Risk Assessment Report

Prepared by: Felix Aburto/Cyber Security Specialists

Date: 08-31-2024

# Executive Summary

This risk assessment provides a comprehensive evaluation of the most critical threats facing our organization's security controls and processes. Our analysis has prioritized risks with an Overall Risk Score of 64 and 56, highlighting vulnerabilities that pose a significant threat to the integrity and security of our operations. The assessment identifies 32 high-risk items and 20 medium-risk items, each of that demands immediate or medium-term action to mitigate potential impacts. Addressing these vulnerabilities is essential to maintaining our organization's resilience against emerging threats and safeguarding our assets and data.

# Key Findings

During the assessment, several controls were identified with high-risk scores. These risks are categorized as critical and require immediate attention to mitigate potential threats to the organization's security posture.

- High-Risk Items: 32 (Score 64)

- Medium-Risk Items: 20 (Score 56)

- Overall Risk Average : 49 (Medium-Risk)

# Detailed Risk Analysis

## Personnel Termination - Risk Score: 64

- Threat: unauthorized access to CUI by former or transferred employees.

- Vulnerability: Unauthorized access

- Risk Explanation: individuals who should no longer have access to CUI may still be able to access sensitive systems, leading to potential security incidents. Implementing these controls mitigates the risk by ensuring that access is promptly revoked or modified during personnel changes, thereby reducing the likelihood and impact of unauthorized access.

## Vulnerability Monitoring and Scanning | Update Vulnerabilities to Be Scanning - Risk Score: 64

- Threat: known vulnerabilities being exploited by attackers.

- Vulnerability: Data modification/ destruction/ corruption

- Risk Explanation: the organization may fail to address critical vulnerabilities, allowing attackers to exploit these weaknesses. This may lead to significant security incidents, including data breaches and system compromises. Implementing this control mitigates the risk by ensuring that vulnerabilities are remediated in accordance with their assessed risk, prioritizing efforts to address the most critical vulnerabilities first, thereby reducing the likelihood and impact of security breaches.

## Vulnerability Monitoring and Scanning - Risk Score: 64

- Threat: unpatched vulnerabilities being exploited by attackers.

- Vulnerability: Data modification/ destruction/ corruption

- Risk Explanation: critical vulnerabilities in systems and applications may go undetected, allowing attackers to exploit these weaknesses. This may lead to significant security incidents, including data breaches and system compromises. Implementing this control mitigates the risk by ensuring that vulnerabilities are regularly identified and addressed, reducing both the likelihood and impact of potential security breaches.

## Incident Handling - Risk Score: 64

- Threat: inability to effectively respond to security incidents.

- Vulnerability: Data Loss/Information Disclosure

- Risk Explanation: the organization may be unable to manage and mitigate the effects of security incidents effectively. This may result in longer recovery times, greater damage, and an increased likelihood of repeat incidents. Establishing a comprehensive incident-handling capability mitigates this risk by ensuring that the organization is prepared to respond to incidents promptly and efficiently, thereby minimizing the impact and ensuring a swift return to normal operations.

## Cryptographic Key Establishment and Management - Risk Score: 64

- Threat: unauthorized access due to compromised or poorly managed cryptographic keys

- Vulnerability: Unauthorized access

- Risk Explanation: cryptographic keys could be compromised or mismanaged, leading to unauthorized access to encrypted data. Implementing this control mitigates the risk by ensuring that cryptographic keys are securely generated, distributed, stored, and eventually destroyed, thus maintaining the integrity and confidentiality of the encrypted data and reducing both the likelihood and impact of potential security breaches.

## Authenticator Management | Protection of Authenticators - Risk Score: 64

- Threat: password exposure

- Vulnerability: Unauthorized access

- Risk Explanation: passwords may be exposed to unauthorized parties during storage or transmission, leading to a high likelihood of compromise. This could result in severe security incidents, such as unauthorized access, data breaches, and loss of sensitive information. Implementing cryptographic protection for password storage and transmission mitigates this risk by ensuring that even if passwords are intercepted or accessed, they may not be easily deciphered, thereby enhancing the overall security of the organization's authentication processes.

## Boundary Protection | Prevent Exfiltration - Risk Score: 64

- Threat: unauthorized access or data breaches via remote devices.

- Vulnerability: Unauthorized access

- Risk Explanation: remote devices could simultaneously connect to organizational systems and external networks, creating a vulnerability that attackers could exploit. Implementing this control mitigates the risk by ensuring that remote devices may not establish split tunneling, thereby protecting the internal network from external threats and reducing both the likelihood and impact of potential security incidents.

## Boundary Protection | Deny by Default — Allow by Exception - Risk Score: 64

- Threat: unauthorized access or data breaches due to overly permissive network traffic rules.

- Vulnerability: Unauthorized access

- Risk Explanation: unauthorized or malicious network traffic could enter the network, leading to security breaches and other harmful events. Implementing a deny-by-default, allow-by-exception policy mitigates this risk by ensuring that only authorized communications are permitted, significantly reducing both the likelihood and impact of potential security incidents.

## Authenticator Management - Risk Score: 64

- Threat: unauthorized access

- Vulnerability: Unauthorized access

- Risk Explanation: users may create weak or easily guessable passwords, increasing the likelihood of unauthorized access to systems. This may result in severe security incidents, such as data breaches and system compromises. Implementing this control mitigates the risk by ensuring that all passwords meet minimum complexity requirements and that a change of characters is enforced, thereby reducing the chances of passwords being compromised and enhancing overall security.

## Collaborative Computing Devices and Applications - Risk Score: 64

- Threat: risk of unauthorized monitoring or recording via remote activation of these devices.

- Vulnerability: Data Loss/Information Disclosure

- Risk Explanation: collaborative computing devices could be remotely activated without user awareness, leading to unauthorized monitoring or recording of sensitive information. Implementing this control mitigates the risk by ensuring that remote activation is prohibited and that users are always aware when these devices are in use, reducing both the likelihood and impact of unauthorized surveillance.

## Plan of Action and Milestones - Risk Score: 64

- Threat: unresolved vulnerabilities and deficiencies remaining in the system.

- Vulnerability: Data Loss/Information Disclosure

- Risk Explanation: the organization may fail to effectively address security deficiencies and vulnerabilities, leading to prolonged exposure to threats. This may result in significant security incidents, including data breaches and operational disruptions. Implementing this control mitigates the risk by ensuring that the organization has a clear plan and timeline for addressing and correcting identified issues, thereby reducing the likelihood and impact of potential security breaches.

## Continuous Monitoring - Risk Score: 64

- Threat: security controls becoming ineffective over time.

- Vulnerability: Damage/destruction of assets

- Risk Explanation: security controls may become outdated or ineffective, leading to increased vulnerability to attacks. Continuous monitoring ensures that the organization may quickly detect and respond to changes in the environment, thereby maintaining the effectiveness of security controls. Implementing this control mitigates the risk by enabling proactive management of security controls, reducing both the likelihood and impact of potential security breaches.

## Boundary Protection | Access Points - Risk Score: 64

- Threat: external attackers gaining access to internal networks.

- Vulnerability: Unauthorized access

- Risk Explanation: publicly accessible systems could serve as entry points for attackers to access internal networks, leading to serious security incidents. Implementing this control mitigates the risk by ensuring that public-facing components are isolated in separate subnetworks, reducing the likelihood and impact of lateral movement from compromised public systems to internal networks.

## Identification and Authentication (organizational Users) | Multi-factor Authentication to Privileged Accounts - Risk Score: 64

- Threat: unauthorized access to both privileged and non-privileged accounts

- Vulnerability: Unauthorized access

- Risk Explanation: the organization is highly vulnerable to unauthorized access to both privileged and non-privileged accounts. The absence of multifactor authentication means that once an attacker compromises a password, they may easily gain access to sensitive systems, leading to potentially catastrophic consequences. Implementing multifactor authentication mitigates this risk by adding an additional layer of security, making unauthorized access significantly more difficult and reducing the overall risk to the organization's systems and data.

## Identification and Authentication (organizational Users) - Risk Score: 64

- Threat: unauthorized access to organizational systems

- Vulnerability: Unauthorized access

- Risk Explanation: unauthorized users, processes, or devices may gain access to the organization's systems, leading to significant security incidents. This could result in data breaches, system compromises, and a loss of trust in the organization's ability to protect its information. Implementing this control mitigates the risk by ensuring that all entities are properly authenticated before being granted access, thereby reducing the likelihood and impact of unauthorized access to the organization's systems and data.

## Policy and Procedures - Risk Score: 64

- Threat: unauthorized access to systems and data

- Vulnerability: Unauthorized access

- Risk Explanation: unauthorized users, processes, or devices may gain access to the organization's systems, leading to significant security incidents. This could result in data breaches, system compromises, and a loss of trust in the organization's ability to protect its information. Implementing this control mitigates the risk by ensuring that all users, processes, and devices are properly identified and authenticated before being granted access, thereby reducing the likelihood and impact of unauthorized access to the organization's systems and data.

## Cryptographic Protection - Risk Score: 64

- Threat: unauthorized access to CUI during transmission

- Vulnerability: Unauthorized access

- Risk Explanation: CUI could be intercepted during transmission, leading to unauthorized access and potential security incidents. Implementing cryptographic mechanisms mitigates the risk by ensuring that all transmitted CUI is encrypted, thus protecting its confidentiality and reducing both the likelihood and impact of potential breaches.

## Boundary Protection - Risk Score: 64

- Threat: unauthorized access to or tampering with communications at critical system boundaries.

- Vulnerability: Unauthorized access

- Risk Explanation: sensitive information transmitted across system boundaries could be intercepted, modified, or otherwise compromised by unauthorized parties. This may lead to serious security incidents, including data breaches and loss of system integrity. Implementing this control mitigates the risk by ensuring that all communications at key system boundaries are monitored, controlled, and protected, reducing both the likelihood and impact of potential security breaches.

## Media Transport | Cryptographic Protection - Risk Score: 64

- Threat: unauthorized access to CUI during transport.

- Vulnerability: Unauthorized access

- Risk Explanation: CUI on digital media could be exposed during transport, leading to unauthorized access and potentially severe security incidents. Implementing cryptographic mechanisms mitigates this risk by ensuring that the information remains secure and confidential, even if the media is intercepted or accessed during transit. If cryptographic protection is not possible, alternative physical safeguards must be used to protect the media.

## Nonlocal Maintenance - Risk Score: 64

- Threat: unauthorized access to systems during remote maintenance sessions.

- Vulnerability: Unauthorized access

- Risk Explanation: remote maintenance sessions could be accessed by unauthorized individuals, leading to significant security incidents. The lack of multifactor authentication increases the likelihood of unauthorized access, and failing to terminate sessions properly may leave systems exposed to continued attacks. Implementing this control mitigates the risk by requiring multifactor authentication for remote maintenance sessions and ensuring that all sessions are securely terminated after use, thereby reducing the likelihood and impact of potential security breaches.

## Information Flow Enforcement - Risk Score: 64

- Threat: the primary threat is the unauthorized transfer of sensitive information, including Controlled Unclassified Information (CUI). This lack of control over information flow allows data to be improperly transferred between different parts of a system or between systems.

- Vulnerability: Data Loss/Information Disclosure

- Risk Explanation: sensitive information, such as Controlled Unclassified Information (CUI), could flow freely and potentially be transmitted to unauthorized entities or systems. Without proper enforcement of information flow policies, there is a heightened risk of data leaks, breaches, and non-compliance with regulatory requirements, that may lead to significant legal, operational, and reputational consequences for the organization.

## Personnel Screening - Risk Score: 64

- Threat: risk of insider threats.

- Vulnerability: Policy breach

- Risk Explanation: individuals who have not been properly vetted may be granted access to systems containing CUI, leading to an increased likelihood of insider threats and significant security incidents. Implementing this control mitigates the risk by ensuring that all individuals are thoroughly screened before being authorized to access sensitive information, thereby reducing the likelihood and impact of potential insider threats.

## Media Storage - Risk Score: 64

- Threat: unauthorized access, theft, or loss of CUI.

- Vulnerability: Unauthorize Access and disclosed information

- Risk Explanation: CUI on system media may be exposed to unauthorized individuals, leading to serious security incidents, including data breaches and loss of sensitive information. Implementing this control mitigates the risk by ensuring that all media containing CUI is securely stored and physically controlled, reducing the likelihood of unauthorized access and the potential impact of such incidents.

## Remote Access | Protection of Confidentiality and Integrity Using Encryption - Risk Score: 64

- Threat: interception and unauthorized access to sensitive data during remote access sessions.

- Vulnerability: Unauthorized access

- Risk Explanation: remote access sessions may be intercepted and compromised by attackers. Without encryption, sensitive data transmitted during these sessions is vulnerable to unauthorized access, leading to potential data breaches, loss of data integrity, and overall system compromise. This may result in severe operational disruptions, financial loss, legal penalties, and significant damage to the organization's reputation.

## Malicious Code Protection - Risk Score: 64

- Threat: risk of malware infections that may compromise the integrity, confidentiality, and availability of organizational systems and data. Malicious code may lead to unauthorized access, data corruption, data breaches, and significant operational disruptions.

- Vulnerability: Data modification/ destruction/ corruption

- Risk Explanation: organizational systems could become infected with malware, leading to serious security incidents. Implementing this control mitigates the risk by ensuring that designated locations within the system are protected against malicious code, reducing both the likelihood and impact of malware-related security breaches

## Malicious Code Protection | Central Management - Risk Score: 64

- Threat: malware infections that go undetected.

- Vulnerability: Data modification/ destruction/ corruption

- Risk Explanation: malicious code could infiltrate the organization's systems unnoticed, leading to serious security incidents. Implementing this control mitigates the risk by ensuring that all systems are regularly scanned for malware and that files from external sources are checked in real-time, reducing both the likelihood and impact of malware infections.

## Media Transport - Risk Score: 64

- Threat: Unauthorized access

- Vulnerability: unauthorized access or distribution of CUI.

- Risk Explanation: CUI on system media may be accessed by unauthorized individuals, leading to significant security incidents, including data breaches and unauthorized distribution of sensitive information. Implementing this control mitigates the risk by ensuring that only authorized users have access to CUI on system media, thereby reducing the likelihood of unauthorized access and the potential impact of such incidents.

## Media Sanitization - Risk Score: 64

- Threat: Unauthorized access

- Vulnerability: the risk of unauthorized access to CUI through discarded or reused media

- Risk Explanation: CUI could be recovered from media that is improperly sanitized or destroyed, leading to significant security incidents, including data breaches and unauthorized disclosure of sensitive information. Implementing this control mitigates the risk by ensuring that all media containing CUI is thoroughly sanitized or destroyed before disposal or reuse, thereby reducing the likelihood of unauthorized access and the potential impact of such incidents.

## Media Use - Risk Score: 64

- Threat: Data modification/ destruction/ corruption

- Vulnerability: unauthorized data transfer, malware introduction, or data loss through removable media.

- Risk Explanation: removable media could be used inappropriately, leading to significant security incidents such as data breaches, introduction of malware, or loss of sensitive information. Implementing this control mitigates the risk by ensuring that the use of removable media is tightly controlled, authorized, and monitored, thereby reducing the likelihood and impact of such incidents.

## System Monitoring - Risk Score: 64

- Threat: undetected attacks or malicious activities.

- Vulnerability: Data modification/ destruction/ corruption

- Risk Explanation: attacks or malicious activities could go undetected, allowing them to escalate and cause significant harm. Implementing this control mitigates the risk by ensuring that systems are continuously monitored, so potential threats are detected early and may be responded to promptly, reducing both the likelihood and impact of security incidents.

## Unsuccessful Logon Attempts - Risk Score: 64

- Threat: The threat associated with not implementing AC-7 (Unsuccessful Logon Attempts) is the increased risk of brute-force attacks.

- Vulnerability: Unauthorized access

- Risk Explanation: attackers may continuously attempt to guess passwords through brute-force attacks, increasing the likelihood of gaining unauthorized access to user accounts. This may lead to data breaches, system compromise, and potentially further exploitation of the organization's systems, resulting in severe operational, financial, and reputational damage.

## Least Privilege | Log Use of Privileged Functions - Risk Score: 64

- Threat: non-privileged users may gain unauthorized access to privileged functions

- Vulnerability: Unauthorized access

- Risk Explanation: non-privileged users could execute privileged functions, leading to unauthorized system changes, data corruption, or security breaches. Without auditing, these actions may go undetected, increasing the potential for significant operational, financial, and reputational damage to the organization.

## Identification and Authentication (organizational Users) | Access to Accounts — Replay Resistant - Risk Score: 56

- Threat: replay attacks

- Vulnerability: Unauthorized access

- Risk Explanation: the organization is vulnerable to replay attacks, where attackers may intercept and reuse authentication credentials to gain unauthorized access to the network. This may lead to severe security incidents, including unauthorized access to sensitive data and systems. Implementing replay-resistant authentication mechanisms mitigates this risk by ensuring that intercepted authentication data may not be reused, thereby reducing the likelihood and impact of replay attacks on the organization's network.

## Media Use | Prohibit Use Without Owner - Risk Score: 56

- Threat: introducing malicious software, unauthorized access, or data breaches

- Vulnerability: Data modification/ destruction/ corruption

- Risk Explanation: unidentified portable storage devices could be used within the organization, leading to severe security incidents such as data breaches or malware infections. This control mitigates the risk by ensuring that only portable storage devices with an identifiable owner are allowed, thereby reducing the likelihood and impact of unauthorized or malicious use of such devices.

## Maintenance Tools | Prevent Unauthorized Removal - Risk Score: 56

- Threat: introducing malicious code into the organization's systems via diagnostic or test media.

- Vulnerability: Data modification/ destruction/ corruption

- Risk Explanation: malicious code could be introduced into the organization's systems via uninspected diagnostic or test media. This may result in severe security incidents, including system compromise and data breaches. Implementing this control mitigates the risk by ensuring that all media are thoroughly scanned for malicious code before being used, thereby protecting the organization's systems from potential malware and other security threats.

## Information in Shared System Resources - Risk Score: 56

- Threat: unauthorized access to sensitive information due to improper handling of shared resources.

- Vulnerability: Unauthorized access

- Risk Explanation: data could be inadvertently transferred between users or processes via shared system resources, leading to unauthorized access and data breaches. Implementing this control mitigates the risk by ensuring that shared resources are managed in such a way that only authorized processes may access the data intended for them, reducing both the likelihood and impact of potential security incidents.

## Least Functionality | Authorized Software — Allow-by-exception - Risk Score: 56

- Threat: unauthorized or malicious software being executed on organizational systems.

- Vulnerability: Data modification/ destruction/ corruption

- Risk Explanation: unauthorized or malicious software may be installed and executed on organizational systems. This could lead to significant security incidents, including malware infections and data breaches. By applying a deny-by-exception or a deny-all, permit-by-exception policy, the organization may prevent unauthorized software from running, thereby reducing the likelihood of security breaches and limiting the potential impact of any unauthorized software that might otherwise be introduced into the environment.

## Risk Assessment - Risk Score: 56

- Threat: unaddressed vulnerabilities and threats to organizational systems and CUI.

- Vulnerability: Incomplete documentation

- Risk Explanation: the organization may fail to identify and address critical vulnerabilities and threats, leading to significant security incidents. Regular risk assessments help the organization stay ahead of potential risks, enabling proactive management and mitigation. Implementing this control mitigates the risk by ensuring that the organization continually evaluates and responds to changes in the risk environment, thereby reducing the likelihood and impact of security breaches.

## Configuration Change Control - Risk Score: 56

- Threat: unauthorized, unapproved, or poorly managed changes to organizational systems

- Vulnerability: Unauthorized changes to systems

- Risk Explanation: the organization is exposed to significant security and operational risks due to unmanaged changes. Unauthorized, unapproved, or poorly documented changes may introduce vulnerabilities, destabilize systems, and lead to data breaches or compliance failures. Without a formal process to track and approve changes, it is difficult to maintain system integrity or respond effectively to incidents, leading to a high overall risk to the organization's operations and assets.

## System Security and Privacy Plans - Risk Score: 56

- Threat: risk of unclear or outdated security postures

- Vulnerability: Policy breach

- Risk Explanation: the organization may operate without a clear understanding of its security posture, system boundaries, and security control implementations. This may lead to significant security incidents and compliance issues. Implementing this control mitigates the risk by ensuring that security plans are thoroughly documented, regularly updated, and aligned with the organization's current operating environment, reducing both the likelihood and impact of security breaches.

## Protection of Audit Information - Risk Score: 56

- Threat: unauthorized access, tampering, or deletion of audit logs.

- Vulnerability: Data modification/ destruction/ corruption

- Risk Explanation: audit logs and tools may be vulnerable to unauthorized access, tampering, or deletion, that could allow attackers to hide their activities and prevent the organization from detecting or responding to security incidents. This may result in undetected breaches, incomplete investigations, and a significant loss of accountability. Implementing this control mitigates the risk by ensuring that audit information and tools are properly secured, maintaining the integrity and reliability of audit records for effective incident detection and response.

## System Monitoring | Inbound and Outbound Communications Traffic - Risk Score: 56

- Threat: undetected unauthorized access or misuse of organizational systems.

- Vulnerability: Unauthorized access

- Risk Explanation: unauthorized access or misuse of systems could go unnoticed, leading to serious security incidents. Implementing this control mitigates the risk by ensuring that unauthorized activities are detected and responded to quickly, reducing both the likelihood and impact of potential security breaches.

## Content of Audit Records - Risk Score: 56

- Threat: lack of user accountability, that may lead to difficulty in investigating and resolving security incidents

- Vulnerability: Data modification/ destruction/ corruption

- Risk Explanation: the organization may be unable to hold users accountable for their actions, leading to a lack of accountability and difficulty in investigating and resolving security incidents. This may result in unaddressed breaches, legal and regulatory issues, and a failure to enforce security policies. Implementing this control mitigates the risk by ensuring that all user actions are traceable, supporting accountability and effective incident response.

## Remote Access | Managed Access Control Points - Risk Score: 56

- Threat: unauthorized remote access to the organization's systems.

- Vulnerability: Unauthorized access

- Risk Explanation: remote access to the organization's systems could occur through unmonitored and unsecured entry points. Without routing remote access through managed control points, attackers are more likely to gain unauthorized access, leading to data breaches, unauthorized system changes, and potentially catastrophic system compromises. This may result in significant operational disruptions, financial losses, and reputational damage, as well as increased vulnerability to further attacks.

## Network Disconnect - Risk Score: 56

- Threat: unauthorized access through inactive or forgotten sessions

- Vulnerability: Unauthorized access

- Risk Explanation: sessions could remain active after the intended user has finished, allowing unauthorized access or misuse of the network connection. Implementing this control mitigates the risk by ensuring that all network connections are terminated when no longer needed, reducing both the likelihood and impact of unauthorized access.

## Device Lock - Risk Score: 56

- Threat: unauthorized access to and viewing of sensitive information during periods of user inactivity.

- Vulnerability: Unauthorized access

- Risk Explanation: sensitive information may be accessed and viewed by unauthorized individuals during periods of user inactivity. Without a session lock, an unattended device becomes vulnerable to anyone nearby, potentially leading to data breaches, unauthorized changes, and exposure of confidential information. This risk increases the chances of significant operational, financial, and reputational damage to the organization.

## Protection of Information at Rest - Risk Score: 56

- Threat: unauthorized access to or disclosure of CUI stored on organizational systems.

- Vulnerability: Unauthorized access

- Risk Explanation: CUI stored on organizational systems could be accessed or disclosed by unauthorized individuals, leading to severe security incidents. Implementing this control mitigates the risk by ensuring that appropriate security measures, such as encryption and access controls, are in place to protect the confidentiality of CUI at rest, reducing both the likelihood and impact of potential breaches.

## Control Assessments - Risk Score: 56

- Threat: undetected weaknesses or ineffective security controls.

- Vulnerability: Data Loss/Information Disclosure

- Risk Explanation: security controls may become ineffective over time, leading to undetected vulnerabilities and a false sense of security. This may result in significant security incidents, including data breaches and system compromises. Implementing this control mitigates the risk by ensuring that security controls are regularly assessed for their effectiveness, allowing the organization to address any weaknesses or gaps before they may be exploited, thereby reducing the likelihood and impact of security breaches.

## Visitor Access Records | Automated Records Maintenance and Review - Risk Score: 56

- Threat: unauthorized access going undetected

- Vulnerability: Incomplete documentation

- Risk Explanation: unauthorized physical access to the facility may go unnoticed or unresolved due to the lack of proper logging. This may lead to serious security incidents, including theft, tampering, or data breaches, with no ability to trace the activity back to a responsible party. Implementing this control mitigates the risk by ensuring that all physical access is logged and may be reviewed, supporting both real-time security monitoring and post-incident investigations.

## Impact Analyses - Risk Score: 56

- Threat: introducing security vulnerabilities or other issues during system changes

- Vulnerability: Unauthorized changes to systems

- Risk Explanation: changes to organizational systems could introduce security vulnerabilities or other issues that significantly weaken the security posture. Without analyzing the security impact before implementation, the organization is at high risk of creating new attack vectors or destabilizing the system. This may lead to severe consequences, including data breaches, operational disruptions, and non-compliance with regulatory requirements, resulting in a high overall risk to the organization.

## Access Restrictions for Change - Risk Score: 56

- Threat: unauthorized changes to systems

- Vulnerability: Unauthorized changes to systems

- Risk Explanation: unauthorized changes could be made to organizational systems, leading to vulnerabilities, system instability, or data breaches. Without proper access controls, it is difficult to ensure that only authorized individuals may make changes, that increases the likelihood and potential impact of harmful modifications. Implementing this control mitigates the risk by ensuring that all changes are tightly controlled and that only authorized personnel have the ability to make those changes, protecting the organization's systems and data.

## Access Restrictions for Change | Automated Access Enforcement and Audit Records - Risk Score: 56

- Threat: unauthorized changes to systems

- Vulnerability: Unauthorized changes to systems

- Risk Explanation: Without automated mechanisms to enforce access restrictions for changes, there is a high likelihood that unauthorized or unapproved changes could be made to critical systems. These unauthorized changes could introduce vulnerabilities, disrupt operations, and lead to serious security incidents. The organization could suffer from data breaches, loss of system integrity, and non-compliance with industry regulations or standards, resulting in substantial financial and reputational damage.

# Recommendations

To address the identified risks, the following actions are recommended:

- Immediate Actions:

- Implement additional controls for the identified high-risk areas within the next quarter.

- Conduct a thorough review of related controls to ensure compliance and effectiveness.

- Medium-Term Actions:

- Review and update the incident response plan to incorporate new threats.

- Enhance employee training on security procedures, focusing on identified weaknesses.

- Long-Term Actions:

- Conduct regular vulnerability assessments and risk evaluations to maintain a proactive security posture.

# Conclusion

This assessment underscores critical vulnerabilities that demand immediate attention to safeguard the organization's security. Proactively addressing these risks will enhance our security posture, fortify our defenses, and ensure the continued protection of our assets and sensitive data against emerging threats.