policy by February 29, 2025.**  **Train network security personnel on implementing and maintaining the deny-by-default, allow-by-exception policy by March 31, 2025.**  **Test and validate the new network traffic policy in a controlled environment to ensure it effectively blocks unauthorized traffic while allowing necessary communications by April 30, 2025.**  **Fully operationalize the new policy across all relevant network interfaces by April 30, 2026.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-7 (10) | **The current system lacks robust measures to prevent the exfiltration of sensitive information, posing a significant risk of data loss. There is no established process for conducting regular exfiltration tests.** | **Information Security Office (ISO)**  **Data Protection Team** | **Funded: Implementation of exfiltration prevention mechanisms and regular testing protocols.**  **Estimated Cost: $30,000 for the deployment of data loss prevention tools, $15,000 for ongoing exfiltration tests, and $10,000 for staff training.** | **Final Completion Date: August 31, 2025** | **Assess current data exfiltration risks and identify critical points for implementing prevention mechanisms by October 31, 2024.**  **Develop and implement a policy for preventing data exfiltration, including specific protocols for internal endpoints, external boundaries, and managed interfaces by December 31, 2024.**  **Procure and deploy data loss prevention tools, including deep packet inspection firewalls and XML gateways, by February 28, 2025.**  **Conduct initial exfiltration tests to validate the effectiveness of the new prevention mechanisms by March 31, 2025.**  **Train relevant personnel on monitoring and responding to exfiltration threats by April 30, 2025.**  **Establish a schedule for regular exfiltration tests and integrate this schedule into the organization's broader security testing framework by May 31, 2025.**  **Fully operationalize exfiltration prevention measures across the organization by August 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-10 |  |  |  |  |  | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-10 | **The system currently lacks a consistent mechanism to automatically terminate network connections after a communication session ends or after a specified period of inactivity, increasing the risk of unauthorized access.** | **Information Security Office (ISO)**  **Network Operations Team** | **Funded: Implementation of automated network disconnect mechanisms.**  **Estimated Cost: $25,000 for software integration, $10,000 for network monitoring enhancements, and $5,000 for staff training.** | **Final Completion Date: July 31, 2025** | **Assess current network configurations to identify gaps in the termination of network connections after session inactivity by October 31, 2024.**  **Develop and implement a policy defining specific inactivity time periods for different types of network access by December 31, 2024.**  **Procure and deploy tools to automate the termination of network connections after communication sessions end or after the defined inactivity periods by February 28, 2025.**  **Integrate automated disconnect mechanisms into existing network infrastructure by April 30, 2025.**  **Conduct staff training on the new network disconnect procedures by May 31, 2025.**  **Test and validate the network disconnect process to ensure proper functionality across all relevant systems by June 30, 2025.**  **Fully operationalize automated network disconnection across the organization by July 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-12 | **The organization lacks a consistent and secure process for establishing and managing cryptographic keys, potentially compromising data integrity and confidentiality.** | **Information Security Office (ISO)**  **Cryptographic Services Team** | **Funded: Implementation of automated cryptographic key management solutions.**  **Estimated Cost: $30,000 for key management software, $15,000 for integration, and $5,000 for staff training.** | **Final Completion Date: August 31, 2025** | **Assess current cryptographic key management practices and identify gaps in key generation, distribution, storage, access, and destruction by October 31, 2024.**  **Develop and implement a policy for cryptographic key management, including organization-defined requirements for key management by December 31, 2024.**  **Procure and deploy automated key management solutions by January 31, 2025.**  **Integrate the new key management system with existing infrastructure by March 31, 2025.**  **Conduct staff training on the new cryptographic key management procedures by May 31, 2025.**  **Test and validate the key management process in a controlled environment by July 31, 2025.**  **Fully operationalize the cryptographic key management process across the organization by August 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-13 | **The organization lacks a defined and consistently implemented cryptographic protection policy, resulting in potential vulnerabilities related to the encryption and decryption of sensitive information.** | **Information Security Office (ISO)**  **Cryptographic Services Team** | **Funded: Development and implementation of cryptographic protection policies and deployment of necessary cryptographic tools.**  **Estimated Cost: $25,000 for policy development, $40,000 for cryptographic tools and software, and $10,000 for staff training.** | **Final Completion Date: August 31, 2025** | **Assess current cryptographic uses within the organization and determine the organization-defined cryptographic uses by October 31, 2024.**  **Develop and implement a cryptographic protection policy that specifies the types of cryptography required for each cryptographic use by December 31, 2024.**  **Procure and deploy cryptographic tools that align with the new policy by February 28, 2025.**  **Integrate the new cryptographic tools with existing systems and workflows by April 30, 2025.**  **Conduct staff training on the new cryptographic protection policy and tools by June 30, 2025.**  **Test and validate the cryptographic protection process in a controlled environment by July 31, 2025.**  **Fully operationalize the cryptographic protection process across the organization by August 31, 2025.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-19 | **The withdrawal of SC-19, specific to Voice Over Internet Protocol (VoIP) security, has left a gap in the organization’s security controls. VoIP is now treated as any other technology or protocol, which requires a reassessment to ensure all necessary security measures are in place.** | **IT Security Team** | **Funded – An estimated $15,000 will be allocated from the current IT security budget. This includes costs for staff time, external audit fees, and potential acquisition of additional security tools if needed.** | **November 30, 2024** | **Assess and Update Communication Security Policies:**  **Review existing communication security policies to ensure they adequately cover VoIP. Identify and address any gaps.**  **Completion Date: September 30, 2024**  **VoIP Technology Assessment and Security Implementation:**  **Evaluate current VoIP systems and implement required security measures such as encryption, secure authentication, and network segmentation. Deploy additional security tools as necessary.**  **Completion Date: October 31, 2024**  **External Security Audit:**  **Conduct an external audit to assess the effectiveness of the newly implemented VoIP security measures and ensure compliance with the updated policies.**  **Completion Date: November 15, 2024**  **Address Audit Findings:**  **Review and address any issues or recommendations from the external audit to ensure the VoIP system is fully secure and compliant.**  **Completion Date: November 30, 2024** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-15 | **The organization lacks controls to prevent unauthorized remote activation of collaborative computing devices and applications. Additionally, there is no system in place to provide clear indications of use when these devices are activated, potentially leading to unauthorized surveillance or data leaks.** | **IT Security Team, Collaborative Technology Support Team** | **Funded – Resources will cover the development of policies, the deployment of technology solutions to prevent unauthorized remote activation, and the installation of indicators to signal device usage.**  **Estimated Cost: $15,000 for policy development and staff training, $25,000 for technology solutions (e.g., software to manage device permissions and indicators), and $10,000 for integrating and testing these systems.** | **Final Completion Date: December 31, 2024** | **Develop and Implement a Remote Activation Policy:**  **Create a comprehensive policy that defines organization-specific exceptions where remote activation of collaborative devices is allowed and prohibit remote activation in all other scenarios.**  **Completion Date: September 30, 2024**  **Deploy Technology Solutions to Enforce Remote Activation Policy:**  **Implement software and hardware controls that prevent unauthorized remote activation of collaborative computing devices and ensure only approved exceptions are enforced.**  **Completion Date: October 31, 2024**  **Install Indicators of Use on Collaborative Devices:**  **Integrate visible and/or audible indicators on collaborative devices (e.g., cameras, microphones) that clearly signal when they are in use or have been remotely activated, ensuring transparency for users.**  **Completion Date: November 30, 2024**  **Training and Awareness Program:**  **Conduct training sessions for staff on the new policies and the correct usage of collaborative devices, including how to recognize the indicators of use.**  **Completion Date: December 15, 2024**  **Final Validation and Testing:**  **Perform final system tests and validation exercises to ensure all controls and indicators are functioning as intended and that the remote activation policy is fully enforceable.**  **Completion Date: December 31, 2024** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-23 | **The organization lacks sufficient mechanisms to protect the authenticity of communication sessions, which may result in vulnerabilities such as man-in-the-middle attacks, session hijacking, and the insertion of false information during sessions.** | **IT Security Team** | **Resource Estimate: Funded – The resources will cover the deployment of session authentication protocols, acquisition of necessary security tools, and staff training on session security.**  **Estimated Cost: $20,000 for implementing session authentication tools, $10,000 for policy development and staff training, and $15,000 for integrating these tools with existing systems.** | **Final Completion Date: January 31, 2025** | **Assess Current Session Authentication Mechanisms:**  **Review and evaluate existing session authentication mechanisms in place within the organization to identify any gaps or vulnerabilities.**  **Completion Date: September 30, 2024**  **Develop and Implement Session Authentication Policy:**  **Create and enforce a policy that mandates the use of session authentication protocols across all communication systems to protect against unauthorized session access and attacks.**  **Completion Date: October 31, 2024**  **Deploy Advanced Session Authentication Tools:**  **Implement advanced session authentication tools (e.g., multi-factor authentication, encryption) to ensure the security and authenticity of communication sessions.**  **Completion Date: November 30, 2024**  **Integration with Existing Systems:**  **Integrate the new session authentication tools and protocols with existing communication systems, ensuring minimal disruption and full compatibility.**  **Completion Date: December 31, 2024**  **Conduct Staff Training and Awareness Program:**  **Provide training for staff on the importance of session authenticity and the correct use of the newly implemented tools and protocols.**  **Completion Date: January 15, 2025**  **Final Testing and Validation:**  **Perform final tests to validate the effectiveness of the session authentication mechanisms, ensuring they adequately protect against the identified risks (e.g., man-in-the-middle attacks).**  **Completion Date: January 31, 2025** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-28 | **The organization currently lacks robust mechanisms to ensure the protection of information at rest, which may expose sensitive data to unauthorized access, alteration, or compromise.** | **IT Security Team, Data Management Team** | **Resource Estimate: Funded – Resources are required for acquiring encryption tools, developing policies, implementing protection mechanisms, and training staff on best practices for data security.**  **Estimated Cost: $30,000 for cryptographic tools and licenses, $20,000 for policy development and implementation, and $10,000 for training and system integration.** | **Final Completion Date: March 31, 2025** | **Assess Information at Rest and Identify Critical Data:**  **Conduct a comprehensive review of all information at rest to identify critical and sensitive data that requires protection.**  **Completion Date: October 31, 2024**  **Develop and Implement Information at Rest Protection Policy:**  **Establish a policy that mandates the protection of information at rest, specifying the use of encryption, access controls, and integrity checks.**  **Completion Date: November 30, 2024**  **Procure and Deploy Cryptographic Mechanisms:**  **Acquire and deploy cryptographic tools to encrypt sensitive information at rest, ensuring the confidentiality and integrity of stored data.**  **Completion Date: December 31, 2024**  **Implement Additional Protection Mechanisms (e.g., WORM, File Share Scanning):**  **Implement Write-Once-Read-Many (WORM) technologies and file share scanning to further protect the integrity of data at rest.**  **Completion Date: January 31, 2025**  **Staff Training on Information at Rest Protection:**  **Train relevant staff on the new policies, tools, and procedures for protecting information at rest, including best practices for data security.**  **Completion Date: February 28, 2025**  **Final Testing and Validation:**  **Conduct final tests and validations to ensure that all protection mechanisms are functioning correctly and that information at rest is adequately secured.** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SI-3 | **The organization lacks comprehensive malicious code protection mechanisms at system entry and exit points. The existing defenses are outdated and do not effectively detect, block, or respond to new and emerging threats such as polymorphic malicious code.** | **IT Security Team, Systems Administration Team** | **Funded – Resources will be allocated for upgrading existing anti-malware solutions, implementing advanced detection mechanisms, and training staff on the updated protocols.**  **Estimated Cost: $50,000 for advanced anti-malware tools and licenses, $15,000 for policy development and integration, and $10,000 for staff training.** | **Final Completion Date: April 30, 2025** | **Upgrade Malicious Code Protection Mechanisms:**  **Implement both signature-based and non-signature-based malicious code protection mechanisms at all system entry and exit points, including firewalls, servers, and endpoint devices. This includes deploying solutions that use AI and heuristic analysis for detecting unknown threats.**  **Completion Date: December 31, 2024**  **Develop and Implement Configuration Management Policy:**  **Establish a robust configuration management policy that ensures all malicious code protection mechanisms are automatically updated as new releases become available. This includes defining procedures for periodic scans and real-time scanning of files.**  **Completion Date: January 31, 2025**  **Configure and Test Malicious Code Protection:**  **Configure the malicious code protection tools to:**  **Perform periodic scans of systems (e.g., weekly scans).**  **Conduct real-time scans of files from external sources (e.g., downloaded files, emails) at endpoints and network entry and exit points.**  **Block or quarantine detected malicious code and automatically alert designated security personnel.**  **Address and document handling procedures for false positives. Completion Date: February 28, 2025**  **Training and Awareness Program:**  **Train IT and security personnel on the updated tools and procedures, including the management of false positives and response protocols. This will ensure that staff can effectively manage and respond to malicious code detections.**  **Completion Date: March 31, 2025**  **Final Testing and Validation:**  **Perform comprehensive testing of the entire system to ensure that all malicious code protection mechanisms are functioning as intended. Validate the effectiveness of the configuration management policy and the system’s ability to detect, block, and respond to both known and unknown threats.**  **Completion Date: April 30, 2025** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SI-3(1) | **The SI-3(1) control for central management of malicious code protection has been withdrawn and incorporated into PL-9. As a result, there may be gaps in centralized management and oversight of malicious code protection mechanisms across the organization.** | **IT Security Team, Policy Management Office** | **Resource Estimate: Funded – Costs will cover the review and integration of SI-3(1) requirements into PL-9, including policy updates and implementation of centralized management tools where necessary.**  **Estimated Cost: $10,000 for policy review and updates, $15,000 for the integration of centralized management tools, and $5,000 for training and staff awareness programs.** | **Final Completion Date: December 31, 2024** | **Review and Update PL-9 Policy to Incorporate SI-3(1) Requirements:**  **Conduct a detailed review of PL-9 (Management Policy) to identify how the requirements of SI-3(1) for central management of malicious code protection can be incorporated. Update the policy accordingly.**  **Completion Date: October 31, 2024**  **Implement Centralized Management Tools for Malicious Code Protection:**  **Deploy or upgrade centralized management tools that align with the updated PL-9 policy to ensure consistent and effective oversight of malicious code protection across the organization.**  **Completion Date: November 30, 2024**  **Training and Awareness Program:**  **Conduct training sessions for IT and security personnel to ensure they understand the updated policy and are proficient in using the centralized management tools.**  **Completion Date: December 15, 2024**  **Final Testing and Validation:**  **Perform final tests to ensure that the centralized management of malicious code protection is effectively integrated and that all systems comply with the updated PL-9 policy.**  **Completion Date: December 31, 2024** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SC-3(2) | **The automatic update feature for malicious code protection tools, previously covered under SI-3(2), is not in place. With the withdrawal and incorporation of this control into SI-3, there may be a risk that critical updates to malicious code protection mechanisms are not consistently applied, leaving the organization vulnerable to new threats.** | **IT Security Team, Systems Administration Team** | **Resource Estimate: Funded – Resources will be allocated to ensure that the automatic update mechanisms are fully integrated into the existing SI-3 control framework and that the tools are properly configured to receive and apply updates.**  **Estimated Cost: $5,000 for policy update and tool configuration, $10,000 for system integration and testing.** | **Final Completion Date: November 30, 2024** | **Review and Update SI-3 Policy to Include Automatic Updates:**  **Ensure that the automatic update requirements from SI-3(2) are fully integrated into the SI-3 control. Update the SI-3 policy to reflect this incorporation and ensure that all malicious code protection tools are configured for automatic updates.**  **Completion Date: September 30, 2024**  **Configure Malicious Code Protection Tools for Automatic Updates:**  **Verify and configure all existing malicious code protection tools to ensure they automatically receive and apply updates as they become available. This includes both signature-based and non-signature-based tools.**  **Completion Date: October 31, 2024**  **Testing and Validation:**  **Conduct thorough testing to confirm that the tools are correctly receiving and applying updates. Ensure there is no disruption to service or protection during the update process.**  **Completion Date: November 30, 2024** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SI-4 | **The organization currently has insufficient system monitoring capabilities, leaving it vulnerable to undetected attacks, unauthorized access, and system misuse. The existing monitoring tools and processes are outdated and do not cover all critical points within the system.** | **IT Security Team, Network Operations Center (NOC)** | **Resource Estimate: Funded – Resources will be dedicated to upgrading system monitoring tools, implementing new monitoring strategies, and training personnel on enhanced monitoring procedures.**  **Estimated Cost: $60,000 for advanced monitoring tools, $20,000 for policy and procedure updates, and $15,000 for staff training and system integration.** | **Final Completion Date: June 30, 2025** | **Assess Current System Monitoring Capabilities:**  **Conduct a thorough assessment of the current system monitoring tools and techniques to identify gaps and areas for improvement, focusing on both internal and external monitoring.**  **Completion Date: November 30, 2024**  **Develop and Implement System Monitoring Policy:**  **Update the system monitoring policy to include organization-defined monitoring objectives, techniques, and methods. Ensure the policy covers detection of attacks, unauthorized access, and the analysis of detected events and anomalies.**  **Completion Date: January 31, 2025**  **Deploy Advanced Monitoring Tools and Devices:**  **Implement advanced intrusion detection and prevention systems, network monitoring software, and other tools to monitor critical points within the system. This includes strategic placement of monitoring devices to minimize impact on network throughput.**  **Completion Date: March 31, 2025**  **Training and Awareness Program:**  **Train IT and security personnel on the new monitoring tools, policies, and procedures. Emphasize the importance of real-time monitoring, anomaly detection, and the correct response to detected threats.**  **Completion Date: April 30, 2025**  **Final Testing and Validation:**  **Conduct final tests to ensure the monitoring tools and procedures are effectively detecting and responding to threats. Validate that the system monitoring activities meet the organization-defined objectives and adjust as necessary based on risk assessments.**  **Completion Date: June 30, 2025** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SI-4(4) | **The organization does not have defined criteria for detecting unusual or unauthorized activities in inbound and outbound communications traffic, nor does it consistently monitor this traffic for potential security threats. This gap could lead to undetected malicious activities such as the presence of malicious code, unauthorized use of credentials, or unauthorized data exfiltration.** | **IT Security Team, Network Operations Center (NOC)** | **Resource Estimate: Funded – Resources will be allocated to develop criteria, implement monitoring tools, and train staff on the identification of unusual or unauthorized activities.**  **Estimated Cost: $25,000 for the development and deployment of monitoring criteria and tools, $10,000 for policy updates, and $5,000 for staff training and testing.** | **Final Completion Date: April 30, 2025** | **Develop Criteria for Unusual or Unauthorized Activities:**  **Define and document the specific criteria for what constitutes unusual or unauthorized activities in inbound and outbound communications traffic, tailored to the organization's operational environment.**  **Completion Date: December 31, 2024**  **Implement Traffic Monitoring Tools:**  **Deploy or upgrade monitoring tools that can continuously monitor inbound and outbound communications traffic according to the defined criteria. This includes tools that detect the presence of malicious code, unauthorized credential usage, and data exfiltration attempts.**  **Completion Date: February 28, 2025**  **Policy Update and Integration:**  **Update the organization’s monitoring policy to include the newly defined criteria and monitoring procedures for communications traffic. Ensure the policy is integrated into the overall system monitoring framework.**  **Completion Date: March 15, 2025**  **Training and Awareness Program:**  **Train relevant staff on the new criteria and monitoring tools, focusing on how to identify and respond to unusual or unauthorized activities in communications traffic.**  **Completion Date: March 31, 2025**  **Final Testing and Validation:**  **Conduct a comprehensive testing phase to validate the effectiveness of the monitoring tools and criteria. Ensure that the system correctly identifies and responds to potential threats in communications traffic.**  **Completion Date: April 30, 2025** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |
| SI-5 | **The organization currently lacks a streamlined process for receiving, generating, and disseminating security alerts, advisories, and directives. This gap could lead to delays in implementing critical security measures, resulting in vulnerabilities to cyber threats.** | **IT Security Team, Compliance Office** | **Resource Estimate: Funded – Resources will be dedicated to establishing procedures for managing security alerts and directives, implementing necessary communication tools, and training staff.**  **Estimated Cost: $15,000 for communication tools and infrastructure, $10,000 for policy development and procedure updates, and $5,000 for staff training.** | **Final Completion Date: March 31, 2025** | **Establish Communication Channels for Receiving External Alerts:**  **Set up dedicated communication channels with external organizations like CISA to ensure continuous and reliable receipt of security alerts, advisories, and directives.**  **Completion Date: November 30, 2024**  **Develop Internal Procedures for Generating and Disseminating Alerts:**  **Create and implement internal procedures for generating security alerts and advisories based on received information and disseminating them to relevant personnel, organizational elements, and external partners as needed.**  **Completion Date: December 31, 2024**  **Implement Security Alert Communication Tools:**  **Deploy tools and platforms that facilitate the rapid dissemination of security alerts and directives to all relevant parties within the organization.**  **Completion Date: January 31, 2025**  **Training and Awareness Program:**  **Train staff on the new procedures and tools for handling security alerts, advisories, and directives, emphasizing the importance of timely compliance and the potential consequences of delays.**  **Completion Date: February 28, 2025**  **Testing and Validation:**  **Conduct tests to ensure that the communication channels, procedures, and tools are working effectively. Validate the organization's ability to receive, generate, and disseminate security alerts and directives in a timely manner.**  **Completion Date: March 31, 2025** | **To be updated as necessary during project execution.** | **During a security audit or risk assessment, it was identified that information flow controls were either inadequate or missing entirely, leading to potential data leakage or security policy violations.** | **Complete** |