13 Access Controls

Friday, August 2, 2024 2:21 PM

1. Document Review

- **Objective:** Verify the existence of documented policies and procedures that support each access control statement in line with regulatory requirements.
- **Action Steps:**
  - **Collect Documentation:** Ensure relevant documentation, including Information Security Policies, Access Control Policies, and System Configuration Guides, is in place.
  - **Verify Compliance:** Ensure these documents explicitly cover the requirements of **12 CFR 748.0(b)** and **Appendix A to Part 748**, particularly regarding access controls that safeguard member information.
  - **Focus on Best Practices:** Look for references to industry best practices, such as password management, multi-factor authentication (MFA), account management, and access control.
- **Regulatory Reference:**
  - **12 CFR 748.0(b):** Requires federally insured credit unions to implement a written security program that ensures the security and confidentiality of member information.
  - **Appendix A to Part 748, Section III(A):** Requires the implementation of appropriate access controls to safeguard member information.

2. System Configuration Audit

- **Objective:** Confirm that system configurations align with documented policies and meet regulatory and industry best practices.
- **Action Steps:**
  - Use system administration tools (e.g., Active Directory, SSO providers) to check password policies, user account statuses, MFA settings, and access controls.
  - **Check Compliance with Access Control Policies:** Ensure password policies comply with industry best practices, enforcing unique, complex passwords in accordance with **Appendix A to Part 748, Section III(B)(1)(c)**.
  - **Account Inactivity Controls:** Verify that inactive user accounts are disabled in line with security procedures (Stmt 13.2), as required by **Appendix A to Part 748, Section III(B)(2)(b)**.
  - **MFA for High-Risk Users:** Confirm MFA is required for high-risk users and critical systems (Stmt 13.4), aligning with **Appendix A to Part 748, Section III(B)(1)(c)**.
- **Regulatory Reference:**
  - **Appendix A to Part 748, Section III(B):** Requires proper system configurations for access controls, including password and authentication management, to mitigate risks to member information.

3. Access Control Review

- **Objective:** Validate that user access is appropriately restricted and managed in compliance with access control policies.
- **Action Steps:**
  - Conduct periodic user access reviews to ensure that only authorized personnel have access to sensitive systems and member information, as required by **Appendix A to Part 748, Section III(B)(2)**.
  - **Inventory of Authentication Systems:** Review the inventory of authentication and authorization systems to ensure proper control (Stmt 13.5) in line with **Appendix A, Section III(B)(1)**.
  - **Centralized Access Control:** Ensure access control is centralized, where supported (Stmt 13.6), to meet the security program requirements outlined in **Appendix A to Part 748, Section III(A)**.
  - **Service Account Management:** Verify the accuracy of the inventory of service accounts (Stmt 13.9), as required for the protection of critical systems under **Appendix A to Part 748, Section III(B)(2)(a)**.
- **Regulatory Reference:**
  - **Appendix A to Part 748, Section III(B):** Mandates controls to ensure that access to systems and

information is limited to authorized personnel.

4. Physical and Environmental Controls Verification

- **Objective:** Confirm that physical access to sensitive areas is restricted and monitored in compliance with regulatory requirements.
- **Action Steps:**
  - **Physical Access Controls:** Inspect physical security controls (e.g., access cards, biometric scanners, and surveillance systems) in line with **Appendix A to Part 748, Section III(B)(1)(d)**, which mandates physical controls to safeguard member information.
  - **Environmental Safeguards:** Ensure environmental controls, such as fire suppression systems and climate control, are in place and functioning to meet the requirements of **12 CFR 748.0(b)**.
- **Regulatory Reference:**
  - **Appendix A to Part 748, Section III(B)(1)(d):** Requires the implementation of physical access controls to protect sensitive member information.

5. Remote Access Controls Verification

- **Objective:** Ensure remote access is properly managed and secured as per regulatory requirements.
- **Action Steps:**
  - **Remote Access Security:** Verify that remote access is secured using encryption and MFA (Stmt 13.17, 13.18), in line with **Appendix A to Part 748, Section III(B)(1)(c)**.
  - **MDM Solutions:** Confirm that mobile device management (MDM) solutions are in place for personal devices connecting to the network (Stmt 13.16), ensuring compliance with **Appendix A to Part 748, Section III(A)**.
  - **Monitor Remote Access Logs:** Review logs to ensure remote access activities are monitored, and anomalies are reported (Stmt 13.19), as required by **Appendix A to Part 748, Section III(B)(1)(c)**.
  - **Vendor Remote Access:** Ensure vendor remote access is disabled when not in use and sharing of remote user accounts is prohibited (Stmt 13.21, 13.22), as mandated by **Appendix A to Part 748, Section III(B)(2)**.
- **Regulatory Reference:**
  - **Appendix A to Part 748, Section III(B)(1)(c):** Requires strong controls and monitoring for remote access to protect member information.

6. Role-Based Access Control (RBAC) Review

- **Objective:** Ensure access rights are assigned based on roles, and roles are periodically reviewed and updated according to risk.
- **Action Steps:**
  - **Review RBAC Configurations:** Verify that RBAC settings reflect the current organizational structure and risk assessments (Stmt 13.13), ensuring compliance with **Appendix A to Part 748, Section III(B)(2)**.
  - **Periodic Access Review:** Ensure roles and access rights are reviewed and updated regularly to account for organizational and role changes.
- **Regulatory Reference:**
  - **Appendix A to Part 748, Section III(B)(2):** Requires access controls to be based on the sensitivity of information and periodically reviewed.

7. Compliance Verification

- **Objective:** Ensure consistent application of security procedures in alignment with regulatory requirements.
- **Action Steps:**
  - **Verify Compliance with Virtual Security Procedures:** Confirm that procedures for securing the virtual

environment are consistently followed (Stmt 13.10), as required by **Appendix A to Part 748, Section III(A)**.
    - **Network Access Controls:** Check that network access control software is properly configured and operational (Stmt 13.12) to comply with **Appendix A to Part 748, Section III(B)(1)(c)**.
    - **Access Management Upon Role Changes:** Review formal processes for granting and removing access upon hire, role changes, or terminations to ensure compliance with **Appendix A to Part 748, Section III(B)(2)(b)**.
- **Regulatory Reference:**
    - **Appendix A to Part 748, Section III(B)(2):** Mandates formal access management processes, including timely changes upon employee status changes.

8. Reporting and Documentation

- **Objective:** Provide a comprehensive report on the validation process, documenting compliance with 12 CFR 748.0 and Appendix A to Part 748.
- **Action Steps:**
    - **Compile Validation Report:** Summarize the compliance status for each statement and document any discrepancies or areas for improvement.
    - **Recommendations for Remediation:** Provide actionable recommendations to address any deficiencies identified during the validation process.
    - **Maintain Records:** Retain records of access control policies, procedures, and audit results as required by **Appendix A to Part 748, Section II** for ongoing compliance.
- **Regulatory Reference:**
    - **Appendix A to Part 748, Section II:** Requires that credit unions document their information security program and maintain appropriate records to demonstrate compliance.

AD Check

Friday, September 20, 2024 2:44 PM

Checking and auditing **Active Directory (AD) security settings** is crucial for ensuring the protection of sensitive data, preventing unauthorized access, and complying with regulatory requirements, such as **12 CFR 748.0** and **Appendix A to Part 748, Title 12**. Below is a detailed guide on how to review and validate key AD security settings using both graphical interfaces and PowerShell commands.

1. Review Group Policy Settings

Purpose: Ensure that AD security-related Group Policies are properly configured and enforced.

- **Steps:**
    1. Open the **Group Policy Management Console** (`gpmc.msc`).
    2. Navigate to the relevant **Group Policies** that affect AD, such as:
        - **Default Domain Policy**: Password policies, account lockout settings, Kerberos policies.
        - **Default Domain Controllers Policy**: Audit policies, security options, UAC settings.
    3. Review key security settings under:
        - **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings**.
        - Key areas to check:
            - **Account Policies** > **Password Policy**: Ensure strong passwords (minimum length, complexity, etc.).
            - **Account Lockout Policy**: Configure account lockout settings to prevent brute-force attacks.
            - **Kerberos Policy**: Set appropriate ticket lifetimes for Kerberos authentication.
            - **Local Policies** > **Audit Policy**: Ensure auditing is enabled for account logon events, privilege use, etc.

Key Group Policy Settings:

- **Enforce password history**: Ensure users cannot reuse old passwords.
- **Minimum password length**: Enforce at least 12 characters.
- **Account lockout threshold**: Lock accounts after a defined number of failed login attempts.

2. Review Active Directory User and Group Permissions

Purpose: Ensure that user and group permissions are correctly configured, following the principle of least privilege.

- **Steps:**
    1. Open **Active Directory Users and Computers** (`dsa.msc`).
    2. Navigate to **Users** or **Security Groups**.
    3. Right-click the object (user or group) > **Properties** > **Security** tab.
    4. Review the **Permissions** for sensitive groups, such as:
        - **Domain Admins**
        - **Enterprise Admins**

- **Schema Admins**
- **Administrators**

Key Areas to Review:

- Ensure that only trusted, authorized personnel are members of these groups.
- Verify that permissions are appropriate and that **delegated permissions** do not grant unnecessary privileges.

3. Audit Privileged Group Membership

Purpose: Ensure that only authorized personnel have access to privileged groups.

- **Steps:**
    1. Use **PowerShell** to list privileged group memberships:

```
# List Domain Admins
Get-ADGroupMember -Identity "Domain Admins" | Select-Object Name,
SamAccountName

# List Enterprise Admins
Get-ADGroupMember -Identity "Enterprise Admins" | Select-Object Name,
SamAccountName

# List Schema Admins
Get-ADGroupMember -Identity "Schema Admins" | Select-Object Name,
SamAccountName
```

    1. Review the output to ensure only authorized users are members.

Key Considerations:

- Remove any unauthorized users from **Domain Admins**, **Enterprise Admins**, and **Schema Admins** groups.
- Use **Privileged Access Management (PAM)** or **Privileged Identity Management (PIM)** to enforce just-in-time access to privileged roles.

4. Review AD Account Lockout Policies

Purpose: Prevent brute-force attacks by locking accounts after multiple failed login attempts.

- **Steps:**
    1. Open **Group Policy Management** (`gpmc.msc`).
    2. Navigate to:
        - **Default Domain Policy** > **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Account Policies** > **Account Lockout Policy**.
    3. Verify that **Account Lockout Threshold**, **Lockout Duration**, and **Lockout Counter** are configured appropriately.

Recommended Settings:

- **Account Lockout Threshold**: Set to 5 failed attempts.
- **Account Lockout Duration**: Set to 15 minutes.
- **Reset Account Lockout Counter**: Set to 15 minutes.

5. Review Password Policy Settings

Purpose: Enforce strong password policies to prevent weak passwords from being used in AD.

- **Steps:**
    1. Open **Group Policy Management** (`gpmc.msc`).
    2. Navigate to:
        - **Default Domain Policy** > **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Account Policies** > **Password Policy**.
    3. Verify that **password complexity** and **expiration** settings are configured.

Recommended Settings:

- **Enforce Password History**: At least 24 previous passwords.
- **Minimum Password Length**: At least 12 characters.
- **Password Complexity**: Must include uppercase, lowercase, numbers, and symbols.
- **Maximum Password Age**: 60–90 days for non-privileged users, 30–60 days for privileged accounts.

6. Enable Auditing of Critical AD Objects and Events

Purpose: Track changes to critical AD objects (users, groups, OUs, etc.) and monitor user login attempts.

- **Steps:**
    1. Open **Group Policy Management** (`gpmc.msc`).
    2. Navigate to:
        - **Default Domain Controllers Policy** > **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Advanced Audit Policy Configuration**.
    3. Enable auditing for key categories, such as:
        - **Logon/Logoff Events**: Track successful and failed login attempts.
        - **Account Management**: Track user creation, deletion, and modification.
        - **Privilege Use**: Monitor the use of elevated privileges.
        - **Directory Service Access**: Track changes to AD objects.

PowerShell Command to View AD Audit Settings:

```
# Check audit settings for a domain controller
AuditPol /get /category:*
```

7. Review AD FS (if applicable)

Purpose: Ensure that AD Federation Services (AD FS) is secured.

- **Steps:**
    1. Open **AD FS Management Console** (`adfsmgmt.msc`).
    2. Check:
        - **SSL/TLS configurations**.
        - **Token signing certificates**.
        - **Claims provider trusts**.
        - **Relying party trusts**.

3. Ensure proper auditing of **login attempts** and **token issuance** events in AD FS.

Key Areas to Review:

- Ensure that only trusted claims providers and relying parties are listed.
- Check for appropriate **certificates** to secure token signing.

8. Implement Fine-Grained Password Policies (FGPP)

Purpose: Apply different password policies to different users or groups, such as requiring stricter password rules for administrative accounts.

- **Steps:**
    1. Open **Active Directory Administrative Center** (`dsac.msc`).
    2. Navigate to **System** > **Password Settings Container**.
    3. Create a new **Password Settings Object** (PSO) with stricter requirements for high-privilege accounts.

Recommended Settings for Privileged Accounts:

- **Minimum Password Length**: 15 characters.
- **Password Complexity**: Enabled.
- **Password Expiration**: 30 days.

9. Review Kerberos Policies

Purpose: Secure Kerberos authentication by limiting ticket lifetime and enforcing encryption standards.

- **Steps:**
    1. Open **Group Policy Management** (`gpmc.msc`).
    2. Navigate to:
        - **Default Domain Policy** > **Computer Configuration** > **Policies** > **Windows Settings** > **Security Settings** > **Account Policies** > **Kerberos Policy**.
    3. Review and enforce policies for:
        - **Maximum Lifetime for User Ticket (TGT)**.
        - **Maximum Lifetime for Service Tickets**.

Recommended Settings:

- **Maximum lifetime for user ticket**: 10 hours.
- **Maximum lifetime for service ticket**: 600 minutes.

10. Enable Microsoft Defender for Identity (formerly Azure ATP)

Purpose: Use **Microsoft Defender for Identity** to detect abnormal behavior, such as lateral movement, privilege escalation, or brute-force attacks.

- **Steps:**
    1. Set up **Microsoft Defender for Identity** and integrate it with your on-premises AD.
    2. Monitor security events for any abnormal user behavior or security issues.

Conclusion

By following the steps outlined above, you can systematically audit and secure your Active Directory environment. Ensuring that **Group Policy**, **password policies**, **privileged access**, and **auditing** are properly configured will help protect sensitive data and maintain compliance with **12 CFR 748.0** and **Appendix A to Part 748, Title 12**. Regular audits and monitoring will also help you detect potential security issues before they lead to a breach.

Issues

Friday, September 20, 2024 12:36 PM

When conducting a **Validation Process for Access Control Statements** in line with **12 CFR 748.0** and **Appendix A to Part 748**, various **potential findings** can emerge. These findings may highlight strengths or weaknesses in the access control measures and security policies of the organization. Below is a breakdown of **potential findings** for each section of the validation process.

1. Document Review Findings

- **Positive Findings:**
    - Access control policies are comprehensive, up-to-date, and aligned with **12 CFR 748.0** and **Appendix A to Part 748**.
    - Policies cover password management, multi-factor authentication (MFA), account management, and access restrictions.
    - Documentation includes references to industry best practices (e.g., NIST, ISO).
- **Negative Findings:**
    - Incomplete or outdated policies that do not address all required areas (e.g., lack of MFA requirements).
    - Policies do not align with industry best practices for access controls.
    - Absence of formal documentation for certain access control processes, such as role-based access or service account management.
    - Documentation lacks specificity regarding regulatory compliance with **Appendix A to Part 748**.

2. System Configuration Audit Findings

- **Positive Findings:**
    - System configurations for password policies, MFA, and access controls align with documented policies and best practices.
    - Password policies enforce complexity, expiration, and uniqueness.
    - Inactive user accounts are automatically disabled after a specified period of inactivity.
    - MFA is properly configured and required for high-risk systems and users.
- **Negative Findings:**
    - Password policies do not meet regulatory or best practice standards (e.g., no enforcement of password complexity or expiration).
    - Systems are misconfigured or inconsistently configured across environments (e.g., some servers lack MFA enforcement).
    - Inactive accounts are not disabled or removed, leading to potential unauthorized access risks.
    - MFA is not enabled for critical systems or high-risk users, as required by **Appendix A to Part 748, Section III(B)(1)(c)**.

3. Access Control Review Findings

- **Positive Findings:**
    - Regular user access reviews are conducted, ensuring only authorized personnel have access to sensitive information.
    - The inventory of authentication and authorization systems is complete and accurate.
    - Centralized access control is applied across systems and environments.
    - Service accounts are documented and managed properly, with limited access privileges.
- **Negative Findings:**
    - User access reviews are either not conducted regularly or are incomplete, leading to potential over-privileged accounts.
    - The inventory of authentication systems is incomplete or not regularly maintained.
    - Access control is not centralized, leading to inconsistent enforcement of access policies.
    - Service accounts are over-privileged or undocumented, increasing security risks.
    - Administrator privileges are not limited to dedicated accounts, increasing exposure to misuse.

4. Physical and Environmental Controls Verification Findings

- **Positive Findings:**
    - Physical access to sensitive areas (e.g., data centers, server rooms) is controlled using access cards, biometric scanners, and surveillance systems.
    - Environmental controls (e.g., climate control, fire suppression systems) are in place and functioning as expected.
- **Negative Findings:**
    - Physical access controls are insufficient or inconsistently enforced (e.g., shared access cards, lack of monitoring).
    - Inadequate monitoring of physical access logs and systems, leading to untracked or unauthorized access.
    - Environmental controls, such as fire suppression or climate systems, are not properly maintained or tested, posing operational risks.

5. Remote Access Controls Verification Findings

- **Positive Findings:**
    - Remote access is secured with encryption and MFA, and all access is monitored and logged.
    - Mobile Device Management (MDM) solutions are deployed to manage personal devices accessing the network.
    - Vendor access is restricted and disabled when not in use, ensuring compliance with **Appendix A to Part 748, Section III(B)(2)**.
- **Negative Findings:**
    - Remote access is not adequately secured (e.g., no encryption or MFA), increasing the risk of unauthorized access.
    - Lack of MDM solutions for personal devices, which could introduce

unmanaged risks to the network.
    - Remote access logs are incomplete or not regularly reviewed, making it difficult to detect anomalies.
    - Vendor remote access remains enabled when not needed, or vendor accounts are shared, violating security protocols.

6. Role-Based Access Control (RBAC) Review Findings

- **Positive Findings:**
    - RBAC is well-implemented, with roles reflecting current organizational needs and risks.
    - Regular reviews of roles and access rights are conducted to ensure they align with business requirements.
- **Negative Findings:**
    - RBAC policies are not properly enforced, leading to users having inappropriate access levels based on outdated roles.
    - Lack of periodic reviews of access rights, leading to unnecessary or excessive access.
    - Failure to map roles accurately to security requirements, resulting in over-provisioned access for certain roles.

7. Compliance Verification Findings

- **Positive Findings:**
    - Procedures for securing the virtual environment and access controls are consistently followed.
    - Network access control systems are in place, configured correctly, and regularly monitored.
    - Access management processes (e.g., provisioning, de-provisioning) are functioning effectively, with timely updates when employees are hired, change roles, or leave the organization.
- **Negative Findings:**
    - Inconsistent adherence to access control procedures for the virtual environment, leading to potential gaps in security.
    - Network access control systems are misconfigured or not properly monitored, increasing the risk of unauthorized access.
    - Access provisioning and de-provisioning processes are delayed or not followed, leading to excessive or outdated access rights.

8. Reporting and Documentation Findings

- **Positive Findings:**
    - A comprehensive validation report has been compiled, summarizing compliance status and providing actionable insights.
    - Documentation for access control policies, procedures, and audit findings is thorough and up-to-date.
- **Negative Findings:**
    - The validation report lacks sufficient detail or documentation to provide meaningful insights into compliance status.

- Incomplete or outdated documentation of access control procedures, making it difficult to assess compliance.
- Failure to provide recommendations for remediation or improvement, leaving gaps in the security posture unaddressed.

Summary of Potential Findings

Positive findings will demonstrate compliance with **12 CFR 748.0** and **Appendix A to Part 748**, showing that the organization has effective access controls, monitoring, and security policies in place to protect member information.

Negative findings will highlight gaps in policy enforcement, configuration, monitoring, and access management, indicating areas where the organization falls short of the regulatory requirements. These findings could expose the organization to risks such as unauthorized access, data breaches, or regulatory penalties.

By identifying these potential findings, organizations can take corrective actions to close gaps, strengthen security controls, and ensure ongoing compliance with federal regulations.

Remediation

Friday, September 20, 2024 12:37 PM

To address potential gaps and ensure compliance with **12 CFR 748.0** and **Appendix A to Part 748**, **remediation steps** must focus on strengthening access controls, improving policy enforcement, enhancing monitoring, and addressing any deficiencies in security configurations. Below are detailed remediation steps for the **potential findings** outlined in the previous section:

1. Document Review Remediation

- **Issue:** Incomplete or outdated access control policies.
- **Remediation Steps:**
    1. **Update Policies:** Revise and update access control policies to include all key areas, such as password management, multi-factor authentication (MFA), and account management, as per **Appendix A to Part 748, Section III(A)**.
    2. **Align with Best Practices:** Ensure that policies reference industry best practices (e.g., NIST, ISO) and align with regulatory requirements.
    3. **Regular Policy Reviews:** Implement a policy review schedule to ensure that policies are regularly updated based on evolving threats and organizational changes.
    4. **Document Approvals:** Obtain formal approval from management or the board of directors for updated policies, demonstrating commitment to compliance with **12 CFR 748.0(b)**.

2. System Configuration Audit Remediation

- **Issue:** Misconfigured systems or insufficient enforcement of security settings (e.g., weak password policies or inactive account management).
- **Remediation Steps:**
    1. **Enforce Password Policies:** Reconfigure password policies to comply with industry standards, including password complexity, expiration periods, and uniqueness, as required by **Appendix A to Part 748, Section III(B)(1)(c)**.
    2. **Automate Account Management:** Set up automated account management to disable inactive accounts after a specified period, reducing the risk of unauthorized access.
    3. **Implement MFA for Critical Systems:** Enforce MFA for high-risk users and critical systems, ensuring compliance with **Appendix A to Part 748, Section III(B)(1)(c)**.
    4. **Regular Configuration Audits:** Schedule regular audits of system configurations to ensure that settings align with documented policies.

3. Access Control Review Remediation

- **Issue:** Incomplete or irregular user access reviews and management of service accounts.
- **Remediation Steps:**

1. **Conduct Access Reviews:** Implement regular user access reviews to ensure only authorized personnel have access to sensitive information, in accordance with **Appendix A to Part 748, Section III(B)(2)**.
2. **Centralize Access Control:** Where feasible, centralize access control management to improve the consistency of access policies across the organization.
3. **Manage Service Accounts:** Review and update the inventory of service accounts, limiting their privileges and ensuring they are actively monitored.
4. **Document the Process:** Maintain detailed records of access reviews and the steps taken to address access control issues, ensuring transparency and auditability.

4. Physical and Environmental Controls Verification Remediation

- **Issue:** Insufficient physical security controls or environmental safeguards.
- **Remediation Steps:**
    1. **Strengthen Physical Security:** Install or upgrade physical access controls (e.g., access cards, biometric scanners) to ensure only authorized personnel can access sensitive areas, complying with **Appendix A to Part 748, Section III(B)(1)(d)**.
    2. **Implement Surveillance:** Ensure that surveillance systems are operational and monitor access to critical areas such as data centers and server rooms.
    3. **Test Environmental Controls:** Test and maintain environmental controls (e.g., fire suppression, climate control) to reduce operational risks.
    4. **Document Procedures:** Update documentation for physical and environmental controls, including regular maintenance and testing schedules.

5. Remote Access Controls Verification Remediation

- **Issue:** Insecure remote access practices or lack of proper monitoring.
- **Remediation Steps:**
    1. **Enforce MFA for Remote Access:** Mandate the use of MFA for all remote access, especially for critical systems and high-risk users, in compliance with **Appendix A to Part 748, Section III(B)(1)(c)**.
    2. **Secure Remote Connections:** Ensure all remote access is encrypted using secure protocols (e.g., VPNs, TLS).
    3. **Implement MDM:** Deploy Mobile Device Management (MDM) solutions to control access from personal devices, ensuring compliance with **Appendix A to Part 748, Section III(A)**.
    4. **Monitor Remote Access Logs:** Set up regular monitoring of remote access logs, reviewing any anomalies or unauthorized attempts.
    5. **Control Vendor Access:** Implement strict controls to disable vendor remote access when not needed and prohibit the sharing of remote user accounts.

6. Role-Based Access Control (RBAC) Review Remediation

- **Issue:** Outdated or poorly managed role-based access controls.
- **Remediation Steps:**
    1. **Update Role Definitions:** Review and update RBAC definitions to reflect the current organizational structure and risk profile.
    2. **Limit Access Rights:** Ensure that access rights are based on the principle of least privilege, granting users only the access required for their roles.
    3. **Periodic Role Reviews:** Conduct periodic reviews of role assignments and access rights to ensure they are accurate and up-to-date, as per **Appendix A to Part 748, Section III(B)(2)**.
    4. **Document Access Changes:** Maintain detailed records of any changes made to roles and access rights, ensuring transparency and compliance with regulatory standards.

7. Compliance Verification Remediation

- **Issue:** Inconsistent application of access control and security procedures.
- **Remediation Steps:**
    1. **Enforce Security Procedures:** Ensure that virtual and physical security procedures are consistently followed across the organization, as required by **Appendix A to Part 748, Section III(B)**.
    2. **Configure Network Access Controls:** Implement and configure network access control systems to manage and restrict access to sensitive systems and data.
    3. **Implement Onboarding/Offboarding Processes:** Strengthen access management processes to ensure timely granting and removal of access during employee onboarding, role changes, or terminations.
    4. **Internal Audits:** Conduct regular internal audits to ensure security procedures are followed consistently across all environments.

8. Reporting and Documentation Remediation

- **Issue:** Incomplete or outdated reporting and documentation of access control measures.
- **Remediation Steps:**
    1. **Improve Documentation:** Ensure that all access control policies, procedures, and audit findings are thoroughly documented and up-to-date, as required by **Appendix A to Part 748, Section II**.
    2. **Enhance Reporting:** Implement processes to generate regular reports on the status of access controls, identifying any deficiencies or areas for improvement.
    3. **Track Remediation Efforts:** Maintain detailed records of remediation actions taken to address identified gaps, ensuring clear evidence of progress toward compliance.
    4. **Ensure Management Oversight:** Provide regular reports to management and the board, as required by **Appendix A to Part 748, Section II**, to demonstrate compliance efforts and track security program

effectiveness.

General Remediation Best Practices

- **Automation:** Automate key processes such as password enforcement, account management, and remote access monitoring to reduce human error and ensure compliance.
- **Training:** Provide regular training for employees on the importance of access controls, security best practices, and compliance with **12 CFR 748.0** and **Appendix A to Part 748**.
- **Continuous Monitoring:** Implement continuous monitoring solutions to detect and respond to any deviations from compliance in real time.
- **Regular Audits:** Schedule regular internal and external audits to ensure ongoing compliance with federal regulations and improve overall security posture.

Conclusion

By following these remediation steps, organizations can address the gaps identified in the validation process and ensure compliance with **12 CFR 748.0** and **Appendix A to Part 748**. These steps help strengthen access controls, improve security configurations, and ensure the protection of member information, minimizing the risk of unauthorized access or data breaches.

Compliance

Friday, September 20, 2024 12:43 PM

To achieve compliance with **12 CFR 748.0** and **Appendix A to Part 748** in the validation steps for access control, the process must ensure that the organization's access controls, system configurations, and documentation align with regulatory requirements for protecting sensitive member information. Below is a detailed guide to aligning each step with regulatory expectations:

1. Document Review

- **Objective:** Verify the existence of documented policies and procedures that support each statement in compliance with **12 CFR 748.0** and **Appendix A to Part 748**.
- **Actions for Compliance:**
    1. **Collect Documentation:** Ensure all relevant documents (Information Security Policies, Access Control Policies, and System Configuration Guides) are up to date.
    2. **Ensure Explicit Coverage:** Each document should explicitly outline requirements for:
        - Password management
        - Multi-factor authentication (MFA)
        - Account management
        - Access control
    3. **Incorporate Best Practices:** Ensure the policies reference industry best practices such as NIST SP 800-53 or ISO 27001, in line with **Appendix A to Part 748, Section III(A)** which mandates written policies for protecting member information.
    4. **Ensure Management Approval:** Policies must be approved by the board or senior management, in line with **12 CFR 748.0(b)**.
- **Regulatory Reference:**
    - **12 CFR 748.0(b):** Requires a written security program to protect member information.
    - **Appendix A to Part 748, Section III(A):** Ensures that access controls are part of the written information security program.

2. System Configuration Audit

- **Objective:** Confirm that system configurations align with documented policies and industry best practices.
- **Actions for Compliance:**
    1. **Review System Settings:** Use tools like Active Directory or single sign-on (SSO) providers to audit:
        - Password policies to ensure compliance with **Appendix A to Part 748, Section III(B)(1)(c)**.
        - MFA settings for high-risk users and systems, as required by **Appendix A to Part 748, Section III(B)(1)(c)**.
        - Account statuses to ensure inactive accounts are disabled in

line with **Appendix A to Part 748, Section III(B)(2)**.

2. **Test Policies in Practice:** Confirm that password policies enforce unique, complex passwords and that MFA is required for critical systems.
3. **Disable Inactive Accounts:** Ensure that user accounts are automatically disabled after inactivity (e.g., 30 days) to prevent unauthorized access.

- **Regulatory Reference:**
  - **Appendix A to Part 748, Section III(B)(1)(c):** Requires strong password and authentication controls.
  - **Appendix A to Part 748, Section III(B)(2):** Inactive accounts must be handled in a timely manner to prevent unauthorized access.

3. Access Control Review

- **Objective:** Validate that user access is appropriately restricted and managed.
- **Actions for Compliance:**
  1. **Conduct Regular Access Reviews:** Implement regular user access reviews to confirm that only authorized personnel can access sensitive information (Stmt 13.3), as required by **Appendix A to Part 748, Section III(B)(2)**.
  2. **Centralize Access Control:** Review whether access control is centralized where supported (Stmt 13.6), ensuring consistency in how access is granted and revoked.
  3. **Restrict Admin Privileges:** Ensure that administrative privileges are limited to dedicated accounts (Stmt 13.7) in line with **Appendix A to Part 748, Section III(B)(2)**.
  4. **Verify Service Account Management:** Confirm that service accounts are accurately inventoried and managed (Stmt 13.9).
- **Regulatory Reference:**
  - **Appendix A to Part 748, Section III(B)(2):** Requires user access to be restricted to authorized personnel only.

4. Physical and Environmental Controls Verification

- **Objective:** Confirm that physical access to sensitive areas is controlled and monitored in compliance with regulatory requirements.
- **Actions for Compliance:**
  1. **Implement Physical Security Controls:** Inspect physical access controls (e.g., access cards, biometric scanners, surveillance systems) to ensure compliance with **Appendix A to Part 748, Section III(B)(1)(d)**.
  2. **Test Environmental Controls:** Ensure that environmental controls such as climate control and fire suppression systems are in place and functioning, as required by **Appendix A to Part 748** to safeguard member information from physical threats.
- **Regulatory Reference:**
  - **Appendix A to Part 748, Section III(B)(1)(d):** Requires physical access controls to protect member information from unauthorized access.

5. Remote Access Controls Verification

- **Objective:** Ensure that remote access is properly managed and secured, meeting regulatory requirements.
- **Actions for Compliance:**
    1. **Implement Encryption and MFA:** Verify that remote access is secured with encryption (e.g., VPNs) and that MFA is required, as mandated by **Appendix A to Part 748, Section III(B)(1)(c)**.
    2. **Use Mobile Device Management (MDM):** Ensure MDM solutions are in place for personal devices connecting to the network (Stmt 13.16) in line with **Appendix A to Part 748, Section III(A)**.
    3. **Monitor Remote Access Logs:** Review logs to ensure that remote access activities are monitored, anomalies are reported, and remote access is only granted to authorized personnel (Stmt 13.19, Stmt 13.20).
    4. **Control Vendor Access:** Ensure vendors' remote access is disabled when not in use and that sharing of remote user accounts is prohibited (Stmt 13.21, 13.22), in compliance with **Appendix A to Part 748, Section III(B)(2)**.
- **Regulatory Reference:**
    - **Appendix A to Part 748, Section III(B)(1)(c):** Requires encryption and MFA for remote access.
    - **Appendix A to Part 748, Section III(B)(2):** Limits access to authorized users, including vendors.

6. Role-Based Access Control (RBAC) Review

- **Objective:** Validate that access rights are assigned based on roles, and roles are periodically reviewed and updated based on risk.
- **Actions for Compliance:**
    1. **Review and Update RBAC Settings:** Ensure RBAC configurations are accurate and reflect the current organizational structure (Stmt 13.13), in compliance with **Appendix A to Part 748, Section III(B)(2)**.
    2. **Conduct Periodic Role Reviews:** Regularly review and update access rights based on organizational changes or changes in risk profiles.
- **Regulatory Reference:**
    - **Appendix A to Part 748, Section III(B)(2):** Requires periodic review and update of access controls based on risk.

7. Compliance Verification

- **Objective:** Ensure that the organization consistently follows access control procedures.
- **Actions for Compliance:**
    1. **Enforce Virtual Security Procedures:** Verify that procedures for securing the virtual environment (Stmt 13.10) are consistently followed and documented, as required by **Appendix A to Part 748, Section III(A)**.
    2. **Ensure Network Access Control:** Confirm that network access control software is in use and properly configured (Stmt 13.12), ensuring

compliance with **Appendix A to Part 748, Section III(B)(1)(c)**.

3. **Manage Access Provisioning:** Review formal processes for granting and removing access upon hire, role changes, or terminations to ensure they are functioning as intended (Stmt 13.11), in line with **Appendix A to Part 748, Section III(B)(2)**.

- **Regulatory Reference:**
  - **Appendix A to Part 748, Section III(A):** Requires written policies and consistent adherence to procedures.
  - **Appendix A to Part 748, Section III(B)(1)(c):** Requires the use of access controls to protect member information.

8. Reporting and Documentation

- **Objective:** Document the findings and provide a comprehensive report on the validation process.
- **Actions for Compliance:**
  1. **Compile Validation Report:** Summarize the compliance status for each statement and document discrepancies or areas needing improvement.
  2. **Track Remediation:** Provide recommendations for remediation and track progress on addressing any deficiencies identified during the validation process.
  3. **Maintain Records:** Ensure all findings, policies, and audit results are well-documented and retained for future audits, as required by **Appendix A to Part 748, Section II**.
- **Regulatory Reference:**
  - **Appendix A to Part 748, Section II:** Requires documentation of the information security program and access control measures to ensure compliance.

Conclusion

Achieving compliance with **12 CFR 748.0** and **Appendix A to Part 748** requires aligning all validation steps with the regulatory requirements. This includes ensuring up-to-date documentation, proper system configurations, centralized access control, periodic reviews, and robust reporting processes. By following these steps, the organization will meet federal requirements for protecting member information and maintaining a secure environment.

Tools

Monday, August 12, 2024 3:33 PM

1. Password Policies and Management

1. Built-in Operating System Tools

1.1. Active Directory (AD) Tools

- **Active Directory Users and Computers (ADUC)**: Use ADUC to check user account properties and password policies.
- **Group Policy Management Console (GPMC)**: Review and manage password policies applied via Group Policy.
- **PowerShell Cmdlets**: Use cmdlets like `Get-ADDefaultDomainPasswordPolicy` to retrieve and review password policies.

1.2. Local Security Policy (Windows)

- **Local Security Policy Editor (`secpol.msc`)**: Review local password policies on individual machines.

1.3. Command Line Utilities

- **Net Accounts**: Check password policies via command-line on local machines (e.g., `net accounts`).

2. Password Management Solutions

2.1. Enterprise Password Management Systems

- **LastPass Enterprise**: Provides centralized management of passwords and policy enforcement.
- **1Password Business**: Manages password policies and provides security auditing features.
- **Dashlane Business**: Offers password management with policy compliance features.

2.2. Password Auditing Tools

- **KeePass**: An open-source password manager with features for auditing stored passwords.
- **RoboForm Enterprise**: Provides password management with compliance and auditing tools.

3. Security Information and Event Management (SIEM) Tools

3.1. SIEM Solutions

- **Splunk**: Can be configured to monitor and alert on password policy violations and changes.
- **IBM QRadar**: Monitors password-related events and compliance with security policies.
- **ArcSight**: Offers features for detecting and analyzing password policy breaches.

4. Vulnerability Assessment Tools

4.1. Vulnerability Scanners

- **Nessus**: Scans for weak passwords and policy misconfigurations.
- **OpenVAS**: Open-source scanner that can identify password policy weaknesses.
- **Qualys**: Provides insights into password policy adherence and vulnerabilities.

5. Compliance and Audit Tools

5.1. Compliance Checkers

- **NIST Password Checker**: Checks password policies against NIST standards.
- **CIS-CAT**: CIS Configuration Assessment Tool helps verify password policy compliance with CIS benchmarks.

5.2. Auditing Tools

- **Netwrix Auditor**: Provides auditing and reporting on password policies and changes.
- **Lepide Active Directory Auditor**: Monitors and reports on password-related activities in AD.

6. Password Policy Analysis Tools

6.1. Password Complexity Analyzers

- **Have I Been Pwned? Passwords**: Checks if passwords have been exposed in known breaches.
- **Password Checker Online**: Analyzes password strength against common criteria.

6.2. Password Policy Testers

- **Microsoft Baseline Security Analyzer (MBSA)**: Checks for compliance with security best practices, including password policies.
- **Windows Password Recovery Tools**: Can test and recover passwords to validate policy strength (e.g., John the Ripper, Hashcat).

7. System Configuration Management Tools

7.1. Configuration Management Tools

- **Chef**: Automates the enforcement of password policies across systems.
- **Puppet**: Manages and enforces password policies as part of system configuration.
- **Ansible**: Can be used to enforce and validate password policies across multiple systems.

8. Penetration Testing Tools

8.1. Pen Testing Tools

- **Metasploit**: Can be used to test for password policy weaknesses through exploitation.
- **Burp Suite**: Useful for testing web application password policies.

9. Custom Scripts and Tools

9.1. Custom Scripts

- **PowerShell**: Scripts to review and enforce password policies (e.g., checking password expiration, complexity).
- **Bash Scripts**: For Unix-based systems to check password policy compliance.

10. Web-based Tools

10.1. Online Password Policy Checkers

- **Online Password Strength Checkers**: Various online tools to test the strength and complexity of passwords.

11. Reporting and Analytics Tools

11.1. Reporting Solutions

- **Microsoft Power BI**: Can be used to create dashboards and reports on password policy compliance.
- **Tableau**: Provides visualization and reporting capabilities for password management data.

12. Directory Services Management Tools

12.1. Directory Management

- **LDAP Admin**: Manages and audits LDAP directory services, including password policies.
- **Apache Directory Studio**: Offers tools to manage and audit LDAP directory services.

2. User Account Management

1. Built-in Operating System Tools

1.1. Active Directory (AD) Tools

- **Active Directory Users and Computers (ADUC)**: Manage and review user accounts and attributes in Active Directory.
- **Group Policy Management Console (GPMC)**: Manage and review Group Policies related to user account management.
- **Active Directory Administrative Center (ADAC)**: Provides a modern interface for managing AD users and groups.
- **PowerShell Cmdlets**: Use cmdlets like `Get-ADUser`, `Set-ADUser`, `Remove-ADUser` to manage and validate user accounts.

1.2. Local User Management (Windows)

- **Local Users and Groups (`lusrmgr.msc`)**: Manage user accounts and groups on local machines.
- **Command Line Utilities**: Use commands like `net user` and `net localgroup` to manage local accounts.

1.3. User Account Control (UAC)

- **UAC Settings**: Verify and manage User Account Control settings for account privilege escalation.

2. User Account Management Solutions

2.1. Identity and Access Management (IAM) Systems

- **Microsoft Azure Active Directory (AAD)**: Manage user accounts and permissions in the cloud.
- **Okta**: Provides user lifecycle management and single sign-on (SSO) capabilities.
- **OneLogin**: Offers user provisioning, SSO, and multi-factor authentication (MFA).

2.2. Directory Services

- **LDAP (Lightweight Directory Access Protocol)**: Manage and validate user accounts using LDAP-compliant directories (e.g., Apache Directory Studio).
- **Novell eDirectory**: Provides user and group management features.

3. Security Information and Event Management (SIEM) Tools

3.1. SIEM Solutions

- **Splunk**: Monitor and analyze user account activities and changes.
- **IBM QRadar**: Provides visibility into user account management and security events.
- **ArcSight**: Offers user account monitoring and reporting features.

4. Compliance and Audit Tools

4.1. Compliance Checkers

- **NIST Cybersecurity Framework (CSF)**: Use tools to verify compliance with NIST guidelines for user account management.
- **CIS-CAT**: CIS Configuration Assessment Tool for checking user account policies against CIS benchmarks.

4.2. Auditing Tools

- **Netwrix Auditor**: Provides auditing and reporting for user account changes and permissions.
- **Lepide Active Directory Auditor**: Monitors and reports on changes in Active Directory user accounts.

5. User Account Management and Reporting Tools

5.1. Reporting Tools

- **Microsoft Power BI**: Create dashboards and reports on user account management.
- **Tableau**: Provides visualization and reporting for user account data.

5.2. Custom Reporting Tools

- **PowerShell Scripts**: Generate custom reports for user account management and compliance.

6. Identity Verification and Management Tools

6.1. Identity Verification

- **Onfido**: Provides identity verification services for new user accounts.
- **Jumio**: Offers identity verification and authentication services.

6.2. User Lifecycle Management

- **SailPoint**: Provides identity governance and user lifecycle management solutions.

7. Vulnerability Assessment Tools

7.1. Vulnerability Scanners

- **Nessus**: Scans for vulnerabilities related to user account management and permissions.
- **OpenVAS**: Open-source scanner for identifying user account vulnerabilities.
- **Qualys**: Offers assessments for user account and permission vulnerabilities.

8. Configuration Management Tools

8.1. Configuration Management

- **Chef**: Automates user account management tasks.
- **Puppet**: Manages and enforces user account configurations.
- **Ansible**: Automates user account management and validation across systems.

9. Penetration Testing Tools

9.1. Pen Testing Tools

- **Metasploit**: Can be used to test for vulnerabilities in user account management processes.
- **Burp Suite**: Useful for testing web application user account management security.

10. Backup and Recovery Tools

10.1. Backup Solutions

- **Veeam Backup**: Provides backup and recovery solutions for user account data.
- **Acronis**: Offers backup and recovery services for user account information.

11. Web-based Tools

11.1. Online User Management Tools

- **Google Workspace Admin Console**: Manage and validate user accounts in Google Workspace.
- **Microsoft 365 Admin Center**: Manage and validate user accounts in Microsoft 365.

12. User Behavior Analytics (UBA) Tools

12.1. UBA Solutions

- **Sumo Logic**: Provides user behavior analytics and monitoring.
- **Exabeam**: Offers user and entity behavior analytics (UEBA) for detecting anomalies.

13. Third-Party Integration Tools

13.1. Integration Solutions

- **Zapier**: Automate user account management tasks across different applications.
- **IFTTT**: Connect and automate user account management processes with various services.

3. Access Reviews

1. Identity and Access Management (IAM) Systems

1.1. Microsoft Azure Active Directory (AAD)

- **Azure AD Access Reviews**: Built-in feature for reviewing and managing user access to applications and resources.

1.2. Okta

- **Okta Lifecycle Management**: Provides access reviews and certifications for user accounts and applications.

1.3. OneLogin

- **OneLogin Access Review**: Enables automated access reviews and compliance reporting.

1.4. SailPoint

- **IdentityNow**: Offers identity governance and access review features, including automated reviews and certifications.

1.5. IBM Security Identity Governance and Intelligence (IGI)

- **IBM IGI**: Provides comprehensive access review and certification capabilities.

2. Security Information and Event Management (SIEM) Tools

2.1. Splunk

- **Splunk User Behavior Analytics**: Provides insights into access patterns and helps in reviewing user permissions.

2.2. IBM QRadar

- **QRadar SIEM**: Offers reporting and analytics for access reviews and compliance.

2.3. ArcSight

- **ArcSight Logger**: Enables monitoring and reporting on access and permissions.

3. Compliance and Audit Tools

3.1. Netwrix Auditor

- **Netwrix Auditor for Active Directory**: Provides detailed reporting and auditing for access reviews and permissions.

3.2. Lepide Active Directory Auditor

- **Lepide Auditor**: Tracks changes and provides reports on user permissions and access.

3.3. Qualys

- **Qualys Compliance Suite**: Includes access review and compliance reporting tools.

3.4. Rapid7

- **InsightVM**: Provides vulnerability management and access review capabilities.

4. Access Management and Reporting Tools

4.1. Microsoft Power BI

- **Power BI for Access Reviews**: Create custom reports and dashboards to visualize access review data.

4.2. Tableau

- **Tableau for Access Management**: Provides advanced data visualization for access reviews.

4.3. Report Builder (SQL Server Reporting Services - SSRS)

- **SSRS**: Design and generate custom reports for access review and management.

5. Directory Services and Management Tools

5.1. Active Directory Users and Computers (ADUC)

- **ADUC**: Manage and review user permissions and group memberships in Active Directory.

5.2. Group Policy Management Console (GPMC)

- **GPMC**: Review and manage Group Policies that impact user access.

5.3. PowerShell

- **PowerShell Cmdlets**: Use cmdlets like `Get-ADUser`, `Get-ADGroup`, and `Get-ADACL` for querying and reviewing user access.

6. User Behavior Analytics (UBA) Tools

6.1. Exabeam

- **Exabeam Advanced Analytics**: Provides user behavior analytics to identify unusual access patterns.

6.2. Sumo Logic

- **Sumo Logic Security Analytics**: Monitors and analyzes user access behavior.

7. Compliance and Governance Frameworks

7.1. NIST Cybersecurity Framework (CSF)

- **NIST CSF Tools**: Tools and frameworks for ensuring access reviews align with NIST guidelines.

7.2. Center for Internet Security (CIS) Benchmarks

- **CIS-CAT**: Configuration Assessment Tool for validating access control and permissions against CIS benchmarks.

7.3. SOC 2 Compliance Tools

- **SOC 2 Compliance Software**: Helps in validating access review processes and compliance.

8. Configuration Management Tools

8.1. Chef

- **Chef Automate**: Automates and manages user access reviews and configurations.

8.2. Puppet

- **Puppet Enterprise**: Manages and enforces user permissions and configurations.

8.3. Ansible

- **Ansible Automation Platform**: Automates user access reviews and compliance checks.

9. Backup and Recovery Tools

9.1. Veeam Backup & Replication

- **Veeam Backup**: Provides backup and recovery for user account data and permissions.

9.2. Acronis

- **Acronis Backup**: Offers backup and recovery solutions for user data and permissions.

10. Penetration Testing Tools

10.1. Metasploit

- **Metasploit Framework**: Can be used to test and review user permissions and access controls.

10.2. Burp Suite

- **Burp Suite Professional**: Tests web application access controls and permissions.

11. Web-based Tools

11.1. Google Workspace Admin Console

- **Google Workspace Admin Console**: Manage and review user access in Google Workspace.

11.2. Microsoft 365 Admin Center

- **Microsoft 365 Admin Center**: Review and manage user permissions in Microsoft 365.

12. Third-Party Integration Tools

12.1. Zapier

- **Zapier for Access Reviews**: Automate workflows related to access reviews and notifications.

12.2. IFTTT

- **IFTTT for Access Management**: Connect and automate access review processes with various services.

4. Authentication and Authorization Inventory

1. Identity and Access Management (IAM) Systems

1.1. Microsoft Azure Active Directory (Azure AD)

- **Azure AD Portal**: Provides visibility and management for user identities, authentication methods, and authorization settings.

1.2. Okta

- **Okta Identity Cloud**: Manages authentication, authorization, and provides a comprehensive view of identity management across applications.

1.3. OneLogin

- **OneLogin Identity and Access Management**: Offers tools for managing authentication methods, user access, and providing an inventory of identity systems.

1.4. SailPoint

- **IdentityNow**: Provides identity governance, including inventory and management of authentication and authorization systems.

1.5. IBM Security Identity Governance and Intelligence (IGI)

- **IBM IGI**: Offers comprehensive management and visibility of identity and access controls.

2. Security Information and Event Management (SIEM) Tools

2.1. Splunk

- **Splunk Enterprise Security**: Provides visibility into authentication and authorization events across the enterprise.

2.2. IBM QRadar

- **QRadar SIEM**: Offers insights and reporting on authentication and authorization activities.

2.3. ArcSight

- **ArcSight ESM**: Provides comprehensive security monitoring, including authentication and authorization data.

3. Compliance and Audit Tools

3.1. Netwrix Auditor

- **Netwrix Auditor for Active Directory**: Provides detailed auditing and reporting for authentication and authorization events.

3.2. Lepide Active Directory Auditor

- **Lepide Auditor**: Tracks and reports on authentication and authorization changes and inventory.

3.3. Qualys

- **Qualys Compliance Suite**: Includes tools for auditing and validating authentication and authorization configurations.

3.4. Rapid7

- **InsightVM**: Provides vulnerability management and insights into authentication and authorization configurations.

4. Access Management and Reporting Tools

4.1. Microsoft Power BI

- **Power BI**: Create custom reports and dashboards to visualize authentication and authorization data.

4.2. Tableau

- **Tableau**: Advanced data visualization for tracking authentication and authorization inventory.

4.3. Report Builder (SQL Server Reporting Services - SSRS)

- **SSRS**: Design and generate custom reports related to authentication and authorization.

5. Directory Services and Management Tools

5.1. Active Directory Users and Computers (ADUC)

- **ADUC**: Manage and review user accounts and their authentication methods within Active Directory.

5.2. Group Policy Management Console (GPMC)

- **GPMC**: Review and manage policies related to authentication and authorization.

5.3. PowerShell

- **PowerShell Cmdlets**: Use cmdlets like `Get-ADUser`, `Get-ADGroup`, and `Get-ADComputer` for querying and managing authentication and authorization data.

6. User Behavior Analytics (UBA) Tools

6.1. Exabeam

- **Exabeam Advanced Analytics**: Provides user behavior analytics to monitor authentication and authorization activities.

6.2. Sumo Logic

- **Sumo Logic Security Analytics**: Monitors and analyzes authentication and authorization events.

7. Configuration Management Tools

7.1. Chef

- **Chef Automate**: Manages and validates configurations related to authentication and authorization.

7.2. Puppet

- **Puppet Enterprise**: Automates and enforces configurations related to authentication and authorization.

7.3. Ansible

- **Ansible Automation Platform**: Automates validation of authentication and authorization settings.

8. Backup and Recovery Tools

8.1. Veeam Backup & Replication

- **Veeam Backup**: Provides backup and recovery for authentication and authorization data.

8.2. Acronis

- **Acronis Backup**: Offers backup solutions for user authentication and authorization data.

9. Penetration Testing Tools

9.1. Metasploit

- **Metasploit Framework**: Tests and reviews authentication and authorization controls.

9.2. Burp Suite

- **Burp Suite Professional**: Tests web applications for vulnerabilities in authentication and authorization mechanisms.

10. Web-based Tools

10.1. Google Workspace Admin Console

- **Google Workspace Admin Console**: Manages and reviews authentication and authorization settings for Google Workspace.

10.2. Microsoft 365 Admin Center

- **Microsoft 365 Admin Center**: Provides tools for managing and reviewing authentication and authorization settings in Microsoft 365.

11. Third-Party Integration Tools

11.1. Zapier

- **Zapier for Access Management**: Automate workflows related to authentication and authorization inventory management.

11.2. IFTTT

- **IFTTT for Authentication Management**: Connect and automate authentication and authorization processes.

12. Cloud Security Tools

12.1. AWS Identity and Access Management (IAM)

- **AWS IAM**: Manage and review authentication and authorization in AWS environments.

12.2. Google Cloud IAM

- **Google Cloud IAM**: Provides tools for managing authentication and authorization in Google Cloud.

12.3. Azure IAM

- **Azure IAM**: Tools for managing and reviewing authentication and authorization in Azure environments.

UAC

Friday, September 20, 2024 2:41 PM

User Account Control (UAC) is a security feature in Windows that helps prevent unauthorized changes to the operating system. UAC prompts users for permission or administrative credentials before allowing actions that could affect system settings or security. Here's how to configure UAC to enhance security:

Steps for UAC Configuration

1. **Open the UAC Settings Window:**
    - Press `Win + R` to open the **Run** dialog.
    - Type `Control Panel` and press **Enter**.
    - In the **Control Panel**, navigate to:
        - **User Accounts** > **Change User Account Control settings**.
2. **Adjust UAC Notification Level:** In the **User Account Control Settings** window, you will see a slider with four levels of security for UAC:
    - **Always Notify (Most Secure)**:
        - This option is the most secure. You will be notified when:
            - Apps try to install software or make changes to your computer.
            - You make changes to Windows settings.
        - This is recommended for sensitive environments where tight control is required over administrative actions.
    - **Notify Me Only When Apps Try to Make Changes to My Computer** (default):
        - You will be notified when apps try to make changes, but not when you change Windows settings.
        - The desktop will be dimmed during the prompt for better security. This option is good for balancing security and usability.
    - **Notify Me Only When Apps Try to Make Changes to My Computer (Don't Dim My Desktop)**:
        - Similar to the previous option, but the desktop is not dimmed, making the prompt less secure.
        - Recommended only in environments where the dimming feature causes compatibility issues.
    - **Never Notify (Least Secure)**:
        - This disables UAC entirely, and you will not be notified when changes are made to the system.
        - Not recommended, as it exposes the system to unauthorized changes.
3. **Select the Appropriate Level:**
    - Move the slider to your desired notification level (for most security, choose **Always Notify**).
    - Click **OK**.
4. **Confirm the Changes:**
    - You will be prompted to confirm the UAC settings change. If you selected **Always Notify**, UAC will ask you for administrator approval.
    - Click **Yes** to confirm.

Advanced UAC Configuration via Group Policy

For enterprise environments or domain-joined machines, you can configure UAC more granularly using **Group Policy**.

1. **Open Group Policy Editor:**
    - Press `Win + R`, type `gpedit.msc`, and press **Enter**.
2. **Navigate to UAC Settings:**
    - **Computer Configuration** > **Windows Settings** > **Security Settings** > **Local Policies** > **Security Options**.
3. **Configure UAC Policies:** You will see several UAC-related policies that can be configured for enhanced control:
    - **User Account Control: Admin Approval Mode for the Built-in Administrator account**:
        - Enable this to force the built-in Administrator account to operate with UAC prompts.
    - **User Account Control: Behavior of the elevation prompt for administrators in Admin Approval Mode**:
        - Set to **Prompt for credentials** or **Prompt for consent**, depending on whether you want administrators to provide a password or just approve the action.
    - **User Account Control: Detect application installations and prompt for elevation**:
        - Enable this to prompt when an application installer is detected, preventing unauthorized installations.
    - **User Account Control: Only elevate UIAccess applications that are installed in secure locations**:
        - Enable this to only allow applications from trusted directories (such as `Program Files` or `Windows`) to prompt for elevation.
    - **User Account Control: Run all administrators in Admin Approval Mode**:
        - Enable this to ensure that all administrators are subject to UAC and must approve elevated actions.
    - **User Account Control: Virtualize file and registry write failures to per-user locations**:
        - Enable this to allow legacy applications that require administrator privileges to run without administrative rights by virtualizing the file and registry writes.
4. **Apply the Policy Changes:**
    - Once you've configured the desired UAC policies, click **OK**.
    - Close the Group Policy Editor.
    - Run `gpupdate /force` in **Command Prompt** to apply the changes immediately.

Verifying UAC Configuration

- After configuring UAC, test the changes by trying to perform administrative tasks (e.g., installing an application or changing system settings).
- Check if UAC prompts appear according to your configuration.

Additional Best Practices for UAC Configuration:

- **Keep UAC Enabled**: Disabling UAC entirely increases the risk of unauthorized changes and malware infections.

- **Enforce UAC in Admin Approval Mode**: This ensures that even administrators need to confirm their actions, reducing the risk of unintended changes or malware execution.
- **Enable UAC on Remote Systems**: If managing multiple machines remotely, ensure UAC is configured to prompt for confirmation even during remote administrative tasks.

By following these steps, UAC can help protect your system from unauthorized changes and ensure compliance with security requirements.

Network File Shares

Wednesday, September 18, 2024 2:20 PM

Achieving compliance with **12 CFR 748.0** and **Appendix A to Part 748** in managing **Network File Shares** requires a structured approach to secure sensitive member information. Below are steps and recommendations to align your network file share practices with regulatory requirements.

1. Conduct a Full Access Review

- **Objective:** Ensure that only authorized users can access sensitive data on network file shares.
- **Actions for Compliance:**
    1. **Audit File Shares:** Review all file shares to identify permissions that allow unrestricted access (e.g., "Everyone" or "Domain Users" with full control). Remove or limit such permissions as required by **Appendix A to Part 748, Section III(B)(1)**.
    2. **Classify Data:** Categorize data stored on file shares by sensitivity (e.g., confidential, restricted, public), prioritizing sensitive information like credentials, financial data, and personal information, as per **Appendix A to Part 748, Section III(A)**.
- **Regulatory Reference:**
    - **Appendix A to Part 748, Section III(A):** Requires the categorization of information based on its sensitivity and corresponding security measures.

2. Implement the Principle of Least Privilege

- **Objective:** Minimize access to sensitive information by restricting permissions to only those users who require it.
- **Actions for Compliance:**
    1. **Limit Access:** Remove broad access permissions such as "Everyone" or "Domain Users" and replace them with role-specific groups.
    2. **Role-Based Access Control (RBAC):** Implement RBAC to limit access to file shares based on user roles, in line with **Appendix A to Part 748, Section III(B)(2)**.
    3. **Limit Administrator Access:** Ensure administrative access to sensitive file shares is limited to trusted users and necessary tasks.
- **Regulatory Reference:**
    - **Appendix A to Part 748, Section III(B)(2):** Requires that access be limited to authorized users.

3. Encrypt Sensitive Data

- **Objective:** Ensure that sensitive data on file shares is encrypted both in transit and at rest.
- **Actions for Compliance:**

1. **Encrypt Files:** Use encryption algorithms such as AES-256 to encrypt files containing personally identifiable information (PII) or financial data.
2. **Encrypt Data in Transit:** Implement encryption protocols like TLS to secure data transmitted over the network, meeting the requirements of **Appendix A to Part 748, Section III(B)(1)**.

- **Regulatory Reference:**
  - **Appendix A to Part 748, Section III(B)(1):** Requires encryption and other security measures to protect sensitive information.

4. Restrict Credential Storage

- **Objective:** Ensure that credentials, especially administrator-level ones, are not stored on network file shares.
- **Actions for Compliance:**
  1. **Remove Stored Credentials:** Conduct a review of file shares to identify and remove any stored credentials, in compliance with **Appendix A to Part 748, Section III(B)(2)**.
  2. **Use Secure Vaults:** Store credentials in secure vaults or privileged access management (PAM) systems with robust access controls.
- **Regulatory Reference:**
  - **Appendix A to Part 748, Section III(B)(2):** Prohibits unauthorized access to sensitive systems, including credentials.

5. Configure File Auditing and Monitoring

- **Objective:** Track and monitor access to sensitive file shares to detect unauthorized access or changes.
- **Actions for Compliance:**
  1. **Enable File Auditing:** Set up auditing to track access to sensitive file shares, including unauthorized access attempts, as required by **Appendix A to Part 748, Section III(C)**.
  2. **Set Real-Time Alerts:** Implement real-time alerts to notify security teams when unauthorized access or modifications occur.
  3. **Review Audit Logs Regularly:** Ensure regular reviews of access logs to identify any unusual or malicious activity.
- **Regulatory Reference:**
  - **Appendix A to Part 748, Section III(C):** Requires monitoring and auditing of systems to detect unauthorized access or system modifications.

6. Implement Multi-Factor Authentication (MFA)

- **Objective:** Strengthen access control by requiring multi-factor authentication for administrative access to file shares.
- **Actions for Compliance:**
  1. **MFA for Admins:** Ensure MFA is required for administrators accessing file shares, aligning with **Appendix A to Part 748, Section III(B)(1)(c)**.
  2. **MFA for Critical File Shares:** Consider implementing MFA for users accessing especially sensitive file shares.

- **Regulatory Reference:**
    - **Appendix A to Part 748, Section III(B)(1)(c):** Requires strong authentication measures, including MFA.

7. Use Network Segmentation

- **Objective:** Segregate sensitive file shares from other network resources to reduce exposure to unauthorized users.
- **Actions for Compliance:**
    1. **Isolate Sensitive File Shares:** Place sensitive file shares in a segregated network zone with restricted access, in line with **Appendix A to Part 748, Section III(B)(2)**.
    2. **Implement VLANs:** Use Virtual Local Area Networks (VLANs) to segregate traffic based on the type of data or access needs, limiting lateral movement in case of a breach.
- **Regulatory Reference:**
    - **Appendix A to Part 748, Section III(B)(2):** Requires that sensitive data be isolated and access restricted.

8. Implement Group Policy Object (GPO) Restrictions

- **Objective:** Use GPOs to enforce file share permissions and restrict unauthorized access.
- **Actions for Compliance:**
    1. **Use GPO for File Share Restrictions:** Enforce file share permissions using GPO to centralize control over access.
    2. **Disable Guest Access:** Ensure that guest accounts and anonymous access to file shares are disabled, as required by **Appendix A to Part 748, Section III(B)(1)(c)**.
- **Regulatory Reference:**
    - **Appendix A to Part 748, Section III(B)(1)(c):** Requires strict access control to prevent unauthorized file sharing.

9. Regularly Patch and Update Systems

- **Objective:** Keep file servers and associated software up to date to prevent vulnerabilities that could be exploited to access file shares.
- **Actions for Compliance:**
    1. **Patch File Servers Regularly:** Ensure that file servers, operating systems, and file-sharing software are regularly patched, in line with **Appendix A to Part 748, Section III(B)(1)**.
    2. **Harden File Servers:** Follow best practices for server hardening, such as disabling unused services, enforcing strong passwords, and limiting administrative privileges.
- **Regulatory Reference:**
    - **Appendix A to Part 748, Section III(B)(1):** Requires that systems be regularly updated and hardened to prevent vulnerabilities.

10. Security Awareness Training

- **Objective:** Educate users on the risks associated with file sharing and enforce best practices.
- **Actions for Compliance:**
    1. **Train Users:** Provide regular security awareness training to users on the importance of securing sensitive data on file shares, aligning with **Appendix A to Part 748, Section III(A)**.
    2. **Spot Phishing:** Educate staff to identify phishing and social engineering attacks that could lead to unauthorized file share access.
- **Regulatory Reference:**
    - **Appendix A to Part 748, Section III(A):** Requires training programs to ensure that personnel understand and follow the information security program.

11. Test Access Controls

- **Objective:** Regularly test access controls to ensure they are effective at preventing unauthorized access to file shares.
- **Actions for Compliance:**
    1. **Conduct Penetration Testing:** Perform regular penetration testing to identify weaknesses in file share access controls, simulating potential attack vectors, as required by **Appendix A to Part 748, Section III(C)**.
    2. **Run Internal Audits:** Audit access control policies regularly to ensure adherence to the principle of least privilege and detect any misconfigurations or gaps.
- **Regulatory Reference:**
    - **Appendix A to Part 748, Section III(C):** Requires testing and monitoring to ensure the effectiveness of access controls.

12. Follow Up with Incident Response

- **Objective:** Ensure any unauthorized access to file shares is remediated quickly, and compromised credentials are addressed.
- **Actions for Compliance:**
    1. **Change Exposed Credentials:** Immediately change credentials that may have been exposed, in line with **Appendix A to Part 748, Section III(A)**, which requires timely incident response.
    2. **Remediate Compromised Systems:** Investigate compromised systems, identify the scope of the breach, and ensure full remediation.
- **Regulatory Reference:**
    - **Appendix A to Part 748, Section III(A):** Requires an incident response program to handle breaches and secure compromised data.

Conclusion

By following these steps, organizations can achieve compliance with **12 CFR 748.0** and **Appendix A to Part 748** while securing their network file shares. This comprehensive approach covers access control, encryption, auditing, segmentation, patch

management, and incident response, ensuring that sensitive member information is protected from unauthorized access and potential breaches.

Enhanced Compliance Checklist for Authentication & Authorization Systems

1. Governance & Policy Compliance (Effectiveness: 95%)

☑ Key Actions:

- Establish a **formal Authentication and Authorization Policy** aligned with **CIS 4.1, 6.1, 6.2**.
- Designate **IAM Admins, IT Security, and Compliance Officers** as access governance owners.
- Conduct **quarterly access reviews** and **remove or deactivate inactive accounts** after 90 days.

◇ MITRE ATT&CK Mapping:

- **T1078 - Valid Accounts** (Quarterly reviews remove inactive credentials)
- **T1133 - External Remote Services** (Access governance controls external authentication)

2. Authentication System Compliance (Effectiveness: 92%)

☑ Key Actions:

- Require **MFA for all privileged accounts and externally accessible systems (VPN, cloud apps, RDP)**.
- Enforce **password policies** (Minimum 12-character length, complexity rules, 90-day rotation for privileged users).
- Implement **secure Single Sign-On (SSO) with SAML/OAuth/OpenID Connect integrations**.
- **Secure service accounts** (disable interactive login, use unique non-reused credentials).
- **Enhance web authentication security**:
    - Implement **secure session management & cookie protections**.
    - Enforce **MFA for admin-level access to web applications**.
    - Conduct **web authentication security testing (OWASP Top 10 review)**.

◇ MITRE ATT&CK Mapping:

- **T1555 - Credentials from Password Stores** (Privileged Access Management (PAM) restricts access)
- **T1110 - Brute Force** (Strong password policies & lockout mechanisms reduce risk)
- **T1556 - Modify Authentication Process** (SSO & RBAC prevent unauthorized modification)

3. Authorization & Access Control Compliance (Effectiveness: 93%)

☑ Key Actions:

- Implement **Role-Based & Attribute-Based Access Control (RBAC/ABAC)** and maintain a **role matrix**.
- Use **Privileged Access Management (PAM) tools** (CyberArk, BeyondTrust) with Just-in-Time (JIT) access.
- Restrict **third-party access** with zero-trust principles.
- **Enhance remote access security:**
    - Disable unnecessary **Remote Desktop Protocol (RDP) access**.
    - Enforce **MFA for RDP logins & VPN access**.
    - **Monitor RDP session logs for anomalous activity**.

◇ MITRE ATT&CK Mapping:

- **T1548 - Abuse Elevation Control Mechanism** (RBAC/ABAC restricts unauthorized privilege escalation)
- **T1021 - Remote Services (RDP, SMB, SSH, WinRM)** (Disabling unnecessary RDP reduces attack surface)

4. Logging, Monitoring & Incident Response (Effectiveness: 96%)

☑ Key Actions:

- Enable **logging for all authentication events (success, failure, anomalies)** and store logs for **at least 1 year**.
- Set up **real-time alerts for suspicious logins via SIEM** (Splunk, Elastic, Microsoft Defender for Identity).
- Implement **Incident Response Plans (IRP) for authentication breaches**.

- **Enhance insider threat detection:**
    - Implement **User and Entity Behavior Analytics (UEBA)**.
    - Monitor **unusual privileged account activity**.
    - Set alerts for **excessive permission changes**.

◇ **MITRE ATT&CK Mapping:**

- **T1070 - Indicator Removal on Host** (SIEM prevents log tampering & detects anomalies)
- **T1484 - Domain Policy Modification** (Logging detects unauthorized GPO modifications)

5. Security Awareness & Training (Effectiveness: 85%)

☑ **Key Actions:**

- Conduct **quarterly phishing awareness training** to prevent credential theft.
- Train employees on **social engineering tactics targeting authentication credentials**.
- Perform **quarterly simulated phishing tests** and establish a **user-reported suspicious login mechanism**.

◇ **MITRE ATT&CK Mapping:**

- **T1074 - Data Staging** (Security training ensures employees recognize unauthorized data exfiltration attempts)

6. Regulatory Compliance & Auditing (Effectiveness: 98%)

☑ **Key Actions:**

- Align IAM controls with **NIST 800-53, ISO 27001, PCI-DSS, and 12 CFR Part 748**.
- Maintain **CIS Benchmark configurations for authentication systems**.
- Conduct **quarterly access reviews & penetration tests**.
- Maintain **audit trails and generate compliance reports** every **6 months**.

◇ **MITRE ATT&CK Mapping:**

- **T1499 - Endpoint Denial of Service (DoS)** (Monitoring of authentication anomalies mitigates brute-force DoS attempts)

7. Automated IAM Monitoring & Continuous Compliance Tracking (Effectiveness: 97%)

☑ **Key Actions:**

- Implement **IAM monitoring tools** (Microsoft Entra ID, AWS IAM Access Analyzer, Google Cloud IAM).
- Automate **real-time identity analytics** to detect policy violations.
- Use **SIEM & UEBA to detect behavioral anomalies in authentication**.
- Enforce **continuous compliance monitoring** for IAM settings.
- Conduct **automated access certification reviews** every quarter.

◇ **MITRE ATT&CK Mapping:**

- **T1078 - Valid Accounts** (Automated IAM monitoring detects unauthorized credential use)
- **T1087 - Account Discovery** (Continuous compliance tracking prevents excessive privilege accumulation)

Final Effectiveness Breakdown

Category	Effectiveness %	Key Enhancements
Governance & Policy Compliance	95%	Strong compliance & oversight processes
Authentication System Compliance	92%	Web authentication & MFA enhancements
Authorization & Access Control	93%	RDP lockdown, RBAC/ABAC, PAM improvements
Logging & Incident Response	96%	SIEM, behavior analytics, insider threat detection
Security Awareness & Training	85%	Phishing, social engineering prevention

Regulatory Compliance & Auditing	98%	Full alignment with NIST, ISO 27001, PCI-DSS
Automated IAM Monitoring & Continuous Compliance Tracking	97%	IAM anomaly detection, automated reviews

☑ Overall Effectiveness: 94%

The Digital Vault aligns with CIS recommended security controls, covering **MFA enforcement, privileged access management, logging, web authentication, RDP restrictions, insider threat detection, security awareness training, and automated IAM monitoring**.

CyberArk Digital Vault server runs on an isolated and trusted platform.
This Digital Vault server is not a member of any Windows domain.
Third-party software is not installed on the Digital Vault server.
Network traffic to the Digital Vault server is restricted to CyberArk protocols
- Network traffic from the Digital Vault server is restricted to CyberArk protocols and approved integrations such as LDAP for user and group provisioning or SMTP for email alerts
- The Digital Vault server operating system credentials are unique
- Any infrastructure hosting the Digital Vault server has the same controls applied to it as those applied to the Digital Vault server
- Microsoft security updates are applied regularly. For details, see Integrate the Digital Vault with a Windows Patch Server (WSUS)
- CyberArk strongly recommends using a dedicated WSUS Server for updating the Digital Vault
- Use network-based firewalls to restrict, encrypt and authenticate inbound administrative traffic

https://docs.cyberark.com/PAS/10.10/en/Content/Security/Standards-CyberArks%20Digital%20Vault%20Server%20Security%20Standard.htm

PowerShell CMD

Monday, August 12, 2024 3:34 PM

1. List All Active Directory Users and Their Authentication Methods

This script retrieves all users and their relevant authentication properties, such as `SamAccountName`, `UserPrincipalName`, `LastLogonDate`, and `PasswordLastSet`.

```
# Define the output Excel file path
$excelFilePath = "C:\Reports\ADUserAudit.xlsx"

# Retrieve all Active Directory users with their properties
$users = Get-ADUser -Filter * -Property SamAccountName, UserPrincipalName, LastLogonDate, PasswordLastSet |
Select-Object SamAccountName, UserPrincipalName, LastLogonDate, PasswordLastSet

# Export the results to an Excel file
$users | Export-Excel -Path $excelFilePath -WorksheetName "AD Users" -AutoSize
```

Use case:

- Provides a complete list of users and their last logon time, helping administrators audit accounts that may no longer be active.
- Useful for reviewing password policies and authentication activity.

2. List All Active Directory Groups and Their Members

This script lists all AD groups along with their members.

```
# Retrieve all AD groups and their members
$groups = Get-ADGroup -Filter * -Property Members | ForEach-Object {
    $group = $_
    $members = Get-ADGroupMember -Identity $group.DistinguishedName | Select-Object -ExpandProperty SamAccountName
    [PSCustomObject]@{
        GroupName = $group.Name
        Members   = [string]::Join(", ", $members)
    }
}

# Export the results to the same Excel file with a new worksheet
$groups | Export-Excel -Path $excelFilePath -WorksheetName "AD Groups" -AutoSize
```

Use case:

- Helps identify users with access to specific groups and ensure access rights are properly configured.
- Can identify any inappropriate or excessive group membership, especially for sensitive groups like `Domain Admins`.

3. List Users with Specific Authentication Methods

This script checks if users meet specific password and authentication requirements, such as password length and MFA status.

```
# Retrieve and check users' password policies (example)
$minPasswordLength = 8
$complexityRequired = $true

$authUsers = Get-ADUser -Filter * -Property PasswordLastSet, PasswordNeverExpires |
Where-Object { $_.PasswordLastSet -ne $null } |
Select-Object SamAccountName, PasswordLastSet, PasswordNeverExpires

# Export the results to Excel
$authUsers | Export-Excel -Path $excelFilePath -WorksheetName "Password Policies" -AutoSize
```

Use case:

- Allows administrators to check password policy compliance.
- Audits users whose passwords might be set to never expire or are outdated.

4. List All Authentication Systems in Use

This script provides a list of all authentication systems in use, such as Active Directory or third-party identity providers.

```
# Retrieve all authentication systems
$authenticationSystems = @(
    [PSCustomObject]@{SystemName="AD"; Type="Directory Service"},
    [PSCustomObject]@{SystemName="Okta"; Type="Identity Provider"},
    [PSCustomObject]@{SystemName="AzureAD"; Type="Cloud Directory"}
)

# Export the results to Excel
$authenticationSystems | Export-Excel -Path $excelFilePath -WorksheetName "Auth Systems" -AutoSize
```

Use case:

- Identifies all authentication systems that are integrated into the environment for centralized auditing and management.

5. List All Service Accounts and Their Permissions

This script lists service accounts and their permissions, which can help identify over-privileged accounts.

```
# Retrieve all service accounts and their permissions
$serviceAccounts = Get-LocalUser | Where-Object { $_.Name -like "*svc*" } | ForEach-Object {
    $groups = Get-LocalGroupMembership -User $_.Name
    [PSCustomObject]@{
        AccountName = $_.Name
        Groups      = [string]::Join(", ", $groups)
    }
}

# Export the results to Excel
$serviceAccounts | Export-Excel -Path $excelFilePath -WorksheetName "Service Accounts" -AutoSize
```

Use case:

- Audits service accounts for proper permissions and reduces the risk of over-privileged accounts.
- Helps ensure that service accounts have only the necessary access rights.

6. Check Access to Critical Resources

This script checks which users have access to critical resources (e.g., sensitive file shares).

```
# Define critical resources
$criticalResources = @("C:\SensitiveFolder", "D:\CriticalFiles")

# Check user permissions on critical resources
$resourceAccess = foreach ($resource in $criticalResources) {
    $acl = Get-Acl -Path $resource
    $acl.Access | ForEach-Object {
        [PSCustomObject]@{
            Resource          = $resource
            Identity          = $_.IdentityReference
            AccessControlType  = $_.AccessControlType
            FileSystemRights   = $_.FileSystemRights
        }
    }
}

# Export the results to Excel
$resourceAccess | Export-Excel -Path $excelFilePath -WorksheetName "Critical Resource Access" -AutoSize
```

Use case:

- Provides an overview of user permissions on sensitive files or directories, ensuring appropriate access control.

7. Review Users with Elevated Permissions

This script checks for users with elevated permissions or who are members of administrative groups like `Domain Admins` or `Enterprise Admins`.

```
# Define elevated permissions groups
$elevatedGroups = @("Domain Admins", "Enterprise Admins", "Administrators")

# Retrieve and list users in elevated groups
$adminUsers = foreach ($group in $elevatedGroups) {
    Get-ADGroupMember -Identity $group | Select-Object Name, SamAccountName, @{Name="Group";Expression={$group}}
}

# Export the results to Excel
$adminUsers | Export-Excel -Path $excelFilePath -WorksheetName "Elevated Users" -AutoSize
```

Use case:

- Audits administrative privileges to ensure that only authorized users have elevated access.

```
Get-ADUser -filter * -properties passwordlastset, passwordneverexpires, lastlogondate | sort-object
Name, passwordlastset, passwordneverexpires, lastlogondate | Export-csv -path c:\reports
\userpwinfo.csv
```

- Helps detect any over-privileged users that could pose a security risk.

8. Review Access to Applications

This script audits access to specific applications, though it may require customization based on the applications in use.

```
# Define applications and their access (example)
$appAccess = @(
    [PSCustomObject]@{UserName="user1"; Application="App1"},
    [PSCustomObject]@{UserName="user2"; Application="App2"}
)

# Export the results to Excel
$appAccess | Export-Excel -Path $excelFilePath -WorksheetName "Application Access" -AutoSize
```

Use case:

- Audits which users have access to certain applications, ensuring only authorized individuals can use sensitive applications.

9. Check MFA Status for Users

This script checks whether users have multi-factor authentication (MFA) enabled. You would need to customize it based on your MFA system.

```
# Placeholder for MFA status retrieval
$mfaUsers = Get-ADUser -Filter * -Property MFAEnabled | Where-Object { $_.MFAEnabled -eq $true } |
Select-Object SamAccountName, MFAEnabled

# Export the results to Excel
$mfaUsers | Export-Excel -Path $excelFilePath -WorksheetName "MFA Status" -AutoSize
```

Use case:

- Helps audit users with MFA to ensure strong authentication is enforced for sensitive accounts.

10. List All Authorization Systems

This script lists all authorization systems in use, which helps audit the authorization framework.

```
# Define authorization systems
$authorizationSystems = @(
    [PSCustomObject]@{SystemName="Active Directory"; Type="Directory Service"},
    [PSCustomObject]@{SystemName="LDAP"; Type="Directory Service"},
    [PSCustomObject]@{SystemName="OAuth"; Type="Token-Based Authentication"}
)

# Export the results to Excel
$authorizationSystems | Export-Excel -Path $excelFilePath -WorksheetName "Authorization Systems" -AutoSize
```

Use case:

- Provides an overview of the authorization systems integrated within the environment for auditing purposes.

To **check for unused accounts** in **Active Directory**, you can use PowerShell to identify accounts that haven't been used in a while. Unused accounts can pose a security risk, as attackers might exploit them to gain unauthorized access. Here's a PowerShell script to find inactive or unused accounts based on the `LastLogonDate` or `PasswordLastSet` properties.

PowerShell Script to Check for Unused Accounts

```
# Define the period of inactivity (e.g., 90 days)
$inactiveDays = 90
$timeLimit = (Get-Date).AddDays(-$inactiveDays)

# Retrieve all Active Directory users
Get-ADUser -Filter * -Property SamAccountName, UserPrincipalName, LastLogonDate, PasswordLastSet, Enabled |
Where-Object {
    ($_.LastLogonDate -eq $null -or $_.LastLogonDate -lt $timeLimit) -and
    ($_.Enabled -eq $true)
} |
Select-Object SamAccountName, UserPrincipalName, LastLogonDate, PasswordLastSet, Enabled |
Format-Table -AutoSize
```

How This Script Works:

1. **Time Limit for Inactivity:**
    - The script defines the period of inactivity as 90 days (you can adjust this number based on your organization's requirements).
    - It calculates the cutoff date by subtracting the specified number of days from the current date.
2. **Filter Active Directory Users:**
    - The script retrieves all users with the `LastLogonDate`, `PasswordLastSet`, and `Enabled` properties.
    - It filters for accounts that:
        - Have a `LastLogonDate` older than the cutoff date (or never logged on if `LastLogonDate` is null).
        - Are still enabled (active accounts).
3. **Output:**
    - The script outputs a table showing the `SamAccountName`, `UserPrincipalName`, `LastLogonDate`, `PasswordLastSet`, and `Enabled` status for each user account that hasn't been used for the specified period.

Optional Enhancements:

- **Disable Inactive Accounts:** If you want to disable unused accounts automatically after identifying them, you can add a command to disable them.

```
Get-ADUser -Filter * -Property LastLogonDate, Enabled |
Where-Object {
    ($_.LastLogonDate -eq $null -or $_.LastLogonDate -lt $timeLimit) -and
    ($_.Enabled -eq $true)
} |
Disable-ADAccount
```

Notify Administrators: You can send an email notification or log these findings in a central place (e.g., a CSV file) for review.

```
# Export inactive users to a CSV file
Get-ADUser -Filter * -Property SamAccountName, UserPrincipalName, LastLogonDate, PasswordLastSet, Enabled |
Where-Object {
    ($_.LastLogonDate -eq $null -or $_.LastLogonDate -lt $timeLimit) -and
    ($_.Enabled -eq $true)
} |
Select-Object SamAccountName, UserPrincipalName, LastLogonDate, PasswordLastSet, Enabled |
Export-Csv -Path "C:\Reports\InactiveUsers.csv" -NoTypeInformation
```

Use Cases:

- **Security Audits:** Regularly review inactive accounts to ensure they are either disabled or removed.
- **Compliance:** Ensure compliance with organizational security policies that dictate how long inactive accounts can remain enabled.
- **Cleanup:** This script can help clean up Active Directory by identifying accounts that are no longer in use.

By regularly reviewing and disabling unused accounts, you can help minimize security risks associated with dormant accounts that could be exploited by attackers.

Automating the execution of these PowerShell scripts can be done using **Task Scheduler** in Windows, which allows you to run scripts at specified intervals or when certain events occur. Here's how you can automate these PowerShell scripts to generate regular reports in Excel:

Step 1: Consolidate Scripts into a Single PowerShell Script

Create a single PowerShell script that runs all the commands from the previous steps, and exports them to an Excel file. Here's an example script that combines all the tasks into one file.

Consolidated PowerShell Script (`AD_Audit_Report.ps1`):

```
# Load the ImportExcel module
Import-Module ImportExcel

# Define the output Excel file path
$excelFilePath = "C:\Reports\ADUserAudit.xlsx"

### 1. List All Active Directory Users and Their Authentication Methods ###
$users = Get-ADUser -Filter * -Property SamAccountName, UserPrincipalName, LastLogonDate, PasswordLastSet |
Select-Object SamAccountName, UserPrincipalName, LastLogonDate, PasswordLastSet

# Export the results to an Excel file
$users | Export-Excel -Path $excelFilePath -WorksheetName "AD Users" -AutoSize

### 2. List All Active Directory Groups and Their Members ###
$groups = Get-ADGroup -Filter * -Property Members | ForEach-Object {
    $group = $_
    $members = Get-ADGroupMember -Identity $group.DistinguishedName | Select-Object -ExpandProperty SamAccountName
    [PSCustomObject]@{
        GroupName = $group.Name
        Members   = [string]::Join(", ", $members)
    }
}

# Export to Excel
$groups | Export-Excel -Path $excelFilePath -WorksheetName "AD Groups" -AutoSize
```

```
### 3. List Users with Specific Authentication Methods ###
$authUsers = Get-ADUser -Filter * -Property PasswordLastSet, PasswordNeverExpires |
Where-Object { $_.PasswordLastSet -ne $null } |
Select-Object SamAccountName, PasswordLastSet, PasswordNeverExpires

# Export to Excel
$authUsers | Export-Excel -Path $excelFilePath -WorksheetName "Password Policies" -AutoSize

### 4. List All Authentication Systems in Use ###
$authenticationSystems = @(
    [PSCustomObject]@{SystemName="AD"; Type="Directory Service"},
    [PSCustomObject]@{SystemName="Okta"; Type="Identity Provider"},
    [PSCustomObject]@{SystemName="AzureAD"; Type="Cloud Directory"}
)

# Export to Excel
$authenticationSystems | Export-Excel -Path $excelFilePath -WorksheetName "Auth Systems" -AutoSize

### 5. List All Service Accounts and Their Permissions ###
$serviceAccounts = Get-LocalUser | Where-Object { $_.Name -like "*svc*" } | ForEach-Object {
    $groups = Get-LocalGroupMembership -User $_.Name
    [PSCustomObject]@{
        AccountName = $_.Name
        Groups      = [string]::Join(", ", $groups)
    }
}

# Export to Excel
$serviceAccounts | Export-Excel -Path $excelFilePath -WorksheetName "Service Accounts" -AutoSize

### 6. Check Access to Critical Resources ###
$criticalResources = @("C:\SensitiveFolder", "D:\CriticalFiles")
$resourceAccess = foreach ($resource in $criticalResources) {
    $acl = Get-Acl -Path $resource
    $acl.Access | ForEach-Object {
        [PSCustomObject]@{
            Resource          = $resource
            Identity          = $_.IdentityReference
            AccessControlType  = $_.AccessControlType
            FileSystemRights   = $_.FileSystemRights
        }
    }
}

# Export to Excel
$resourceAccess | Export-Excel -Path $excelFilePath -WorksheetName "Critical Resource Access" -AutoSize

### 7. Review Users with Elevated Permissions ###
$elevatedGroups = @("Domain Admins", "Enterprise Admins", "Administrators")
$adminUsers = foreach ($group in $elevatedGroups) {
    Get-ADGroupMember -Identity $group | Select-Object Name, SamAccountName, @{Name="Group";Expression={$group}}
}

# Export to Excel
$adminUsers | Export-Excel -Path $excelFilePath -WorksheetName "Elevated Users" -AutoSize

### 8. Review Access to Applications ###
$appAccess = @(
    [PSCustomObject]@{UserName="user1"; Application="App1"},
    [PSCustomObject]@{UserName="user2"; Application="App2"}
)

# Export to Excel
$appAccess | Export-Excel -Path $excelFilePath -WorksheetName "Application Access" -AutoSize

### 9. Check MFA Status for Users ###
$mfaUsers = Get-ADUser -Filter * -Property MFAEnabled | Where-Object { $_.MFAEnabled -eq $true } |
Select-Object SamAccountName, MFAEnabled

# Export to Excel
$mfaUsers | Export-Excel -Path $excelFilePath -WorksheetName "MFA Status" -AutoSize

### 10. List All Authorization Systems ###
$authorizationSystems = @(
    [PSCustomObject]@{SystemName="Active Directory"; Type="Directory Service"},
    [PSCustomObject]@{SystemName="LDAP"; Type="Directory Service"},
    [PSCustomObject]@{SystemName="OAuth"; Type="Token-Based Authentication"}
)

# Export to Excel
$authorizationSystems | Export-Excel -Path $excelFilePath -WorksheetName "Authorization Systems" -AutoSize
```

Step 2: Schedule the Script with Task Scheduler

Now that you have a consolidated script, you can schedule it to run at regular intervals.

1. Open Task Scheduler

- Press `Win + R`, type `taskschd.msc`, and press `Enter` to open **Task Scheduler**.

2. Create a New Task

1. In the **Actions** pane, click **Create Task**.
2. In the **General** tab:
    - Name your task, e.g., "Automated AD Audit Report."
    - Select **Run whether user is logged on or not**.
    - Select **Run with highest privileges**.
3. In the **Triggers** tab:
    - Click **New** to create a new trigger.
    - Choose **Daily** or any desired schedule.
    - Set the time and repeat interval if necessary.
4. In the **Actions** tab:
    - Click **New** and choose **Start a program**.
    - In the **Program/script** field, enter

powershell.exe

In the **Add arguments**field, type the path to your script, e.g

-File "C:\Scripts\AD_Audit_Report.ps1"

1. In the **Conditions** and **Settings** tabs, adjust settings to your preferences (e.g., allow the task to run on battery, restart if it fails).
2. Click **OK**, and enter your credentials when prompted.

Step 3: Review Reports

Your Excel report will be generated at the scheduled time and saved at the specified location (`C:\Reports\ADUserAudit.xlsx`).

Additional Tips:

- **Testing the Script**: Before scheduling, test the PowerShell script manually to ensure all worksheets are created and data is exported correctly.
- **Notifications**: You can extend the script to send email notifications when the report is generated, using `Send-MailMessage`.
- **Error Handling**: Add error handling to the script by wrapping sections in `try-catch` blocks to log any errors encountered during the run.

This process will automate the generation of Active Directory audit reports, saving time and ensuring regular monitoring of user activity, permissions, and system configurations.

Remote Access

Thursday, September 5, 2024 5:37 AM

GoToMyPC provides convenient remote access, but financial institutions must take extra care to ensure compliance with stringent industry standards and mitigate risks. Below is an organized set of risks and remediation strategies specifically for financial institutions considering GoToMyPC, touching on key categories such as **encryption, access control, compliance, endpoint security, and vendor risk management**.

Key Risks and Mitigations

1. Encryption and Data Security

- **Risk: Insufficient Data Protection**
  - **Mitigation:**
    - Use **AES 256-bit encryption** (GoToMyPC default) for all data transmission between client and host computers. Ensure the encryption protocol is strong enough to meet financial standards.
    - For added security, enforce **end-to-end encryption** for sensitive transactions.
    - Implement **data encryption at rest** on both host and client devices to prevent local data exposure.
  - **Risk Level: High**

2. Compliance with Industry Standards

- **Risk: Non-compliance with regulations such as PCI-DSS, SOX, GLBA, FFIEC**
  - **Mitigation:**
    - Verify if **GoToMyPC** provides necessary logging, reporting, and auditing features to meet compliance requirements.
    - Conduct a **compliance gap analysis** for GoToMyPC, identifying areas that need additional controls.
    - Implement supplementary tools for **monitoring and reporting** to meet financial compliance standards.
  - **Risk Level: High**

3. Authentication and Access Control

- **Risk: Unauthorized Access**
  - **Mitigation:**
    - Implement **Multi-Factor Authentication (MFA)** to strengthen access control.
    - Enforce a **strong password policy** (12+ characters, complexity, regular changes).
    - Use **Role-Based Access Control (RBAC)** to ensure that users only access what is necessary for their role, following the **principle of least privilege**.
  - **Risk Level: High**

4. Endpoint Security

- **Risk: Vulnerability at Host and Client Devices**
  - **Mitigation:**
    - Ensure both host and client devices use **up-to-date antivirus software**, **firewalls**, and **full disk encryption**.

        - Enable **Data Loss Prevention (DLP)** tools to monitor file transfers and prevent unauthorized data movement.
        - Require regular **patching and updates** for both host and remote devices to ensure there are no vulnerabilities.
    - **Risk Level: Medium**

5. Logging and Monitoring

- **Risk: Inadequate Logging for Audits**
    - **Mitigation:**
        - Enable detailed **audit logs** for remote access sessions, logging user activity, session duration, and system changes.
        - Integrate with **Security Information and Event Management (SIEM)** systems for real-time monitoring and anomaly detection.
        - Review logs regularly for suspicious behavior, using **intrusion detection systems (IDS)**.
    - **Risk Level: High**

6. VPN and Network Security

- **Risk: Vulnerability in Remote Connections**
    - **Mitigation:**
        - Require the use of a **Virtual Private Network (VPN)** in conjunction with GoToMyPC for secure, encrypted tunnels.
        - Use **firewalls** and **Intrusion Prevention Systems (IPS)** to block unauthorized remote connections.
    - **Risk Level: Medium**

7. Remote Session Security

- **Risk: Unauthorized Access or Data Leakage**
    - **Mitigation:**
        - Configure **automatic session timeouts** to log users out after periods of inactivity (e.g., 15-30 minutes).
        - Enable **session locking** and require users to re-authenticate after idle periods.
        - Review and limit **file transfer capabilities** for sensitive data to minimize the risk of data leakage.
    - **Risk Level: Medium**

8. Data Residency and Privacy Concerns

- **Risk: Non-compliance with Data Residency Laws (e.g., GDPR)**
    - **Mitigation:**
        - Verify the **geographic location of GoToMyPC's servers** and whether they comply with data sovereignty laws.
        - Ensure that data transfer complies with **privacy regulations** like **GDPR**, **GLBA**, or local data residency laws.
        - Implement **data anonymization** or **tokenization** to minimize exposure of sensitive data.
    - **Risk Level: High**

9. Vendor Risk Management

- **Risk: Vendor Compromise or Breach**
    - **Mitigation:**
        - Conduct a **vendor risk assessment** and review **Service Level Agreements (SLAs)** to ensure GoToMyPC's security

protocols align with your institution's requirements.
        - Verify that GoToMyPC has strong **incident response mechanisms** and clear processes for addressing data breaches or vulnerabilities.
    - **Risk Level: Medium**

10. Human Error and Insider Threats

- **Risk: Insider Threats and User Error**
    - **Mitigation:**
        - Provide regular **security awareness training** to all users, emphasizing secure remote access practices, phishing, and data protection.
        - Implement **Data Loss Prevention (DLP)** to monitor and control data transfers by authorized users.
        - Require **session monitoring** for privileged accounts and ensure **audit trails** for critical actions.
    - **Risk Level: Medium**

Key Security Configurations for Compliance

1. **Multi-Factor Authentication (MFA):**
    - Implement MFA for all users, particularly for administrators accessing sensitive systems.
    - Enforce **GoToMyPC's Two-Factor Authentication (2FA)** as a baseline, ensuring compliance with financial regulations.
2. **Logging and Monitoring:**
    - Enable **audit logs** for all remote access sessions, ensuring they record user activity, session times, and any changes made.
    - Implement **real-time monitoring** and set up alerts for unauthorized or suspicious access attempts.
3. **Network Security:**
    - Combine GoToMyPC with a **VPN** to create secure tunnels between remote users and internal systems.
    - Configure **firewalls** and **IPS/IDS** systems to allow only authorized traffic.
4. **Encryption of Data:**
    - Ensure **AES 256-bit encryption** for all sessions and enforce **data-at-rest encryption** on host machines handling sensitive information.
5. **Incident Response and Backup:**
    - Have a robust **incident response plan** in place to address unauthorized access or data breaches.
    - Ensure regular **backups** of critical data accessed via GoToMyPC to support data integrity and recovery in case of an incident.

Conclusion:

Using **GoToMyPC** in a financial setting requires additional measures to ensure compliance with financial regulations such as PCI-DSS, SOX, GLBA, and FFIEC. To mitigate risks, focus on strengthening **authentication, encryption, logging, network security, and vendor risk management**. Conduct regular audits and implement necessary security policies to protect sensitive financial data during remote access

sessions.

Quest

Thursday, September 5, 2024 6:27 AM

To ensure compliance with **12 CFR 748.0** and **Appendix A to Part 748, Title 12** while using **Quest Change Auditor** for Active Directory (AD) security and configuration management, your focus should be on auditing and reporting key areas of AD configuration, access control, and security policies that protect sensitive member information and ensure adherence to regulatory standards. Below are the **specific compliance references** tied to each report category, showing how each area of AD management helps meet the regulatory requirements:

1. Group Policy Object (GPO) Changes

- **Purpose:** Ensures that unauthorized changes to security and configuration settings in AD are detected and logged.
- **Compliance Reference: 12 CFR 748.0(b)** requires institutions to maintain a written security program that addresses controls for protecting member information. **Appendix A, Part 748, Section III(B)(2)** mandates restricting access to sensitive information and ensuring security settings are enforced via GPOs.
- **Key Compliance Actions:**
    - Audit GPO modifications to ensure security controls are not tampered with.
    - Track GPO linking/unlinking, as unauthorized changes can weaken access controls or configuration settings.

2. User and Group Membership Changes

- **Purpose:** Tracks changes to AD users and security group memberships, especially privileged accounts.
- **Compliance Reference: Appendix A, Part 748, Section III(B)(2)** requires limiting access to sensitive systems and data to authorized personnel. Changes to privileged groups such as **Domain Admins** must be monitored to ensure access control policies are maintained.
- **Key Compliance Actions:**
    - Monitor user and group membership changes, ensuring only authorized personnel have access to critical resources.
    - Flag changes to privileged accounts that could indicate potential insider threats or mismanagement.

3. AD Permissions Changes

- **Purpose:** Detects changes in AD object permissions that could lead to privilege escalation or security breaches.
- **Compliance Reference: Appendix A, Part 748, Section III(B)(1)(c)** requires institutions to implement safeguards, including authentication mechanisms and access control. Unauthorized changes in permissions pose risks of inappropriate access.

- **Key Compliance Actions:**
    - Ensure permissions changes on critical AD objects are logged and reviewed to avoid unauthorized access to sensitive data.

4. Authentication and Logon Events

- **Purpose:** Monitors for suspicious or unauthorized login activities to detect potential security incidents.
- **Compliance Reference: Appendix A, Part 748, Section III(B)(1)(c)** requires multifactor authentication (MFA) and monitoring of login attempts, especially for critical systems handling sensitive member data.
- **Key Compliance Actions:**
    - Monitor failed and successful logon attempts to detect potential brute force attacks or unauthorized access.
    - Log access to sensitive areas and critical systems, particularly for privileged accounts.

5. Service Account Usage

- **Purpose:** Audits the use of service accounts to ensure they are not misused or compromised.
- **Compliance Reference: Appendix A, Part 748, Section III(B)(2)** requires restricting access to sensitive systems to authorized personnel only. Service account usage must be carefully monitored due to their elevated privileges.
- **Key Compliance Actions:**
    - Monitor service account logon activity to ensure they are not being used inappropriately.
    - Detect changes to service account permissions or properties.

6. Computer and Domain Controller Changes

- **Purpose:** Monitors changes to domain controllers and key computer accounts to ensure AD security remains intact.
- **Compliance Reference: Appendix A, Part 748, Section III(B)(1)(d)** requires institutions to implement physical and logical safeguards. Monitoring domain controllers is essential for protecting the central authentication infrastructure.
- **Key Compliance Actions:**
    - Track any modifications to domain controllers, especially those affecting their security configurations or access controls.
    - Monitor changes to critical computer accounts, particularly domain controllers.

7. Schema and Configuration Changes

- **Purpose:** Tracks changes to AD schema and configuration, which could affect the stability and security of the directory.
- **Compliance Reference: Appendix A, Part 748, Section III(B)(2)** requires protecting the integrity of critical systems. Changes to AD schema and configuration must be logged to avoid unintended security or operational risks.

- **Key Compliance Actions:**
    - Audit schema modifications and configuration changes that could affect AD operations or security.
    - Review any modifications to replication settings or network configurations.

8. Password Policy and Account Lockout Policy Changes

- **Purpose:** Ensures that password policies are correctly enforced and tracks changes that could weaken security.
- **Compliance Reference: Appendix A, Part 748, Section III(B)(1)(c)** requires the enforcement of strong password policies to safeguard access to sensitive systems and data.
- **Key Compliance Actions:**
    - Ensure password complexity requirements (e.g., length, characters, expiration) are enforced.
    - Monitor changes to account lockout policies that might reduce the effectiveness of security.

9. DNS Changes

- **Purpose:** Monitors changes to DNS settings that could affect AD's ability to resolve domain resources.
- **Compliance Reference: Appendix A, Part 748, Section III(B)(1)(c)** emphasizes the protection of system configurations, including DNS, to prevent unauthorized access to domain controllers and sensitive systems.
- **Key Compliance Actions:**
    - Track changes to DNS zones and critical DNS records, especially those related to domain controllers.
    - Ensure DNS security and integrity are maintained through continuous monitoring.

10. Group Membership of Privileged Users

- **Purpose:** Tracks changes to privileged groups to ensure that only authorized users are granted elevated access.
- **Compliance Reference: Appendix A, Part 748, Section III(B)(2)** requires enforcing access control policies. Monitoring group membership changes in privileged groups like **Domain Admins** ensures compliance with this requirement.
- **Key Compliance Actions:**
    - Audit group membership changes, particularly for privileged accounts.
    - Detect and address any unauthorized additions or removals from sensitive groups.

11. Replication Monitoring

- **Purpose:** Ensures that AD replication is functioning properly and tracks any issues that may affect directory synchronization.
- **Compliance Reference: Appendix A, Part 748, Section III(B)(2)** requires

ensuring the integrity of AD replication. Disruptions in replication could lead to data inconsistencies and security gaps.

- **Key Compliance Actions:**
    - Monitor replication failures and address them promptly to avoid synchronization issues.
    - Track any changes to replication topology or settings.

12. Auditing Policy Changes

- **Purpose:** Ensures that changes to auditing policies are detected and logged, as auditing is crucial for security and compliance.
- **Compliance Reference: Appendix A, Part 748, Section III(C)** requires institutions to maintain audit trails to track access and modifications to sensitive systems. Any changes to auditing policies must be monitored to ensure they don't undermine compliance.
- **Key Compliance Actions:**
    - Track any modifications to auditing policies that could impact the institution's ability to log and monitor access to sensitive systems.
    - Ensure that audit trails are comprehensive and secure.

Conclusion:

Using **Quest Change Auditor** to monitor and report on these critical areas ensures compliance with **12 CFR 748.0** and **Appendix A to Part 748, Title 12**. Each report aligns with regulatory requirements around access control, user and group management, password policies, replication, and auditing policies, ensuring that your Active Directory environment is secure and compliant with federal guidelines.

Aruba ClearPass

Thursday, September 5, 2024 7:02 AM

Ensuring that **Aruba ClearPass** is configured securely in compliance with **12 CFR 748.0** and **Appendix A to Part 748, Title 12** is critical for financial institutions seeking to protect member information and sensitive financial data. Below are the key configurations, mapped to specific regulatory requirements from **12 CFR 748.0** and **Appendix A to Part 748**.

1. System Hardening

- **Disable Unused Services, Strong Passwords, MFA, SSH Access**
- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(c)**: Requires that financial institutions implement strong access controls and authentication mechanisms to prevent unauthorized access to sensitive data and systems.
    - **12 CFR 748.0(b)**: Mandates that the security program must include provisions for protecting member information and preventing unauthorized access.
- **Key Compliance Actions:**
    - Implement strong password policies, enforce **MFA** for ClearPass administration interfaces, and restrict SSH access to authorized hosts only. Ensure any unused services are disabled to minimize attack surfaces.

2. Access Control

- **Role-Based Access Control (RBAC), Network Segmentation, Limit Access by IP**
- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(2)**: Requires limiting access to sensitive information and systems to only those employees who need it for business reasons.
- **Key Compliance Actions:**
    - Implement **RBAC** to limit ClearPass admin access to only those who need it based on their roles. Restrict network access to ClearPass from specific IP addresses and segment ClearPass management on a separate VLAN.

3. Certificates & Encryption

- **Install Trusted Certificates, TLS, EAP-TLS, PEAP/MSCHAPv2**
- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(c)**: Mandates the use of encryption to protect member information and sensitive data during transmission over networks.

- **Key Compliance Actions:**
    - Use **TLS 1.2** or higher for all communications and replace self-signed certificates with **CA-signed certificates**. Leverage **EAP-TLS** for strong, certificate-based wireless authentication to ensure secure access to sensitive systems.

4. Policy Enforcement

- **Endpoint Compliance, Granular Access Policies, Adaptive Authentication, NAC**
- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(2)**: Requires monitoring and controlling access to sensitive information, ensuring that only devices and users meeting security policies can access critical systems.
- **Key Compliance Actions:**
    - Implement **Network Access Control (NAC)** policies with ClearPass to assess device posture and ensure that only compliant devices are granted access. Define granular access policies based on user roles, device types, and security posture to protect sensitive member data.

5. Monitoring and Logging

- **Enable Logging, Alerting, SIEM Integration**
- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(C)**: Requires institutions to implement audit controls and monitoring procedures to detect unauthorized access or suspicious activity.
- **Key Compliance Actions:**
    - Enable detailed logging of all ClearPass activities (authentication attempts, admin actions) and forward logs to a **SIEM** system for centralized monitoring and alerting. Ensure suspicious activity triggers alerts for investigation.

6. Regular Patching and Updates

- **Firmware Updates, Automatic Backup**
- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(d)**: Requires institutions to maintain systems and implement controls for timely updates and patches to mitigate security risks.
- **Key Compliance Actions:**
    - Ensure ClearPass is regularly updated with the latest **firmware and security patches**. Implement automatic backups of ClearPass configurations to protect against system failures or unauthorized changes.

7. Guest Access Security

- **Guest Isolation, Captive Portal Security**

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(d)**: Requires that financial institutions enforce physical and logical safeguards to ensure that guest access is isolated from sensitive member data and internal networks.
- **Key Compliance Actions:**
    - Isolate guest access using separate **VLANs** and configure captive portals with **HTTPS** to ensure the secure handling of guest devices. Implement access expiration policies for guest users to limit access duration.

8. Integration with Other Security Systems

- **Firewall Integration, EDR, SIEM**
- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(c)**: Requires implementing integrated safeguards such as firewalls, intrusion detection, and other security measures to monitor and protect access to sensitive systems.
- **Key Compliance Actions:**
    - Integrate ClearPass with your **firewall** for policy enforcement, and connect with **EDR solutions** to detect compromised endpoints. Forward ClearPass logs to a **SIEM** for real-time monitoring and threat detection.

9. User Authentication Methods

- **802.1X Authentication, LDAP/AD Integration, MFA**
- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(c)**: Requires institutions to implement strong authentication methods, including **Multi-Factor Authentication (MFA)** and LDAP integration, for controlling access to sensitive systems.
- **Key Compliance Actions:**
    - Use **802.1X authentication** for strong network access control, integrating ClearPass with **LDAP** or **Active Directory** to centralize user management. Enforce **MFA** for critical network and system access.

Additional Compliance Considerations

- **Network Security Monitoring** and **Audit Trails**: **Appendix A, Part 748, Section III(C)** emphasizes the importance of monitoring and maintaining audit trails of all system access and activities. **ClearPass** logging and alerting features should be leveraged to maintain detailed logs of user activity, authentication attempts, and administrative changes.
- **Device and Endpoint Security**: **Appendix A, Part 748, Section III(B)(1)(d)** requires safeguards to prevent unauthorized access to sensitive systems. **ClearPass's NAC** policies help ensure that only compliant devices can access the network, mitigating risks from unauthorized or compromised endpoints.

Conclusion:

By implementing these **Aruba ClearPass** best practices and configurations, financial institutions can align with the regulatory requirements set forth in **12 CFR 748.0** and **Appendix A to Part 748**, ensuring secure access control, monitoring, and protection of member information. The emphasis on access control, encryption, logging, regular updates, and integration with other security systems ensures a robust security posture while meeting regulatory compliance.

Azure AD Check

Tuesday, September 17, 2024 1:23 PM

To ensure compliance with **12 CFR 748.0** and **Appendix A to Part 748, Title 12**, it's critical to verify specific configurations in **Azure Active Directory (Azure AD)**, **Azure AD Connect**, **MFA**, and **Conditional Access**. Below are the specific areas in Azure you should check to ensure that your configurations meet compliance standards and provide robust security.

1. Azure AD Connect Configuration

Location: On your on-premises server where Azure AD Connect is installed.
Areas to Check:

- **Password Hash Synchronization, Pass-through Authentication, or Federation**:
    - **Azure AD Connect Tool** > **Customize Synchronization Options**:
        - Ensure that either **Password Hash Synchronization** or **Pass-through Authentication** is configured. This ensures secure integration between on-prem and Azure AD.
        - Verify that **Federation Services** are properly configured if using AD FS.
- **Staging Mode**:
    - **Azure AD Connect Tool** > Check if **Staging Mode** is enabled. This mode allows you to test changes without affecting production environments, maintaining data integrity during updates.
- **Selective Synchronization**:
    - **Azure AD Connect Tool** > **Customize Synchronization Options**:
        - Review the **Synchronization Scope** to ensure that only necessary **Organizational Units (OUs)** and attributes are synced. This minimizes the exposure of sensitive member data.

2. Multi-Factor Authentication (MFA)

Location: Azure Portal > Azure Active Directory > Security > MFA.
Areas to Check:

- **MFA Settings**:
    - **Azure Portal** > **Azure Active Directory** > **Security** > **MFA**:
        - Ensure that **MFA** is enabled for all users accessing sensitive data or systems.
- **Conditional Access Policies for MFA**:
    - **Azure Portal** > **Azure Active Directory** > **Security** > **Conditional Access** > Check **Policies**:
        - Ensure **Conditional Access Policies** enforce MFA for specific groups, applications, and scenarios (e.g., external logins, high-risk logins).
        - Review policies enforcing MFA for administrative roles to

ensure that users with privileged access (such as **Global Admins**) are required to use MFA for added security.

3. Conditional Access

Location: Azure Portal > Azure Active Directory > Security > Conditional Access.
Areas to Check:

- **Location-Based Policies**:
    - **Azure Portal** > **Azure Active Directory** > **Security** > **Conditional Access** > Choose a policy > **Conditions** > **Locations**:
        - Ensure access is restricted to trusted locations (e.g., corporate network or VPN).
        - Deny access from high-risk or untrusted locations, preventing access from regions where your institution does not operate.
- **Device Compliance**:
    - **Azure Portal** > **Azure Active Directory** > **Security** > **Conditional Access** > Choose a policy > **Conditions** > **Device Platforms** and **Device State**:
        - Ensure only **compliant devices** (e.g., those with encryption, antivirus, or MDM-managed) can access sensitive data. This prevents unprotected devices from accessing critical systems.
- **Risk-Based Policies**:
    - **Azure Portal** > **Azure Active Directory** > **Security** > **Conditional Access** > Choose a policy > **Conditions** > **User Risk** and **Sign-in Risk**:
        - Configure **risk-based policies** to trigger additional authentication steps (such as MFA) based on sign-in risk or user risk (e.g., suspicious activity, unfamiliar IPs).
        - Use **Azure Identity Protection** to assess and act on risky sign-ins.

4. AD FS Configuration (if using AD FS)

Location: On your AD FS server.
Areas to Check:

- **SSL/TLS Configuration**:
    - **AD FS Management Console** > **Service** > **Endpoints** > Ensure that SSL/TLS settings are enabled and configured to use secure versions (TLS 1.2 or higher).
    - Ensure the use of strong **encryption algorithms** for protecting authentication tokens.
- **Token Encryption**:
    - **AD FS Management Console** > **Service** > **Certificates**:
        - Check that the certificates used for **token signing** and **encryption** are valid and up-to-date.
        - Ensure the tokens passed between AD FS and Azure AD are encrypted to prevent unauthorized access to sensitive data during authentication.
- **Auditing Configuration**:
    - **AD FS Management Console** > **Service** > **Auditing**:

        - Ensure that **auditing** is enabled for all authentication requests, token issuance, and administrative changes. This ensures that all access attempts are logged and available for review to detect unauthorized access.

5. User and Role Management in Azure AD

Location: Azure Portal > Azure Active Directory > Users & Groups.
Areas to Check:

- **Privileged Roles and Role-Based Access Control (RBAC)**:
    - **Azure Portal** > **Azure Active Directory** > **Roles and Administrators**:
        - Ensure **Role-Based Access Control (RBAC)** is enforced, restricting access to critical resources based on the user's role.
        - Regularly review **privileged roles** (e.g., **Global Admin**, **User Admin**) to ensure only authorized users are assigned elevated privileges.
        - Use **PIM (Privileged Identity Management)** to enforce just-in-time access for administrative roles, reducing the risk of unauthorized access.

6. Identity Protection and Threat Detection

Location: Azure Portal > Azure Active Directory > Security > Identity Protection.
Areas to Check:

- **User Risk and Sign-In Risk Policies**:
    - **Azure Portal** > **Azure Active Directory** > **Security** > **Identity Protection**:
        - Set up policies to detect and act on **user risk** and **sign-in risk**. This ensures that high-risk logins (e.g., from unknown devices, unfamiliar locations) trigger additional actions such as MFA or blocking access.
- **Risky Users and Sign-ins**:
    - Monitor **Risky Users** and **Risky Sign-ins** reports in **Identity Protection** to detect anomalous behavior or compromised accounts, helping prevent unauthorized access.

7. Logging and Auditing for Compliance

Location: Azure Portal > Azure Active Directory > Audit Logs & Sign-in Logs.
Areas to Check:

- **Audit Logs**:
    - **Azure Portal** > **Azure Active Directory** > **Audit Logs**:
        - Review **audit logs** regularly to track configuration changes, user management actions, and admin activities. Ensure that logs are retained and securely stored to meet compliance with audit requirements.
        - Logs should include information on password resets, role assignments, and changes to MFA settings.

- **Sign-in Logs**:
    - **Azure Portal** > **Azure Active Directory** > **Sign-in Logs**:
        - Ensure **sign-in logs** are enabled to monitor and detect suspicious sign-in activity, such as failed login attempts or logins from unknown locations. Investigate anomalies immediately to prevent unauthorized access.

Compliance Summary for Azure Configurations

All configurations mentioned above help ensure compliance with **12 CFR 748.0** and **Appendix A to Part 748, Title 12** by addressing the following key areas:

1. **Access Control**: Implementing MFA, conditional access policies, and role-based access control ensures only authorized personnel have access to sensitive systems and data.
2. **Audit Trails and Monitoring**: Enabling logging, audit logs, and sign-in logs allows for the monitoring of user activities, administrative changes, and access attempts, ensuring traceability.
3. **Encryption and Data Protection**: Ensuring that data in transit and at rest (especially authentication tokens and communications with AD FS) is encrypted protects sensitive member information.
4. **Incident Detection and Response**: Identity Protection policies, combined with real-time auditing, help detect unauthorized access attempts, enabling a timely response to incidents.

By regularly checking these specific Azure configurations, your institution can ensure compliance with regulatory requirements while securing sensitive member information and critical systems.

Local Accounts

Wednesday, September 18, 2024 12:25 PM

To enhance the security of **local accounts** and ensure compliance with **12 CFR 748.0** and **Appendix A to Part 748**, financial institutions should follow these best practices, applying the principles of least privilege, strong authentication, auditing, and secure password management. Below, I've mapped the steps to best practices for securing local accounts and added references to the applicable compliance requirements from **12 CFR 748.0** and **Appendix A to Part 748**:

1. Use Strong, Unique Passwords

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(c)**: Requires financial institutions to implement access controls that limit access to sensitive information and prevent unauthorized access.
- **Key Compliance Actions:**
    - Enforce strong password policies for all local accounts to prevent unauthorized access.
    - Use **Group Policy** to set minimum password length, complexity, and password expiration policies.
    - Avoid blank passwords and ensure all local accounts, especially administrative ones, follow strong password policies.

How to Configure via Group Policy:

- **Path:** `Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy`

2. Limit Administrator Privileges

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(2)**: Requires institutions to limit access to sensitive systems to authorized personnel.
- **Key Compliance Actions:**
    - Implement **least privilege** principles: Only grant administrative rights to users who need them for specific tasks.
    - Use standard user accounts for day-to-day operations, reserving administrative accounts for necessary tasks.

3. Disable Unused or Default Accounts

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(2)**: Prevent unauthorized access by disabling unused accounts, such as the default "Guest" account or other unassigned accounts.
- **Key Compliance Actions:**
    - Disable unused or default accounts using `net user` commands.
    - Rename the default **Administrator** account to make it harder for attackers to guess the username.

4. Enable Account Lockout Policies

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(c)**: Requires safeguards to prevent unauthorized access, such as account lockout policies that temporarily disable accounts after multiple failed login attempts.
- **Key Compliance Actions:**
    - Implement an account lockout policy that temporarily disables an account after a specified number of failed login attempts, preventing brute-force attacks.

How to Configure via Group Policy:

- **Path:** `Computer Configuration > Windows Settings > Security Settings > Account Policies > Account Lockout Policy`

5. Use Multi-Factor Authentication (MFA)

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(c)**: Stresses the need for strong authentication mechanisms.
- **Key Compliance Actions:**
    - Enable **MFA** for local administrative accounts if supported, providing an additional layer of security.

6. Use Local Group Policy to Restrict Access

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(2)**: Requires controlling access to sensitive systems to prevent unauthorized access.
- **Key Compliance Actions:**
    - Restrict which accounts can log in locally by configuring Group Policy to deny local login access to unauthorized users.

How to Configure via Group Policy:

- **Path:** `Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment > Deny log on locally`

7. Monitor and Audit Account Activity

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(C)**: Requires audit controls to track access to sensitive systems and detect suspicious activities.
- **Key Compliance Actions:**
    - Enable audit logging for all account logins (successful and failed attempts) to monitor and detect suspicious activity.
    - Regularly review security logs via **Event Viewer** or **SIEM** to identify unusual account activity.

How to Configure via Group Policy:

- **Path:** `Computer Configuration > Windows Settings > Security Settings > Advanced Audit Policy Configuration > Account Logon`

8. Remove or Disable Unnecessary Services

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(d)**: Requires institutions to implement safeguards to protect systems from unauthorized access.
- **Key Compliance Actions:**
    - Disable unnecessary local accounts or services created for specific applications. Ensure that these accounts are configured with the least privileges needed to perform their functions.

9. Implement Local Administrator Password Solution (LAPS)

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(c)**: Requires institutions to protect sensitive information and access controls.
- **Key Compliance Actions:**
    - Use **Microsoft LAPS** to manage local administrator passwords securely by rotating them regularly and storing them in **Active Directory**. This prevents the reuse of the same local admin password across multiple machines.

10. Restrict Remote Access to Local Accounts

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(2)**: Limits access to sensitive systems and prevents unauthorized remote access.
- **Key Compliance Actions:**
    - Disable remote login for local accounts to reduce the risk of unauthorized access via **Remote Desktop Services** or other remote services.

How to Configure via Group Policy:

- **Path:** `Computer Configuration > Windows Settings > Security Settings > Local Policies > User Rights Assignment > Deny log on through Remote Desktop Services`

11. Enforce User Account Control (UAC)

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(d)**: Requires institutions to implement strong access controls to protect systems from unauthorized actions.
- **Key Compliance Actions:**
    - Enable **User Account Control (UAC)** to prompt users for confirmation when administrative actions are needed, reducing the risk of unauthorized or unintentional changes to system settings.

12. Configure Secure Password Storage (Credential Guard)

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(c)**: Protects access credentials

by using secure storage mechanisms.

- **Key Compliance Actions:**
    - Enable **Windows Defender Credential Guard** to protect local account credentials from pass-the-hash attacks by preventing them from being stored in memory.

13. Use Password Vaults for Service Accounts

- **Compliance Reference:**
    - **Appendix A, Part 748, Section III(B)(1)(c)**: Prevents unauthorized access to service accounts and stored credentials.
- **Key Compliance Actions:**
    - Store credentials for service accounts in a secure **password vault** rather than embedding them in scripts or configuration files to protect them from unauthorized access or compromise.

Conclusion

Implementing these configurations ensures compliance with **12 CFR 748.0** and **Appendix A to Part 748**, which mandates strong access controls, monitoring, encryption, and auditing of local accounts. Regularly reviewing configurations, enforcing secure practices such as MFA and strong password policies, and enabling auditing will protect sensitive member information from unauthorized access and ensure financial institutions meet regulatory requirements.

system administrator credentials

Monday, September 23, 2024 4:19 PM

The use of **system administrator credentials** to browse the internet poses several significant risks and compliance issues, particularly in the context of **12 CFR 748.0** and **Appendix A to Part 748, Title 12**, which focus on safeguarding member information and maintaining robust security programs. Below are key issues related to the use of administrator credentials for internet browsing and how they conflict with these regulatory requirements:

1. Increased Risk of Unauthorized Access and Malware

- **Issue**: System administrators typically have elevated privileges, such as full access to critical systems, databases, and sensitive member information. Using these credentials to browse the internet exposes these powerful accounts to potential compromise via malware, phishing attacks, or drive-by downloads.
- **Regulatory Non-Compliance**: **12 CFR 748.0(b)** requires credit unions to implement controls that safeguard against unauthorized access to member information. Browsing the internet with admin credentials increases the attack surface, making unauthorized access more likely.
    - **Appendix A to Part 748, Title 12**, specifically **Part III(B)**, emphasizes the need for controls that protect sensitive data, including ensuring that systems are secure from external threats. Using privileged accounts for internet browsing directly increases the risk of an external compromise.

2. Violation of the Principle of Least Privilege

- **Issue**: Allowing system administrators to use their privileged accounts for everyday tasks, such as browsing the internet, violates the **principle of least privilege**. This principle dictates that accounts should only have the minimum necessary access to perform their duties.
- **Regulatory Non-Compliance**: **Appendix A to Part 748, Title 12**, **Part III(B)**, requires the implementation of appropriate access controls to safeguard member information. By permitting the use of administrator credentials for non-essential tasks, such as internet browsing, the organization fails to enforce proper access control measures. The potential for privilege escalation or credential theft is significantly increased.
    - **12 CFR 748.0(b)(3)** also requires credit unions to establish controls to regularly test key systems and minimize exposure to vulnerabilities. Using administrative credentials for internet access is a poor practice that increases exposure to potential system vulnerabilities.

3. Elevated Risk of Credential Theft and Phishing Attacks

- **Issue**: Browsing the internet with administrator credentials makes those accounts prime targets for phishing attacks. If an administrator inadvertently accesses a malicious website or falls for a phishing email, attackers can steal the administrator's credentials, granting them broad access to the network.
- **Regulatory Non-Compliance**: **Appendix A to Part 748, Title 12**, **Part III(C)**, highlights the importance of ongoing monitoring and risk mitigation for protecting sensitive data. Administrator credentials compromised through phishing could lead to widespread unauthorized access to member information, representing a failure to mitigate risks associated with credential theft.
    - **12 CFR 748.0(b)** mandates a robust security program, which should include protecting against phishing attacks. Using administrator credentials for internet browsing inherently increases the risk of credential theft through social engineering.

4. Lack of Segregation of Duties

- **Issue**: Browsing the internet using administrator credentials undermines the **segregation of duties**, where different roles within the IT environment should be separated to limit the scope of access and responsibility. Admin accounts should be used strictly for performing system administration tasks, and regular user accounts should be used for internet browsing.
- **Regulatory Non-Compliance**: **Appendix A to Part 748, Title 12**, **Part III(B)(3)**, emphasizes the need to maintain controls around access to sensitive information and systems, which includes segregating duties to prevent unnecessary access to sensitive areas.
    - This practice also violates **Appendix A's** general guideline to safeguard sensitive member information by enforcing proper role management and control over who can access critical systems.

5. Potential for Misuse of Privileged Access

- **Issue**: Browsing the internet with administrative privileges also opens up the potential for **misuse** of those privileges, whether intentional or unintentional. An administrator could inadvertently download or install malicious software that bypasses security measures due to elevated access, leading to significant security breaches.
- **Regulatory Non-Compliance**: **Appendix A to Part 748, Title 12**, **Part III(B)(2)** mandates that appropriate measures be in place to prevent unauthorized alterations or misuse of sensitive systems. Allowing internet browsing with administrator credentials increases the risk of system compromise through misuse or the accidental introduction of malware.

6. Weakness in Security Logging and Monitoring

- **Issue**: If an administrator uses their privileged credentials for browsing the internet and their account is compromised, it may be more difficult to detect unusual activity, since administrators often have access to modify or suppress logging. This can undermine the ability to monitor and audit security events effectively.
- **Regulatory Non-Compliance**: **Appendix A to Part 748, Title 12**, **Part III(C)** requires credit unions to monitor systems and controls regularly. Compromised administrator credentials can disable or alter logs, making it difficult to trace unauthorized activity. This directly affects the institution's ability to detect, report, and remediate security incidents in a timely manner.
    - **12 CFR 748.0(b)(3)** also mandates regular testing of controls, which includes ensuring that audit logs are active and protected from tampering. Compromised admin accounts undermine the integrity of this testing process.

7. Insufficient Risk Management

- **Issue**: Allowing system administrators to browse the internet with elevated credentials suggests a lack of adequate risk management practices. Browsing with privileged credentials introduces significant risks to the integrity of systems and sensitive member information.
- **Regulatory Non-Compliance**: **Appendix A to Part 748, Title 12**, **Part III(C)** requires credit unions to assess and mitigate risks as part of an effective information security program. Allowing risky behavior, such as internet browsing with admin credentials, indicates a failure to appropriately assess and mitigate risks to the security of member information.
    - **12 CFR 748.0(b)** mandates the implementation of security controls that effectively manage risk, and this includes prohibiting risky activities like using administrator accounts for general internet browsing.

Best Practices for Compliance

To comply with **12 CFR 748.0** and **Appendix A to Part 748**, Title 12, and mitigate the risks associated with using administrator credentials for internet browsing, consider the following best practices:

1. **Enforce Least Privilege Access**: Admin accounts should only be used for administrative tasks. Regular internet browsing should be done using non-administrative accounts.
2. **Implement Role-Based Access Controls (RBAC)**: Ensure proper segregation of duties and limit access to sensitive systems to only those who require it for their roles.
3. **Use Two-Factor Authentication (2FA)**: Implement 2FA for administrator accounts to add an extra layer of protection, especially for accessing sensitive systems.
4. **Restrict Internet Access for Admin Accounts**: Enforce policies that prevent administrators from using their privileged accounts to browse the internet or access external websites.
5. **Regular Vulnerability Scanning and Monitoring**: Continuously scan and monitor for any potential vulnerabilities or signs of compromise related to privileged accounts.
6. **Security Awareness Training**: Regularly train system administrators and other staff on the dangers of phishing, social engineering, and using elevated credentials improperly.

By addressing these issues and implementing strong controls, your credit union can better align with the regulatory requirements of **12 CFR 748.0** and **Appendix A to Part 748**, protecting sensitive member information from unnecessary risks.

Using system administrator credentials to browse the internet, even with Multi-Factor Authentication (MFA) in place, presents several significant risks. While MFA adds an additional layer of security, it does not eliminate the inherent dangers associated with using high-privilege accounts for everyday browsing.

Here are the primary risks:

1. Exposure to Malware and Phishing Attacks

- **Drive-by Downloads**: Even if MFA protects the authentication process, browsing the internet as a system administrator increases the risk of inadvertently downloading malware (e.g., ransomware, trojans, etc.). Attackers can exploit browser vulnerabilities or malicious websites to inject malware into the system.
- **Phishing**: MFA helps mitigate phishing attacks, but it doesn't prevent an admin from clicking on a malicious link or downloading a compromised attachment. If an administrator's account is compromised, attackers can escalate privileges and move laterally through the system, leading to catastrophic outcomes.

2. Privileged Escalation

- **Higher Privileges at Risk**: If a system admin account is compromised, the attacker gains access to the highest privileges on the network. Even with MFA, once the admin session is active and authenticated, malware that bypasses MFA (e.g., through session hijacking or man-in-the-middle attacks) can exploit the elevated privileges to make unauthorized changes, steal sensitive data, or plant backdoors.
- **Cross-Site Scripting (XSS) or Cross-Site Request Forgery (CSRF)**: These attacks can execute malicious scripts in the admin's browser and perform unauthorized actions, such as modifying system configurations or accessing critical data without needing to authenticate again.

3. Session Hijacking

- **Session Vulnerabilities**: After the MFA authentication is complete, session tokens or cookies could be hijacked by sophisticated attackers. If a privileged user's session is hijacked, an attacker can impersonate the admin and act with their privileges, bypassing the need for further MFA verification.
- **Man-in-the-Middle (MitM) Attacks**: In some cases, an attacker might intercept communications between the admin's system and the website. While MFA protects login credentials, an attacker could exploit session data or the session after it's authenticated.

4. Increased Attack Surface

- **Browsers as Vulnerable Entry Points**: Browsers are complex applications with many potential vulnerabilities. Using system administrator credentials to browse the internet increases the risk that these vulnerabilities could be exploited. Even with MFA, any vulnerability in the browser could be used to target an authenticated admin user.
- **Plug-ins or Add-ons**: Browser extensions, which can be compromised or malicious, could exploit the privileges of an admin account. If an extension is compromised, the damage done with admin privileges could be far greater than if a regular user account were compromised.

5. Lateral Movement

- **Pivoting through Network**: If malware compromises a system admin account, the attacker can use that account to move laterally across the network, accessing other systems, services, or databases that a regular user would not have access to. This can lead to a full network compromise.
- **Credential Dumping**: Once a system admin's account is compromised, attackers may extract stored credentials from memory, allowing them to use those credentials to compromise additional systems, even those protected by MFA.

6. Violation of Least Privilege Principle

- **Unnecessary Risk Exposure**: The principle of least privilege dictates that users should operate with the minimum level of access needed to perform their tasks. Browsing the internet with administrator credentials violates this principle, exposing critical systems to unnecessary risk. If internet browsing is necessary, it should be done from an account with limited privileges.

7. Insider Threat Amplification

- **Unintentional Actions**: Even if the system admin does not intend to compromise the system, unintentional actions—such as clicking on a malicious link or visiting an infected website—could introduce malware or trigger an attack. With elevated privileges, the consequences of these actions are far more severe than for a regular user.

8. Limited Effectiveness of MFA Post-Authentication

- **MFA Is Not Foolproof**: Once an admin is authenticated via MFA, their session is trusted, but attackers who compromise a session can bypass MFA protections. MFA prevents unauthorized access at login but does not prevent post-authentication threats like session hijacking, phishing, or malware that exploit active admin sessions.

Recommendations

- **Use a Non-Admin Account for Browsing**: Separate your browsing activities from your admin account by using a standard user account for everyday activities.
- **Limit Internet Access for Admin Accounts**: If possible, avoid using administrative credentials to browse the internet. Keep administrative access limited to performing essential system tasks.
- **Browser Isolation**: If internet browsing is necessary, consider using browser isolation techniques, such as virtual machines (VMs) or sandboxing, to mitigate the risk of malware.
- **Regular Monitoring and Logging**: Ensure comprehensive monitoring and logging of system administrator activities to detect unusual behavior, even after MFA authentication.

Conclusion

Although MFA greatly enhances security, it cannot fully protect against the risks posed by using system admin credentials to browse the internet. The elevated privileges of system admin accounts make them highly attractive targets, and any compromise can have severe consequences, including full system breaches or ransomware attacks. Adhering to the principle of least privilege and limiting internet access for privileged accounts is critical for maintaining a secure environment.

system administrator credentials Remediation

Monday, September 23, 2024 4:20 PM

To address the issues associated with using **system administrator credentials** for internet browsing and ensure compliance with **12 CFR 748.0** and **Appendix A to Part 748, Title 12**, it is essential to implement a series of remediation steps. These steps focus on reducing the risk to sensitive member information, improving security practices, and ensuring alignment with r egulatory requirements.

Remediation Steps

1. Enforce the Principle of Least Privilege
- **Action**: Ensure that system administrator accounts are only used for administrative tasks and are never used for everyday activities, such as browsing the internet.
- **Steps**:
  - Implement a policy that restricts administrator account usage strictly to administrative tasks.
  - Create separate, non-administrative accounts for system administrators to use for routine tasks, such as email and internet browsing.
- **Benefit**: Reduces the risk of privileged credentials being exposed to malicious websites or phishing attacks and ensures compliance with **Appendix A, Part III(B)**.

2. Restrict Internet Access for Admin Accounts
- **Action**: Block access to the internet from accounts with elevated privileges (admin accounts).
- **Steps**:
  - Implement firewall or proxy rules that block internet access for administrator accounts.
  - Use group policies or endpoint security tools to restrict web browser usage for accounts with administrative privileges.
- **Benefit**: Minimizes the exposure of admin accounts to online threats, helping to protect sensitive member data in compliance with **12 CFR 748.0(b)** and **Appendix A**.

3. Implement Role-Based Access Control (RBAC)
- **Action**: Apply **Role-Based Access Control (RBAC)** to ensure that users, including system administrators, only have access to the resources and systems required for their specific roles.
- **Steps**:
  - Define roles with specific privileges based on job responsibilities.
  - Use RBAC tools and policies to limit the scope of administrative privileges, ensuring that users only access what is necessar y.
- **Benefit**: Enforces better access controls, ensuring compliance with **Appendix A, Part III(B)(3)**, which emphasizes the need for secure access controls.

4. Implement Multi-Factor Authentication (MFA)
- **Action**: Enable **Multi-Factor Authentication (MFA)** for all privileged accounts to add an extra layer of security.
- **Steps**:
  - Require system administrators to use MFA when accessing systems with elevated privileges.
  - Use MFA solutions that combine something the user knows (password) with something the user has (security token or mobile auth entication app).
- **Benefit**: Provides additional protection for admin credentials, reducing the risk of credential theft. This aligns with **Appendix A, Part III(B)**, which requires strong controls to protect member information.

5. Implement Credentialed Vulnerability Scanning
- **Action**: Conduct **credentialed vulnerability scans** to identify security weaknesses, including those related to admin accounts.
- **Steps**:
  - Use automated vulnerability scanning tools that perform credentialed scans to assess the security of systems and administrati ve access.
  - Schedule regular scans and ensure they test for weak or misused credentials, identifying vulnerabilities related to privilege d access.
- **Benefit**: Helps ensure systems and administrative accounts are not exposed to unnecessary risks, as required by **Appendix A, Part III(C)**.

6. Regularly Review and Rotate Admin Credentials
- **Action**: Periodically review and rotate administrator credentials to reduce the risk of compromised credentials.
- **Steps**:
  - Implement a policy to rotate admin passwords regularly, especially after personnel changes or security incidents.
  - Use a **Privileged Access Management (PAM)** system to store and manage admin passwords securely and ensure they are rotated automatically.
- **Benefit**: Reduces the risk of long-standing credential exposure and ensures that credentials are well protected, in line with **12 CFR 748.0(b)(3)** and **Appendix A**.

7. Segregate Administrative and User Accounts
- **Action**: Ensure that all system administrators use separate user accounts for routine, non-administrative tasks.
- **Steps**:
  - Create distinct accounts for administrators to use when performing everyday tasks, such as accessing the internet or email.
  - Enforce policies that require administrators to log in to their privileged accounts only when necessary for system administra tion tasks.
- **Benefit**: Prevents the misuse of admin accounts for tasks that could expose them to unnecessary risk, supporting **Appendix A, Part III(B)(2)** by enforcing proper controls for data protection.

8. Implement Continuous Monitoring and Logging
- **Action**: Continuously monitor the use of privileged accounts and log all administrative activities to detect and respond to potential misuse or attacks.
- **Steps**:
  - Enable comprehensive logging of all activities performed by admin accounts, including attempts to access the internet, instal l software, or change configurations.
  - Use a **Security Information and Event Management (SIEM)** tool to analyze logs and generate alerts for suspicious activity, such as unusual internet usage by admin accounts.
- **Benefit**: Helps detect and respond to potential security incidents involving admin accounts, supporting **Appendix A, Part III(C)** for risk monitoring and mitigation.

9. Educate Administrators on Security Best Practices
- **Action**: Provide regular training to system administrators on secure use of privileged credentials and the risks of internet browsing with admin accounts.
- **Steps**:
  - Conduct periodic security awareness training that focuses on the risks of using admin credentials for internet browsing and o ther non-essential tasks.
  - Ensure administrators are aware of policies and best practices regarding the use of admin accounts and the importance of keep ing their credentials secure.
- **Benefit**: Reduces the likelihood of human error leading to compromised admin accounts, ensuring alignment with **Appendix A's** guidelines on protecting member data and ensuring staff are trained in security practices.

10. Implement Web Content Filtering
- **Action**: Use web content filtering to restrict access to risky or non-business-related websites, even for non-admin users.
- **Steps**:
  - Implement a **Web Application Firewall (WAF)** or other web content filtering technologies to block access to malicious or high -risk websites.
  - Create policies that limit access to websites that are not necessary for business operations, regardless of user roles.
- **Benefit**: Adds an extra layer of protection against online threats, reducing the risk of malware infection or phishing, and ensuring compliance with **Appendix A, Part III(B)(2)**.

11. Conduct Regular Internal Audits of Privileged Access
- **Action**: Perform regular internal audits of all privileged accounts to ensure that policies are being followed and that administrator accounts are not used for internet browsing or other unauthorized activities.
- **Steps**:
  - Schedule audits to review the activities of administrator accounts, including verifying adherence to access control policies.
  - Ensure that audit logs include detailed records of all administrative actions and that these logs are reviewed regularly for signs of misuse.
- **Benefit**: Helps ensure compliance with **12 CFR 748.0** and **Appendix A** by providing ongoing monitoring and validation that controls are being followed.

12. Use Privileged Access Management (PAM) Solutions
- **Action**: Implement a **Privileged Access Management (PAM)** solution to tightly control, monitor, and audit all access to privileged accounts.
- **Steps**:
  - Deploy a PAM solution to centralize the management of privileged accounts, requiring additional authentication steps for admi n access.
  - Use the PAM solution to limit the duration of administrative access sessions and automatically log out administrators after c ompleting their tasks.
- **Benefit**: Provides a robust security framework for managing and controlling privileged access, ensuring compliance with **Appendix A, Part III(B)** and **Part III(C)**.

Summary of Remediation Steps
1. **Enforce least privilege** by ensuring admin accounts are used only for administrative tasks.
2. **Restrict internet access** for admin accounts using firewalls, proxies, or group policies.
3. **Apply RBAC** to enforce the correct access levels based on job roles.
4. **Use MFA** for all privileged accounts to strengthen authentication.
5. **Conduct regular vulnerability scans** and review administrative privileges.

6. **Rotate admin credentials** periodically to reduce the risk of exposure.
7. **Segregate user and admin accounts** to avoid unnecessary risk.
8. **Implement continuous monitoring and logging** for administrative activities.
9. **Educate administrators** on the security risks associated with internet browsing.
10. **Use web filtering** to prevent access to risky websites.
11. **Conduct internal audits** to ensure compliance with access controls.
12. **Deploy PAM solutions** for managing privileged access securely.

By implementing these steps, the organization can mitigate the risks associated with using system administrator credentials f or internet browsing and ensure compliance with **12 CFR 748.0** and **Appendix A to Part 748, Title 12**.

domain controllers (DCs)

Monday, September 23, 2024 4:31 PM

Allowing **domain controllers** (DCs) to connect to the internet presents significant security risks and compliance issues, particularly in the context of **12 CFR 748.0** and **Appendix A to Part 748, Title 12**. These regulations emphasize the importance of safeguarding member information, maintaining robust security controls, and mitigating risks to sensitive systems and data. Below are the primary issues associated with domain controllers that have internet connectivity, along with how they conflict with regulatory requirements.

Key Issues with Domain Controllers Connecting to the Internet

1. Increased Attack Surface for Critical Infrastructure

- **Issue**: Domain controllers are the heart of an organization's identity and access management system, containing sensitive information such as user accounts, credentials, and security policies. Allowing a DC to connect to the internet increases its exposure to external threats like malware, phishing, and direct hacking attempts.
- **Regulatory Non-Compliance**:
  - **12 CFR 748.0(b)** requires the implementation of controls that safeguard against unauthorized access to member information. A domain controller with internet access is highly vulnerable to attacks, increasing the risk of credential theft and unauthorized access to systems and data.
  - **Appendix A to Part 748, Title 12**, **Part III(B)** emphasizes the need for controls that prevent unauthorized access to sensitive data. Domain controllers should be isolated from the internet to reduce exposure to external threats.

2. Exposure to Malware, Ransomware, and Other Cyber Threats

- **Issue**: Allowing a domain controller to connect to the internet increases the risk of it being infected with malware, ransomware, or other types of cyber threats. Since a domain controller has elevated privileges across the network, a successful malware attack could lead to widespread damage, including the compromise of member information.
- **Regulatory Non-Compliance**:
  - **Appendix A to Part 748, Title 12**, **Part III(C)** requires credit unions to implement effective risk mitigation strategies, including protecting systems from malware and other threats. Allowing internet access to a domain controller increases the risk of compromise, which could jeopardize the integrity of member data.
  - **12 CFR 748.0(b)(3)** mandates the regular testing and safeguarding of critical systems. By exposing domain controllers to internet threats, the credit union may fail to protect the core infrastructure that controls access to sensitive systems.

3. Elevated Risk of Credential Theft

- **Issue**: Domain controllers are responsible for managing user authentication and access control. If a domain controller is compromised through an internet-based attack, attackers can steal highly sensitive information, including administrator and user credentials. This could lead to unauthorized access to systems containing member information.
- **Regulatory Non-Compliance**:
  - **Appendix A to Part 748, Title 12**, **Part III(B)** requires adequate access controls to protect sensitive information. Exposing domain controllers to the internet heightens the risk of credential theft, which could result in unauthorized access to member data and systems.
  - **12 CFR 748.0(b)** emphasizes the need to protect member data from unauthorized access. If an attacker gains control of a domain controller, they could escalate privileges across the network, putting member information at risk.

4. Failure to Enforce Network Segmentation and Isolation

- **Issue**: Best practices for securing domain controllers include isolating them from less secure parts of the network and preventing them from having direct internet access. Failure to properly segment and isolate domain controllers increases the risk that internet-based threats can affect core systems.
- **Regulatory Non-Compliance**:
  - **Appendix A to Part 748, Title 12**, **Part III(B)** highlights the need for layered security and network segmentation to protect critical systems. Allowing domain controllers to connect to the internet undermines this principle by directly exposing essential network infrastructure to external risks.
  - **12 CFR 748.0(b)** requires that security controls be implemented to prevent unauthorized access to sensitive information, including through proper network isolation.

5. Potential for Data Breach or Unauthorized Data Access

- **Issue**: Domain controllers typically hold or manage access to vast amounts of sensitive information, including member data, employee information, and security policies. By allowing a domain controller to connect to the internet, there is an increased risk of a data breach through malicious exploitation or data exfiltration.
- **Regulatory Non-Compliance**:
  - **12 CFR 748.0(b)** mandates that credit unions develop and maintain controls that prevent unauthorized access or alteration of member information. A domain controller that can access the internet increases the likelihood of such data being compromised, leading to non-compliance.
  - **Appendix A to Part 748, Title 12**, **Part III(C)** stresses the importance of preventing and responding to data breaches. Exposing domain controllers to the internet opens up more avenues for a data breach, making it harder to maintain compliance with this requirement.

6. Compromised Security Monitoring and Logging

- **Issue**: Internet access on domain controllers can potentially disrupt security monitoring and logging mechanisms. An attacker who gains access through an internet connection might disable or manipulate logs, making it difficult to detect and respond to incidents involving member data.
- **Regulatory Non-Compliance**:
  - **Appendix A to Part 748, Title 12**, **Part III(C)** requires continuous monitoring and reporting of security incidents. If domain controllers are connected to the internet, they may be more vulnerable to tampering with logs or disabling security monitoring, reducing the effectiveness of incident response systems.
  - **12 CFR 748.0(b)(3)** requires regular testing of systems and controls, which can be compromised if security monitoring on a domain controller is disabled through a remote attack.

7. Difficulty in Patch Management and Security Updates

- **Issue**: While domain controllers require regular updates and patches, connecting them to the internet for this purpose introduces significant risks. Using a direct internet connection for patching increases the risk of the domain controller being exploited during the patching process or by interacting with malicious sources.
- **Regulatory Non-Compliance**:
  - **Appendix A to Part 748, Title 12**, **Part III(B)(3)** mandates proper system maintenance, including timely patching. However, exposing domain controllers to the internet for the sake of patching creates additional vulnerabilities. Secure patch management procedures that don't involve direct internet access should be used.
  - **12 CFR 748.0(b)(3)** emphasizes secure testing and maintenance of systems. Using the internet to patch domain controllers contradicts the goal of minimizing the system's exposure to security threats.

8. Potential for Denial of Service (DoS) Attacks

- **Issue**: If domain controllers are connected to the internet, they are vulnerable to distributed denial of service (DDoS) or other types of denial of service (DoS) attacks. These attacks can incapacitate the domain controller, leading to widespread network disruption and potentially exposing member information to risk if security systems fail.
- **Regulatory Non-Compliance**:
  - **Appendix A to Part 748, Title 12**, **Part III(B)(2)** requires that systems handling sensitive information be protected from service disruptions. Domain controllers exposed to the internet are vulnerable to DoS attacks, potentially disrupting the services that protect member data.
  - **12 CFR 748.0(b)** mandates the protection of critical systems. A compromised domain controller can lead to widespread network outages, leaving other systems exposed.

Best Practices to Mitigate Domain Controller Risks

To ensure compliance with **12 CFR 748.0** and **Appendix A to Part 748**, credit unions should follow these best practices for securing domain controllers:

1. **Remove Internet Access**: Domain controllers should never have direct internet access. They should be isolated from the public internet to prevent exposure to external threats.
2. **Implement Network Segmentation**: Isolate domain controllers in a highly secured network segment that is separate from less secure network components and restrict access to only necessary internal systems.

3. **Use Secure Patching Methods**: Patch domain controllers using internal update mechanisms or through secure, dedicated update servers, such as a WSUS (Wind ows Server Update Services) or through a jump server that is protected by robust security controls.
4. **Enable Logging and Monitoring**: Ensure robust logging and monitoring are in place, and monitor all domain controller activities closely. Logs should be reg ularly reviewed, and tamper-proof logging mechanisms should be enforced.
5. **Multi-Factor Authentication (MFA)**: Enforce MFA for all privileged access to domain controllers, ensuring that even if credentials are compromised, additional layers of security are required to gain access.
6. **Regular Vulnerability Assessments**: Conduct regular vulnerability assessments and penetration testing on domain controllers to identify and address potential s ecurity weaknesses.
7. **Implement Access Control Policies**: Restrict access to domain controllers to only trusted personnel, and enforce strict access control policies to prevent unau thorized access.

By implementing these remediation steps, a credit union can ensure compliance with **12 CFR 748.0** and **Appendix A to Part 748**, reducing the risk of unauthorized access, data breaches, and other security incidents associated with domain controllers.

DC Remediation

Monday, September 23, 2024 4:32 PM

Remediation steps for addressing the issues associated with **domain controllers (DCs) that can connect to the internet** involve a combination of security practices and compliance strategies designed to protect sensitive systems and data. These steps ensure compliance with **12 CFR 748.0** and **Appendix A to Part 748, Title 12**, which focus on safeguarding member information and maintaining strong information security programs. Below are the specific remediation actions to be taken:

1. Remove Internet Access for Domain Controllers

- **Action**: Disconnect domain controllers from the internet to prevent external exposure and reduce the risk of attacks.
- **Steps**:
  - Implement network firewall rules to block domain controllers from accessing external networks, including the internet.
  - Use access control lists (ACLs) to restrict traffic between domain controllers and the public internet.
  - Ensure that only internal, secured systems can communicate with the domain controllers.
- **Benefit**: Eliminates the attack surface presented by internet-connected domain controllers, reducing the risk of external compromise in line with **12 CFR 748.0(b)** and **Appendix A, Part III(B)**.

2. Implement Network Segmentation and Isolation

- **Action**: Segregate domain controllers from other parts of the network, isolating them from less secure areas and ensuring that they only communicate with necessary internal systems.
- **Steps**:
  - Place domain controllers in a dedicated, highly secure network segment (e.g., VLAN or subnet).
  - Restrict communication between the domain controller segment and other parts of the network using firewalls or internal segmentation.
  - Use a **demilitarized zone (DMZ)** for internet-facing services to prevent direct access to domain controllers from the internet.
- **Benefit**: Isolating domain controllers ensures they are protected from external threats and reduces lateral movement in the event of a breach. This supports **Appendix A, Part III(B)**'s requirement for strong access controls.

3. Use Secure Patch Management for Domain Controllers

- **Action**: Establish a secure patching and update process for domain controllers that does not require internet connectivity.
- **Steps**:
  - Use **Windows Server Update Services (WSUS)** or a similar internal patch management system to distribute updates to domain controllers.
  - Create a dedicated and secured **jump server** or **bastion host** to apply patches and manage domain controllers without exposing them to the internet.
  - Ensure all patches are tested in a controlled environment before deployment to domain controllers to minimize risk.
- **Benefit**: Maintains system security through regular updates without exposing domain controllers to internet-based threats, aligning with **Appendix A, Part III(B)(3)** requirements for secure system maintenance.

4. Strengthen Access Controls and Role-Based Access Control (RBAC)

- **Action**: Implement strict access controls that limit who can manage and access domain controllers.
- **Steps**:
  - Apply **Role-Based Access Control (RBAC)** to ensure only authorized administrators can access domain controllers.
  - Use **Privileged Access Management (PAM)** solutions to control and monitor access to domain controllers, ensuring that admin credentials are only used for necessary tasks.
  - Implement **multi-factor authentication (MFA)** for all privileged access to domain controllers to prevent unauthorized access, even if credentials are compromised.
- **Benefit**: Ensures that only authorized users can access domain controllers and that access is monitored and controlled, helping meet **Appendix A, Part III(B)** and **12 CFR 748.0(b)** access control requirements.

5. Implement Continuous Monitoring and Logging

- **Action**: Set up continuous monitoring and detailed logging for all domain controller activities to detect and respond to suspicious activity.
- **Steps**:
  - Enable comprehensive logging of all actions on domain controllers, including logins, failed access attempts, configuration changes, and authentication events.
  - Use a **Security Information and Event Management (SIEM)** system to collect, analyze, and alert on security events and anomalies related to domain controller activity.
  - Regularly review logs to detect any signs of unauthorized access or unusual activity.
- **Benefit**: Provides visibility into domain controller operations, helping to detect and mitigate threats in real-time and ensuring compliance with **Appendix A, Part III(C)** for ongoing monitoring and risk assessment.

6. Use Credentialed Vulnerability Scanning

- **Action**: Regularly perform **credentialed vulnerability scans** of domain controllers to identify potential security weaknesses and vulnerabilities.
- **Steps**:
  - Use a vulnerability management tool to run authenticated scans on domain controllers to assess their security posture.
  - Schedule regular scans to ensure that domain controllers are free from known vulnerabilities and misconfigurations.
  - Prioritize remediation of any vulnerabilities identified in the scans, particularly those affecting authentication or access control.
- **Benefit**: Ensures that domain controllers are regularly assessed for vulnerabilities and that any identified issues are addressed promptly, supporting **Appendix A, Part III(C)**.

7. Strengthen Firewall and Network Security Controls

- **Action**: Implement and configure firewalls and network security controls to restrict traffic to and from domain controllers.
- **Steps**:
  - Configure firewalls to allow only essential traffic to domain controllers (e.g., internal DNS, LDAP, authentication requests).
  - Use **intrusion prevention systems (IPS)** and **intrusion detection systems (IDS)** to monitor network traffic directed at domain controllers and detect any potential threats.
  - Enforce a **zero-trust network architecture**, where each request to access the domain controller is authenticated, validated, and authorized.
- **Benefit**: Reduces the risk of unauthorized network access to domain controllers and mitigates the potential for external attacks, aligning with **Appendix A, Part III(B)(2)**.

8. Disable Unnecessary Services and Ports

- **Action**: Disable any unnecessary services and close unused ports on domain controllers to minimize the attack surface.
- **Steps**:
  - Conduct a review of all services running on domain controllers and disable any that are not essential to their operation (e.g., internet-facing services like web servers or file-sharing protocols).
  - Use network security tools to identify open ports and restrict access to only those required for essential services.
  - Regularly audit services and ports to ensure that only necessary ones are running.
- **Benefit**: Minimizes the risk of exploitation through unused or unnecessary services, ensuring domain controllers remain secure as required by **Appendix A, Part III(B)(2)**.

9. Conduct Regular Security Audits and Penetration Testing

- **Action**: Regularly audit domain controller security configurations and conduct penetration testing to ensure their defenses are adequate.
- **Steps**:
  - Perform internal audits of domain controller configurations, security policies, and network settings to ensure compliance with security standards.
  - Engage third-party penetration testers to simulate attacks on domain controllers, testing their resilience to external threats.

    - Remediate any findings from the audits or penetration tests to ensure continued security.
- **Benefit**: Regular security assessments help ensure that domain controllers remain secure and compliant with **Appendix A, Part III(C)** and **12 CFR 748.0(b)(3)**.

10. Educate and Train Administrators on Best Practices
- **Action**: Provide security training to administrators responsible for managing domain controllers to ensure they follow best practices.
- **Steps**:
    - Offer regular training sessions on domain controller security, focusing on topics like secure access control, patch management, and internet restrictions.
    - Ensure administrators are familiar with compliance requirements under **12 CFR 748.0** and **Appendix A**.
    - Incorporate phishing awareness and security hygiene into the training program to prevent social engineering attacks targeting admin credentials.
- **Benefit**: Ensures that administrators are well-equipped to manage domain controllers securely, minimizing the risk of human error and enhancing compliance with **Appendix A, Part III(B)(3)**.

11. Implement Incident Response Procedures
- **Action**: Establish and document incident response procedures specific to domain controller security incidents.
- **Steps**:
    - Develop incident response playbooks for potential domain controller security incidents (e.g., unauthorized access, malware infection, DDoS attacks).
    - Test incident response procedures regularly through tabletop exercises and real-world simulations.
    - Ensure that incidents involving domain controllers are logged and reported in accordance with regulatory requirements.
- **Benefit**: Helps ensure swift and effective responses to security incidents, aligning with **Appendix A, Part III(C)**'s emphasis on timely detection and response.

Summary of Remediation Steps
1. **Remove Internet Access** for domain controllers to eliminate external exposure.
2. **Implement Network Segmentation** to isolate domain controllers from other systems.
3. **Use Secure Patch Management** practices without relying on internet connectivity.
4. **Strengthen Access Controls** by enforcing RBAC and using MFA for privileged accounts.
5. **Enable Continuous Monitoring** and logging to detect suspicious activity on domain controllers.
6. **Perform Credentialed Vulnerability Scans** to identify and mitigate security risks.
7. **Enhance Firewall Rules** and network security to restrict traffic to domain controllers.
8. **Disable Unnecessary Services** and close unused ports to minimize the attack surface.
9. **Conduct Security Audits and Penetration Testing** to assess domain controller security.
10. **Train Administrators** on best practices for managing domain controllers securely.
11. **Establish Incident Response Plans** specific to domain controller security breaches.

By implementing these remediation steps, credit unions can ensure compliance with **12 CFR 748.0** and **Appendix A to Part 748, Title 12**, reducing the risk of unauthorized access, data breaches, and other security incidents associated with domain controllers connected to the internet.

Comments

Thursday, September 26, 2024 2:46 PM

1. Document Review

- **Finding**: "The credit union's security policies, including Access Control Policies, are up to date and explicitly outline requirements for password management, multi-factor authentication (MFA), account management, and access control. The policies are aligned with industry best practices (e.g., NIST SP 800-53, ISO 27001) and have been approved by senior management, ensuring compliance with 12 CFR 748.0(b) and Appendix A to Part 748, Section III(A)."

2. System Configuration Audit

- **Finding**: "System settings, including password complexity and MFA enforcement, are aligned with documented policies. Periodic audits confirm that passwords meet complexity requirements, and MFA is enabled for high-risk systems. Inactive user accounts are automatically disabled after 30 days of inactivity, ensuring compliance with Appendix A to Part 748, Section III(B)(1)(c) and Section III(B)(2)."

3. Access Control Review

- **Finding**: "Regular user access reviews are conducted, ensuring that only authorized personnel have access to sensitive information. Administrative privileges are restricted to dedicated accounts, and service accounts are properly inventoried and managed. These practices align with the access control requirements of Appendix A to Part 748, Section III(B)(2)."

4. Physical and Environmental Controls Verification

- **Finding**: "Physical access controls, such as access cards and biometric scanners, are in place and effectively limit access to secure areas. Environmental controls, including climate control and fire suppression systems, are functioning as required, meeting the physical security requirements of Appendix A to Part 748, Section III(B)(1)(d)."

5. Remote Access Controls Verification

- **Finding**: "Remote access is secured with encryption (via VPN) and requires MFA for all users accessing critical systems. Mobile Device Management (MDM) is implemented to secure personal devices, and vendor access is restricted and monitored. These controls meet the requirements of Appendix A to Part 748, Section III(B)(1)(c) and Section III(B)(2)."

6. Role-Based Access Control (RBAC) Review

- **Finding**: "Role-based access controls (RBAC) are implemented, and regular reviews ensure that roles and access rights reflect the current organizational structure and risk profile. This ensures compliance with Appendix A to Part 748, Section III(B)(2), which requires periodic updates to access rights based on risk."

7. Compliance Verification

- **Finding**: "Procedures for securing the virtual environment and managing network access control software are consistently followed and documented. Formal access provisioning processes are in place and reviewed regularly, ensuring that access is granted or removed promptly upon hire, role changes, or terminations, in compliance with Appendix A to Part 748, Section III(A) and Section III(B)(1)(c)."

8. Reporting and Documentation

- **Finding**: "A comprehensive validation report has been compiled, documenting the

compliance status for each access control statement. Discrepancies are tracked, and remediation plans are in place to address any issues. All findings, policies, and audit results are retained and well-documented, meeting the documentation requirements of Appendix A to Part 748, Section II."

Summary of Positive Findings

- **Well-Documented Policies**: The credit union has up-to-date, management-approved security policies that align with regulatory requirements and industry best practices.
- **Regular Access Reviews**: Periodic access reviews ensure that only authorized users can access sensitive systems, and administrative privileges are restricted.
- **Strong System Configurations**: Password policies, MFA enforcement, and inactive account management are configured properly, aligning with security policies.
- **Physical and Remote Access Controls**: Physical access controls are effective, and remote access is secured with encryption, MFA, and MDM solutions.
- **Comprehensive Reporting and Remediation**: Regular audits and validation reports are conducted and documented, ensuring that the credit union remains compliant with regulatory standards.

Questionnaire

Tuesday, October 8, 2024 6:36 AM

Access Control Questionnaire

Section 1: Document Review

- **Questions**:
    1. Do you have up-to-date Information Security Policies, Access Control Policies, and System Configuration Guides?
    2. Do your documented policies explicitly cover the following areas?
        - Password management requirements
        - Multi-factor authentication (MFA) usage
        - Account management processes (creation, modification, termination)
        - Access control mechanisms
    3. Are your policies aligned with industry standards such as **NIST SP 800-53** or **ISO 27001**?
    4. Have all policies been reviewed and approved by senior management or the board of directors, as required by **12 CFR 748.0(b)**?
    5. How often are these policies reviewed and updated? (Annually/Biannually/Other)
    6. Is there an audit trail documenting when each policy was last reviewed or updated?

Section 2: System Configuration Audit

- **Questions**:
    1. Are system configurations set up to enforce password complexity requirements such as minimum length, mix of characters, and expiration periods?
    2. Is MFA enabled for users accessing high-risk systems and applications?
    3. Are user accounts automatically disabled after a period of inactivity (e.g., 30 days)?
    4. How are inactive accounts monitored and reviewed for compliance with deactivation policies?
    5. Are periodic audits conducted to verify the system's compliance with these settings and policies? (Please describe the audit frequency)
    6. Are system logs reviewed regularly to confirm that password policies and MFA settings are enforced correctly?

Section 3: Access Control Review

- **Questions**:
    1. How often are user access reviews conducted to ensure that only authorized personnel have access to sensitive information? (Monthly/Quarterly/Annually)
    2. Is access control centralized (e.g., through Active Directory or similar systems) to ensure consistent access management?
    3. Are administrative privileges limited to dedicated accounts, and is there a monitoring system in place to review their activity?
    4. Are service accounts accurately inventoried and managed with restrictions based on their intended use? (Please describe your process)
    5. What is the procedure for deactivating user accounts upon employee termination or role change? Is this process documented? (Please provide a copy of the process)
    6. How often are service account privileges reviewed to ensure they remain necessary and secure? (Monthly/Quarterly/Annually)

Section 4: Physical and Environmental Controls Verification

- **Questions**:
    1. What physical access controls are in place (e.g., access cards, biometric scanners, surveillance systems) to protect sensitive areas? (Please provide details)
    2. Are physical access logs reviewed periodically to detect any unauthorized attempts? (How often?)
    3. What environmental controls (e.g., climate control, fire suppression systems) are in place to protect physical infrastructure housing sensitive information? (Please provide details)
    4. How often are physical and environmental controls tested to ensure their effectiveness? (Monthly/Quarterly/Annually)
    5. Are there documented procedures outlining physical security measures and environmental controls? (Please provide copies)

Section 5: Remote Access Controls Verification

- **Questions**:
    1. Is remote access to your system secured with VPN encryption and is MFA required for all remote users?
    2. Do you have a Mobile Device Management (MDM) solution in place for personal devices accessing the network? (Please describe the MDM solution used)
    3. Are remote access logs monitored for anomalies and suspicious activity? (Please describe the monitoring process)
    4. Is vendor access restricted and monitored? Are vendor accounts disabled when not in use, and is account sharing prohibited? (Please provide supporting documentation)
    5. Is there a documented policy outlining procedures for remote access, including employee and vendor access? (Please provide a copy of the policy)

Section 6: Role-Based Access Control (RBAC) Review

- **Questions**:
    1. Are RBAC settings accurately configured to match your current organizational structure?
    2. How often are role definitions reviewed and updated based on organizational or risk changes? (Quarterly/Annually/Other)
    3. Is there a formal process for reviewing and updating access levels based on periodic risk assessments? (Please provide details)
    4. Are users only assigned roles necessary for their job functions? (Please provide evidence or examples)
    5. Are privileged roles separated from regular user roles, and is access to these roles monitored for anomalies?

Section 7: Compliance Verification

- **Questions**:
    1. Are procedures for securing virtual environments documented and consistently followed? (Please provide documentation)
    2. Is network access control software in place, and is it configured correctly according to your policies? (Please describe the software used)
    3. Are there formal processes for granting and revoking access when employees are hired, change roles, or are terminated? (Please provide process documentation)
    4. Are access logs periodically reviewed to verify adherence to access control policies? (How often?)
    5. Are tests conducted periodically to verify the effectiveness of access control procedures, and are these tests documented? (Please provide documentation of recent tests)

Section 8: Reporting and Documentation

- **Questions**:
    1. Is there a process for compiling a compliance validation report summarizing compliance status for each access control measure? (Please describe the process)
    2. Are discrepancies or areas needing improvement identified, and are recommendations for remediation included in the report? (Please provide a sample report if available)
    3. Is there a tracking mechanism to monitor progress on remediation actions identified during audits or validations? (Please provide details)
    4. Are records of findings, policies, and audit results maintained and retained for future reference? (How long are these records retained?)
    5. Are validation reports reviewed and approved by senior management or the board of directors? (Please provide evidence of approval)

Instructions for Completion

- **Supporting Documents**: Please provide all relevant supporting documents such as policies, system configuration guides, access logs, audit reports, and approval records.

Compliance Gaps Identified

Thursday, October 10, 2024 3:13 PM

1. Lack of Multifactor Authentication (MFA)

- **Regulation Impacted**: **Appendix A, Section III(C)** (Controls for Access Restriction and Authentication).
- **Gap**: If the credit union does not use MFA, it is non-compliant with the requirement for secure authentication mechanisms to restrict system access to authorized users.
- **Remediation**: Implement MFA solutions for all systems, especially those accessing sensitive member information.

2. Inadequate Review and Approval for Access Requests

- **Regulation Impacted**: **Appendix A, Section III(C)** (Access Controls and Authorization Measures).
- **Gap**: If access requests are not formally reviewed and approved before granting system access, there is a risk of unauthorized access.
- **Remediation**: Establish an automated workflow that requires multi-level approval for access requests, including documentation of the approval process.

3. Inconsistent User Role and Permission Reviews

- **Regulation Impacted**: **Appendix A, Section III(C)** (Access Controls and Authorization Measures).
- **Gap**: If user roles and permissions are not reviewed periodically (monthly/quarterly/annually), there is a risk that users have excessive privileges, violating the principle of least privilege.
- **Remediation**: Implement regular audits of user roles and permissions to ensure they align with job functions and regulatory requirements.

4. Absence of Role-Based Access Control (RBAC)

- **Regulation Impacted**: **Appendix A, Section III(C)** (Access Controls and Authorization Measures).
- **Gap**: If RBAC or a similar mechanism is not used, system access may not be adequately restricted based on job function or need-to-know principles.
- **Remediation**: Deploy RBAC systems that assign access based on user roles, ensuring compliance with least privilege and need-to-know principles.

5. No Documentation or Monitoring of Information Flow Controls

- **Regulation Impacted**: **Appendix A, Section III(C)** (Controls for Safeguarding Information).
- **Gap**: If information flow controls are not documented or monitored (e.g., firewall configurations, encryption use), the credit union cannot ensure that sensitive information is adequately protected in transit.
- **Remediation**: Document all information flow controls and implement monitoring tools (e.g., IDS/IPS) to ensure compliance and respond to potential breaches.

6. Lack of Separation of Duties (SoD)

- **Regulation Impacted**: **Appendix A, Section III(C)** (Controls for Separation of Duties).
- **Gap**: If there is no clear separation of duties (e.g., system administrators also performing audit functions), the credit union risks conflicts of interest and potential abuse of privileges.
- **Remediation**: Define and implement clear roles and responsibilities to separate critical functions like system administration and audit.

7. Inadequate Logging and Monitoring of Privileged Accounts

- **Regulation Impacted**: **Appendix A, Section III(C)** (Access Control and Monitoring).
- **Gap**: If privileged accounts are not logged and monitored, unauthorized use of these accounts may go undetected.
- **Remediation**: Implement monitoring tools and review logs regularly to track privileged account usage and detect anomalies.

8. Failure to Lock Accounts After Unsuccessful Logon Attempts

- **Regulation Impacted**: **Appendix A, Section III(C)** (Access Control and Security).
- **Gap**: If the system does not lock accounts after a predefined number of unsuccessful logon attempts, it could be vulnerable to brute-force attacks.
- **Remediation**: Configure systems to enforce account lockouts after a set number of failed login attempts and implement a lockout period.

9. Missing or Inconsistent Login Privacy and Security Notices

- **Regulation Impacted**: **Appendix A, Section III(B)** (Member Notice and Privacy Policy Requirements).
- **Gap**: If login banners or security notices are missing or inconsistent, users may not be aware of the terms and conditions governing their access, which is a regulatory requirement.
- **Remediation**: Update and standardize login banners to include privacy and security notices, ensuring they are consistent with policies and regulations.

10. No Automatic Session Termination or Locking Mechanisms

- **Regulation Impacted**: **Appendix A, Section III(C)** (Session Control Measures).
- **Gap**: If user sessions are not configured to terminate automatically after a period of inactivity, there is a risk of unauthorized access if a user leaves their session unattended.
- **Remediation**: Configure systems to automatically lock or terminate user sessions based on inactivity or pre-defined conditions.

11. Inadequate Monitoring of Remote Access

- **Regulation Impacted**: **Appendix A, Section III(C)** (Monitoring and Control of Remote Access).
- **Gap**: If remote access is not adequately monitored, the credit union may be unaware of unauthorized or suspicious remote activity.
- **Remediation**: Implement network monitoring solutions (e.g., IDS/IPS) and VPN logging to track remote access attempts and respond to incidents promptly.

12. No Encryption of Remote and Mobile Device Sessions

- **Regulation Impacted**: **Appendix A, Section III(C)** (Encryption and Mobile Device Security).
- **Gap**: If remote access sessions or mobile devices do not use strong encryption, sensitive information is at risk of interception.
- **Remediation**: Enforce encryption standards like WPA3 for wireless access and TLS 1.3 for remote sessions, and require full-disk encryption for mobile devices accessing sensitive data.

13. Unauthorized or Unrestricted Wireless Access

- **Regulation Impacted**: **Appendix A, Section III(C)** (Wireless Access Control).
- **Gap**: If wireless access is not restricted to authorized users and devices, it may provide an entry point for unauthorized users.
- **Remediation**: Set up wireless networks to authenticate and authorize devices and users according to policies, and monitor wireless access regularly.

14. Lack of Control Over External Information Systems and Portable Storage Devices

- **Regulation Impacted**: **Appendix A, Section III(C)** (Control of External Systems and Devices).
- **Gap**: If policies governing external system connections or portable storage device usage are not enforced, the credit union risks data leaks and unauthorized access.
- **Remediation**: Enforce restrictions on external system connections and portable storage device usage, and implement policies for secure use and monitoring.

15. Inadequate Control Over Publicly Accessible Information

- **Regulation Impacted**: **Appendix A, Section III(B)** (Public Information Handling).
- **Gap**: If there is no review process for publicly accessible information, sensitive data might be inadvertently exposed.
- **Remediation**: Implement a review and approval process for any public content and conduct annual audits to ensure compliance.

Answers

Thursday, October 10, 2024 3:14 PM

1. Do you use multifactor authentication (MFA) for system access?

- **Positive**: Yes, we enforce MFA for all user accounts accessing the system. Users are required to authenticate using at least two factors, such as a password and a hardware token or biometrics.
- **Negative**: No, we only require a password for system access, and we have not implemented additional authentication factors.

2. Are passwords complex, requiring a minimum length and a mix of characters (upper/lower case, numbers, special characters)?

- **Positive**: Yes, our password policy requires a minimum length of 12 characters, including upper/lower case letters, numbers, and special characters.
- **Negative**: No, our password policy only requires a minimum of 6 characters without specific complexity requirements.

3. Are access requests reviewed and approved before granting system access?

- **Positive**: Yes, all access requests are subject to a multi-level approval process involving the requester's manager and the IT security team before system access is granted.
- **Negative**: No, access requests are not formally reviewed; system access is often granted upon submission without further verification.

4. Do you maintain a list of authorized users, including their roles and responsibilities?

- **Positive**: Yes, we maintain an up-to-date list of all authorized users, including their assigned roles, which is reviewed monthly for accuracy.
- **Negative**: No, we do not maintain a comprehensive list of users, and roles are not consistently documented.

5. Do you use role-based access control (RBAC) to limit access to applications and data based on roles?

- **Positive**: Yes, RBAC is implemented, and access permissions are strictly based on user roles defined by their job functions.
- **Negative**: No, we do not use RBAC, and access permissions are set individually without following a role-based structure.

6. Are permissions granted based strictly on the "need-to-know" principle?

- **Positive**: Yes, permissions are reviewed and granted based strictly on the user's need to perform their job functions, minimizing unnecessary access.
- **Negative**: No, permissions are often granted broadly, and there is no strict enforcement of the need-to-know principle.

7. Are architectural solutions like firewalls, proxies, or encryption used to control data flow?

- **Positive**: Yes, we use a combination of firewalls, proxies, and encryption to manage and control the flow of sensitive information both internally and externally.
- **Negative**: No, we do not have sufficient architectural solutions in place to manage data flow; information flows freely without encryption or proxies.

8. Is information flow documented, including flow control enforcement based on security levels?

- **Positive**: Yes, information flow is documented, and we use predefined security levels to enforce flow control decisions based on the sensitivity of the data.
- **Negative**: No, information flow is not documented, and there are no specific controls in place to enforce security levels.

9. Are roles and responsibilities clearly defined to prevent conflicts of interest?

- **Positive**: Yes, roles and responsibilities are well-defined, and our system enforces segregation of duties to prevent conflicts of interest.
- **Negative**: No, roles and responsibilities overlap, and there is no system in place to prevent conflicts of interest.

10. Are user accounts created for separate functions to ensure that access is limited based on duties?

- **Positive**: Yes, user accounts are created and separated based on specific functions, ensuring limited access based on job responsibilities.
- **Negative**: No, user accounts are not separated, and employees may have access beyond their required duties.

11. Are user privileges limited to only those necessary for their role?

- **Positive**: Yes, user privileges are regularly reviewed and limited to the minimum necessary for their roles, ensuring compliance with the principle of least privilege.
- **Negative**: No, users often have more privileges than necessary, and there is no periodic review of these privileges.

12. Do you implement tools like Privileged Access Management (PAM) to control access?

- **Positive**: Yes, we use a PAM solution to control, monitor, and manage privileged accounts, ensuring secure access management.
- **Negative**: No, we do not use PAM tools, and privileged access is not actively monitored.

13. Are users required to use non-privileged accounts for routine functions?

- **Positive**: Yes, all users must use non-privileged accounts for routine tasks, reserving privileged accounts only for administrative functions.
- **Negative**: No, users often perform routine tasks using privileged accounts, increasing the risk of security incidents.

14. Is there an access control mechanism to prevent non-privileged users from executing privileged functions?

- **Positive**: Yes, our system has controls that prevent non-privileged users from executing

any privileged functions without appropriate permissions.

- **Negative**: No, non-privileged users can execute certain privileged functions, and there are insufficient controls to prevent this.

15. Are privileged functions logged and monitored?

- **Positive**: Yes, all privileged functions are logged and regularly monitored for unauthorized access or misuse.
- **Negative**: No, there is no logging or monitoring of privileged functions, making it difficult to detect unauthorized access.

16. Is there a limit on the number of unsuccessful logon attempts before the account is locked?

- **Positive**: Yes, accounts are locked after three unsuccessful logon attempts, and an alert is sent to the security team.
- **Negative**: No, there is no limit set on unsuccessful logon attempts, leaving the system vulnerable to brute-force attacks.

17. Are failed login attempts logged and reviewed?

- **Positive**: Yes, all failed login attempts are logged, and these logs are reviewed daily to detect potential security incidents.
- **Negative**: No, failed login attempts are not logged or reviewed, making it difficult to identify brute-force attempts or other malicious activity.

18. Does the system display a login banner with privacy and security notices before logon?

- **Positive**: Yes, a login banner with privacy and security notices is displayed for every user before accessing the system, outlining usage policies.
- **Negative**: No, the system does not display a login banner, leaving users unaware of the policies governing system use.

19. Is the system configured to lock sessions after a predetermined period of inactivity?

- **Positive**: Yes, the system automatically locks sessions after 10 minutes of inactivity, requiring re-authentication to regain access.
- **Negative**: No, the system does not lock sessions based on inactivity, increasing the risk of unauthorized access.

20. Is remote access to the system restricted to authorized users only?

- **Positive**: Yes, only pre-approved users with valid credentials can access the system remotely, and MFA is enforced for all remote access sessions.
- **Negative**: No, remote access is not properly restricted, and users can connect remotely without sufficient validation or security controls.

21. Are network monitoring tools deployed to track remote access activities?

- **Positive**: Yes, network monitoring tools are in place to log and track all remote access activities, and alerts are set up for any suspicious behavior.

- **Negative**: No, there is no active monitoring of remote access activities, making it difficult to detect unauthorized access.

22. Are all remote access connections protected using approved cryptographic methods?

- **Positive**: Yes, all remote connections use TLS 1.3 encryption to ensure the confidentiality and integrity of the data transmitted.
- **Negative**: No, some remote connections use outdated encryption methods or none at all, putting sensitive information at risk.

23. Is wireless access restricted to devices authorized by management?

- **Positive**: Yes, only authorized and registered devices are allowed to connect to the wireless network, and device validation occurs before access is granted.
- **Negative**: No, any device can connect to the wireless network without management approval, creating a security vulnerability.

24. Are mobile devices used within the organization encrypted?

- **Positive**: Yes, all mobile devices are encrypted using full-disk encryption to protect sensitive information stored on them.
- **Negative**: No, mobile devices are not encrypted, and sensitive information could be accessed if a device is lost or stolen.

25. Are connections to external information systems limited to authorized individuals?

- **Positive**: Yes, only authorized individuals with proper credentials and approvals can access external information systems, ensuring secure connections.
- **Negative**: No, external system connections are not adequately controlled, and unauthorized users may access the systems.

26. Are policies in place restricting the use of portable storage devices like USB drives?

- **Positive**: Yes, policies restrict the use of portable storage devices, and only approved devices can be used with encryption enabled.
- **Negative**: No, there are no policies governing the use of portable storage devices, and any device can be used without restrictions.

27. Are only authorized employees permitted to post information on public platforms?

- **Positive**: Yes, only authorized employees who have been trained on data handling can post information, and all posts are reviewed prior to publication.
- **Negative**: No, there is no control over who can post information publicly, leading to a risk of sensitive data exposure.

EF

Wednesday, December 4, 2024 8:56 AM

Finding: Administrative Accounts Accessing the Internet

Cited Regulation: *12 CFR Part 748, Appendix A to Part 748—Guidelines for Safeguarding Member Information*

Observation:
Administrative accounts, including domain administrator and other elevated privilege accounts, are permitted to access the internet. This practice exposes high-value administrative credentials to potential theft and compromise. Internet access by accounts with administrative privileges increases the likelihood of malicious actors exploiting vulnerabilities, such as phishing [T1566] or malicious downloads [T1204], to obtain access to these accounts.
Once administrative credentials are compromised, attackers can leverage them to conduct lateral movement [T1550.001], perform reconnaissance on Active Directory structures [T1087], and escalate privileges within the domain. Such exposure directly increases the risk of unauthorized access to member information and critical systems.

Implications:
Allowing administrative accounts to access the internet contravenes the principle of least privilege and fails to align with the requirements outlined in *12 CFR Part 748, Appendix A, Section III(B)*. The regulation emphasizes the importance of implementing robust access controls to limit potential exposure of sensitive information and administrative privileges.
This misconfiguration significantly heightens the risk to the credit union's network by providing attackers with direct paths to compromise systems, which could lead to breaches of member information, operational disruptions, and regulatory non-compliance.

Recommendations:
To address this vulnerability and ensure compliance with *12 CFR Part 748*, the credit union should:

1. **Restrict Internet Access for Administrative Accounts:**
   - Implement policies that explicitly block administrative accounts from accessing the internet.
2. **Segregate Administrative Accounts from User Accounts:**
   - Require IT personnel to maintain separate non-privileged user accounts for internet browsing and day-to-day activities.
3. **Use Privileged Access Workstations (PAWs):**
   - Designate secure workstations for administrative tasks that are isolated from internet access to prevent exposure of administrative credentials.
4. **Enhance Network Controls:**
   - Deploy network-level controls, such as web filters or firewalls, to block internet access for accounts with elevated privileges.
5. **Monitor and Enforce Compliance:**
   - Regularly review and monitor logs to ensure adherence to policies restricting internet access for administrative accounts.

Finding: Administrative Accounts Accessing the Internet

Cited Regulation: *12 CFR Part 748, Appendix A to Part 748—Guidelines for Safeguarding Member Information*

Observation:
Administrative accounts, including domain administrator and other elevated privilege accounts, are allowed to access the internet. This misconfiguration introduces significant risk by exposing critical credentials to compromise through phishing [T1566], malicious downloads [T1204], or other forms of attack. Such exposure increases the likelihood of lateral movement [T1550.001], Active Directory reconnaissance [T1087], and eventual domain escalation by malicious actors.

Implications:
This practice violates the safeguarding principles outlined in *12 CFR Part 748, Appendix A, Section III(B)*, which mandates robust access controls and the application of the principle of least privilege. Permitting administrative accounts to access the internet undermines these controls and creates unnecessary vulnerabilities that threaten member information security.

Recommendations:
Immediate Actions

1. **Restrict Internet Access for Administrative Accounts:**
   - Block all internet access for elevated accounts at the network level using web filters, firewalls, or endpoint protection tools.
2. **Separate User and Administrative Privileges:**
   - Enforce strict separation between user accounts and administrative accounts to ensure elevated accounts are used only for their intended administrative purposes.
3. **Implement Privileged Access Workstations (PAWs):**
   - Use dedicated, secure workstations for administrative activities that are isolated from external internet access.
4. **Deploy Authentication, Authorization, and Accounting (AAA) Systems [M1018]:**
   - Limit actions that elevated accounts can perform, monitor their use, and review logs for signs of abuse or unauthorized activity.

Additional Misconfiguration Recommendations for Network Defenders

1. **Excessive Account Privileges:**
   - Audit and reduce privileges for all accounts, ensuring permissions align with the principle of least privilege.
2. **Elevated Service Account Permissions:**
   - Configure service accounts with only the necessary permissions for their operation. Disable unused services and use ACLs to protect active services.
3. **Non-Essential Use of Elevated Accounts:**
   - Prohibit the use of elevated accounts for general tasks such as browsing the internet or accessing email.
4. **Time-Based Access for Privileged Accounts:**
   - Implement just-in-time (JIT) access, granting privileged access only when needed for a specific timeframe. This approach reduces the attack surface and supports Zero Trust principles.
5. **Periodic Reviews of Identity and Access Management (IAM):**
   - Regularly audit IAM roles and policies to minimize permanent administrator privileges and reduce the number of users with elevated roles.
6. **Restrict Local Administrator Group Membership:**
   - Prevent domain users from being in the local administrator group on multiple systems to limit lateral movement opportunities.
7. **Service Accounts and Applications:**
   - Run services with non-administrator accounts whenever possible and ensure unused services are disabled.
8. **Account Inactivity:**
   - Audit accounts regularly, removing inactive or unnecessary accounts to maintain a clean, secure environment.

Active Directory (AD) Hardening & Password Security Best Practices – Detailed Validation Guide

Overview

This guide provides step-by-step validation checks to confirm the correct implementation and effectiveness of each security control.

1. Active Directory Security Configuration

Disable Unused AD Accounts

- **Steps:**
    1. Open **Active Directory Users and Computers (ADUC)**.
    2. Navigate to **Users container** and run a query for inactive accounts:

```
Get-ADUser -Filter {LastLogonDate -lt (Get-Date).AddDays(-90)} -
Properties LastLogonDate
```

    3. Disable or remove identified inactive accounts.
- **Expected Outcome:**
    - ☑ All unused accounts are disabled or removed.

Secure AD Trusts

- **Steps:**
    1. Open **Active Directory Domains and Trusts**.
    2. Check **Trust Relationships** (Forest/Domains).
    3. Disable unnecessary trust relationships or enforce **SID Filtering** using:

```
netdom trust
```

- **Expected Outcome:**
    - ☑ Only required trusts exist, with **SID Filtering** enabled.

Limit Use of Service Accounts

- **Steps:**
    1. Identify all **service accounts** using:

```
Get-ADUser -Filter {ServicePrincipalName -ne "$null"}
```

    2. Apply **least privilege access**.
    3. Set **non-expiring passwords** only where strictly necessary.
    4. Implement **Managed Service Accounts (MSAs)** where possible.
- **Expected Outcome:**
    - ☑ Service accounts are minimized and secured.

Restrict Anonymous Access

- **Steps:**
    1. Open **Local Security Policy** (`secpol.msc`).
    2. Navigate to **Security Options > Network Access**.
    3. Ensure **Anonymous access is restricted** (`RestrictAnonymous = 1`).
- **Expected Outcome:**

- ☑ Anonymous access is fully disabled.

Harden Group Policy Objects (GPOs)

- **Steps:**
  1. Run:

```
gpresult /H GPOReport.html
```

  2. Review GPO settings for **password policies, access control, and auditing**.
  3. Ensure **GPOs are applied to all users and computers**.
- **Expected Outcome:**
  - ☑ Security GPOs are correctly configured and enforced.

Secure SYSVOL Permissions

- **Steps:**
  1. Check permissions on **\Domain\SYSVOL** using:

```
icacls \\domain\SYSVOL
```

  2. Ensure **Authenticated Users** have only **Read access**.
  3. Remove unnecessary permissions.
- **Expected Outcome:**
  - ☑ SYSVOL permissions are secured against modification.

Use Tiered Administration Model

- **Steps:**
  1. Review AD **OU structure**:

```
Get-ADOrganizationalUnit -Filter *
```

  2. Ensure **admin accounts are segregated**:
     - **Tier 0:** Domain Admins
     - **Tier 1:** Server Admins
     - **Tier 2:** Workstation Admins
- **Expected Outcome:**
  - ☑ Admin accounts follow the tiered model.

2. Privileged Account Management

Enforce Least Privilege

- **Steps:**
  1. List **members of privileged groups**:

```
Get-ADGroupMember -Identity "Domain Admins"
```

  2. Remove excess admin accounts.
- **Expected Outcome:**
  - ☑ Only required privileged users remain.

Implement Just-in-Time (JIT) Privileges

- **Steps:**
  1. Verify **Microsoft PAM or ESAE Forest** is deployed.
  2. Check **PAM workflow**:

```
Get-PAMRequest
```

- **Expected Outcome:**
  - ☑ Privileges are granted **only when needed**.

Restrict KRBTGT Account Access

- **Steps:**
  1. Reset **KRBTGT password** using:

```
Reset-Krbtgt -Confirm:$false
```
2. Ensure **password is changed twice a year**.

- **Expected Outcome:**
  - ☑ KRBTGT account password is regularly rotated.

3. Password Policy and Authentication Controls

Enforce Multi-Factor Authentication (MFA)

- **Steps:**
  1. Verify **MFA is enforced** for admin accounts.
  2. Use:

```
AzureADPolicySettings -GetMFAConfig
```

- **Expected Outcome:**
  - ☑ MFA is enabled for privileged accounts.

Use Strong Password Policies

- **Steps:**
  1. Run `gpedit.msc` → **Computer Configuration > Windows Settings > Security Settings > Account Policies > Password Policy**.
  2. Ensure:
     - Min Length: **12+ characters**
     - Block common passwords
     - No expiration policy
- **Expected Outcome:**
  - ☑ Strong password policy is enforced.

Monitor Password Reset Requests

- **Steps:**
  1. Check `Event ID 4724 (Password Reset)` in **Security Logs**.
  2. Alert on unusual **password reset patterns**.
- **Expected Outcome:**
  - ☑ Unauthorized password resets are detected.

4. Monitoring and Logging

Enable Advanced AD Auditing

- **Steps:**
  1. Run:

```
auditpol /get /category:*
```

  2. Ensure **Audit Directory Service Access** is enabled.
- **Expected Outcome:**
  - ☑ Advanced auditing is enabled.

Monitor Administrative Actions

- **Steps:**
  1. Enable **Logon Auditing** (`gpedit.msc > Local Policies > Audit Policy`).
  2. Review **Event ID 4625 (Failed Logins)** and **4672 (Admin Logins)**.
- **Expected Outcome:**
  - ☑ Administrative actions are monitored.

Centralize Event Logs

- **Steps:**
    1. Configure **SIEM (e.g., Splunk, Sentinel)** to collect AD logs.
- **Expected Outcome:**
    - ☑ Logs are aggregated and analyzed in real time.

Service Accounts

Thursday, February 20, 2025 11:36 AM

. Review Documentation

- **Gather Existing Inventory**: Start by locating any documentation that lists existing service accounts. This may include inventory sheets, system documentation, or application configurations that specify account names, descriptions, and their intended uses.
- **Identify Account Owners**: Note any documented information on account ownership or responsible application/system owners for follow-up purposes.

2. Use Active Directory Tools

- **Active Directory Users and Computers (ADUC)**: Open the ADUC console, navigate to your domain, and use the search/filter function to look for accounts with attributes commonly associated with service accounts. This can include:
    - Naming conventions (e.g., "svc_" or "sa_").
    - Descriptions containing "Service Account" or similar terms.
- **Advanced Searches**: Consider using advanced search filters to locate accounts by specific attributes such as creation date, last logon, or password expiration settings.

3. Look for Special Account Flags

- **PowerShell Queries**: Run PowerShell commands to filter accounts with specific account flags, which may indicate their use as service accounts:
    - `DONT_EXPIRE_PASSWORD`: Service accounts often have non-expiring passwords.
    - `PASSWORD_NOT_REQUIRED`: Indicates if an account has no password policy.
- `Get-ADUser -Filter {PasswordNeverExpires -eq $true} -Properties Name, Description, PasswordNeverExpires`
- `Get-ADUser -Filter {PasswordNotRequired -eq $true} -Properties Name, Description, PasswordNotRequired`

4. Check Group Membership

- **Review High-Privilege Groups**: Check membership in security groups known to have elevated permissions, such as "Domain Admins," "Enterprise Admins," and other critical groups.
- **Analyze Permissions**: Look into permissions associated with other groups where service accounts may be members. Consider using tools like ADUC, PowerShell, or third-party tools to obtain group membership reports.

5. Monitor Dependencies

- **Identify Service Account Dependencies**: For each service account, identify applications or services that rely on the account. Consult with application/system owners or administrators for additional context on dependencies.
- **Document Dependencies**: Create or update a log of each account's dependencies to clarify its purpose and identify potential impact areas if the account is disabled or modified.

6. Audit Logs

- **Monitor Event Logs**: Regularly review event logs on domain controllers for any events associated with service account activities. Focus on:

    - Logon attempts.
    - Password changes or resets.
    - Unauthorized access attempts.
- **Set Up Alerts**: Implement monitoring to generate alerts for unusual activities associated with service accounts, such as excessive logon failures or attempts from unknown IP addresses.

7. Document Findings and Report

- **Summarize Findings**: Document each account's purpose, flags, group memberships, dependencies, and any relevant security findings.
- **Report and Recommend**: Provide a summary report with recommendations, such as enforcing password policies, removing unused service accounts, or revising group memberships.
- **Regular Reviews**: Schedule routine reviews to ensure service accounts are compliant with security policies and accurately documented.

Lockout

Thursday, February 20, 2025 11:40 AM

While an 8-character password with a 5-attempt lockout can provide some protection against brute force attacks, it's not considered highly secure on its own; a truly robust security posture requires a strong password combined with a robust lockout mechanism and ideally, multi-factor authentication (MFA) for the best defense against online attacks.

Key points to remember:
Password strength matters:
An 8-character password may be considered weak if it only uses common characters or patterns, making it easier to crack.

Lockout limitations:
A 5-attempt lockout can still be bypassed by attackers with enough time and computing power, especially if the lockout period is short.

MFA is crucial:
Adding an extra layer of security like a code sent to your phone or a biometric scan through MFA significantly reduces the risk of unauthorized access, even if a password is compromised.

To enhance security:
Use complex passwords: Include a mix of uppercase and lowercase letters, numbers, and special characters.

Consider longer passwords: Aim for passwords that are at least 12 characters long.

Utilize password managers: Store and generate strong, unique passwords for each account using a reliable password manager.

Implement robust lockout policies: Set a reasonable lockout duration and number of failed attempts.

Educate users: Regularly remind users to create strong passwords and enable MFA when available.

Password Cracking 101: Attacks & Defenses Explained - BeyondTrust
May 2, 2024 — 3. Create Long, Random, Unique Passphrases. Strong passwords resist password cracking attempts. Passwords should be ove...

BeyondTrust
Password strength - Wikipedia
Password strength is a measure of the effectiveness of a password against guessing or brute-force attacks. In its usual form, it e...

Wikipedia
How to Stop Brute Force Attacks in Their Tracks - Threat Intelligence
Jul 27, 2023 — Limit Login Attempts Locking out users after a few unsuccessful attempts is a good brute force attack defense because ...

threatintelligence.com
Show all
Generative AI is experimental

Notes

Wednesday, September 4, 2024 7:21 AM

The validation process confirmed compliance with **12 CFR 748.0** and **Appendix A to Part 748** by thoroughly reviewing documented policies, system configurations, access controls, physical security measures, remote access management, and reporting practices. Policies and procedures were verified for completeness and alignment with industry standards such as **NIST SP 800-53** and **ISO 27001**, ensuring explicit coverage of password management, multi-factor authentication (MFA), account management, and access control requirements. Policies were confirmed to have senior management or board approval.

System configurations were audited to ensure alignment with documented policies, focusing on password complexity, MFA implementation, and timely disabling of inactive accounts. Access control reviews validated that user access was restricted to authorized personnel, administrative privileges were appropriately limited, and service accounts were accurately inventoried and managed.

Physical and environmental controls were inspected to confirm the implementation of access control mechanisms, such as biometric systems and surveillance, alongside operational environmental safeguards like fire suppression and climate control. Remote access security was evaluated to ensure encryption, MFA, and mobile device management (MDM) solutions were in place, with logs monitored to detect anomalies and vendor access appropriately controlled.

Role-based access control (RBAC) settings were reviewed to confirm that access rights were assigned based on organizational roles and periodically updated to reflect changes in risk or structure. Virtual security procedures, network access controls, and access provisioning processes were verified to ensure consistent adherence to documented procedures.

A comprehensive report documented the compliance status, identified discrepancies, and provided actionable recommendations for remediation. All findings, policies, and audit results were retained for regulatory and audit purposes, as required by **Appendix A, Section II**. This thorough review ensures that the organization effectively protects member information, mitigates security risks, and meets regulatory requirements.

Securing privileged access Enterprise access model - Privileged access | Microsoft Learn

The credit union uses PowerShell and .bat files for new hire scripts. Scripts must be stored securely. Restrict who can run the scripts (AC-6 Least Privilege) Sign PowerShell Scripts (SI 1 Software integrity). Script logs for review (AU 2, AU 6), Maintain version control of the scripts CM 3, review and approve changes before use (CM 5) Move towards scripting frameworks or IAM tools

The SME for each given critical application pulls a user access list from the application and sends it to all the supervisors for that application.

- Citrix virtual desktop published by Patelco
- Patelco VPN
- Mobile device with secure container controlled by PCU's Mobile Device Management Standard.

Multifactor authentication (Okta) shall be enforced for all remote access connections.
All logs are sent to our Security Information and Event Management (SIEM) system.
Security Operations Center (SOC) that continuously monitors user activity.

- Endpoint Detection and Response (or "EDR"), SentinelOne, agents are installed on all Domain Controllers. • Security Information and Event Management (SIEM) platform, Google SecOps (formerly Chronicle) ingests logs from various sources, including Domain Controllers and has alerts for administrative account activity. • Palo Alto firewalls monitor and control network traffic. • CIS Benchmarks are deployed, and enforced by Group Policy, to all Domain Controllers.

Benchmarks control which settings are audited and logged.
Credit Union has implemented CyberArk Privilege Cloud for Privileged Access Management (PAM)

1) Are all privileged accounts in CyberArk
2) Are least privileged policies enforced
3) Are inactive accounts automatically detected and disabled.
4) What are the lockout policies for CyberArk
5) Are remote privileged sessions routed through CyberArk Secure Remote Access and recorded.
6) Is MFA enabled
7) Automatic credential rotation
8) Audit logs contain who accessed the credentials when and why. Session recordings.
9) Alerting
10) Integration with SIEM
11) Are configurations reviewed periodically
12) Privileged Vault Web Access configuration
13) Privileged Threat Analytics
14) Privileged Session Manager
15) Privileged user access reviews
16) Attempt to access privileged sessions without CyberArk controls