Independent testing of controls

Friday, August 16, 2024 11:59 AM

Checklist for Validation Process: Stmt 5 and Sub-Statements
Aligned with Appendix A to Part 748, Title 12
Preparation

1. Understand Requirements

- **Action:** Review and understand regulatory requirements for testing, controls, and assessments as outlined in Appendix A.
- **Reference: Section III(B)(1)** – Ensure the validation process aligns with regulatory requirements for evaluating controls and risk assessments.

2. Gather Documentation

- **Action:** Collect all necessary documentation, such as audit reports, vulnerability scans, penetration testing reports, and previous assessments.
- **Reference: Section III(B)(1)** – Collect reports for evaluating controls and findings.

3. Identify Stakeholders

- **Action:** Ensure key teams such as internal audit, IT security, and external auditors are included in the validation process.
- **Reference: Section III(C)** – Stakeholders should be involved in reporting and validating findings.

4. Plan Validation

- **Action:** Develop a validation plan with detailed steps for assessing IT controls, testing procedures, and remediation actions. Are the audit plans derived from the risk assessment.
- **Reference: Section III(B)** – Regularly monitor and evaluate controls based on regulatory requirements.

Validation Steps

1. Validate IT Controls Audit (Stmt 5.1)

- **Action:** Review audit reports to ensure all critical controls are adequately covered.
- **Reference: Section III(B)(1)(a)** – Guidelines for independent assessments of control environments.
- **Action:** Verify the audit schedule to ensure regular reviews are conducted.
- **Reference: Section III(A)(2)** – Periodic reviews and audits must be scheduled.
- **Action:** Confirm audit procedures align with regulatory requirements.
- **Reference: Section III(A)(1)** – Audits must follow proper policies and procedures.

2. Validate Internal Vulnerability Scanning (Stmt 5.2)

- **Action:** Review internal vulnerability scanning reports for thoroughness.
- **Reference: Section III(A)(4)** – Regular monitoring of internal vulnerabilities.
- **Action:** Ensure that scanning occurs at regular intervals, as outlined in policy.
- **Reference: Section III(A)(4)** – Periodic internal vulnerability assessments are required.
- **Action:** Check for a documented remediation process for identified vulnerabilities.
- **Reference: Section III(B)(1)(b)** – Corrective actions must be taken to address vulnerabilities.

3. Validate External Vulnerability Scanning (Stmt 5.3)

- **Action:** Review external vulnerability scanning reports to confirm coverage of external systems.
- **Reference: Section III(A)(4)** – External threats must be regularly monitored.
- **Action:** Verify that external scans are conducted as scheduled.
- **Reference: Section III(A)(4)** – External risk assessments must occur periodically.
- **Action:** Confirm that remediation processes are in place for issues found during external scans.
- **Reference: Section III(B)(1)(b)** – Risks identified in external vulnerability scans must be mitigated.

4. Validate Internal Penetration Testing (Stmt 5.4)

- **Action:** Review reports to ensure comprehensive internal penetration testing of systems.
- **Reference: Section III(B)(1)(a)** – Independent assessments of internal systems are required.
- **Action:** Verify that internal penetration tests are conducted according to the organization's policy.
- **Reference: Section III(A)(4)** – Periodic penetration testing is necessary.
- **Action:** Ensure that findings from penetration tests are documented and addressed.
- **Reference: Section III(B)(1)(b)** – Remediation must follow penetration testing.

5. Validate External Penetration Testing (Stmt 5.5)

- **Action:** Review reports for external penetration testing to confirm external-facing systems are tested.
- **Reference: Section III(A)(4)** – External testing guidelines for assessing security risks.
- **Action:** Ensure that external penetration tests are scheduled and conducted regularly.
- **Reference: Section III(A)(4)** – External testing must follow a regular schedule.
- **Action:** Confirm that issues identified in external testing are properly addressed.
- **Reference: Section III(B)(1)(b)** – Corrective actions must be implemented for risks identified.

6. Validate Social Engineering Testing (Stmt 5.6)

- **Action:** Review social engineering testing reports to ensure all vectors, such as phishing and pretexting, are tested.
- **Reference: Section III(A)(5)** – Testing must address human vulnerabilities.
- **Action:** Confirm that the scope includes testing for human elements such as employee susceptibility to social engineering.
- **Reference: Section III(A)(5)** – Policies must include testing for human-related risks.
- **Action:** Verify that results are integrated into employee training programs.
- **Reference: Section III(B)(1)(c)** – Employee awareness programs must be adjusted based on test outcomes.

7. Validate Penetration Testing Program (Stmt 5.7)

- **Action:** Review the documentation of the penetration testing program to ensure it is tailored to the credit union’s needs.
- **Reference: Section III(A)(1)** – Security programs must be customized based on specific risk factors.
- **Action:** Confirm that the scope of the program covers all critical systems and assets.
- **Reference: Section III(B)(1)(a)** – The testing program must comprehensively cover security areas.
- **Action:** Ensure that the penetration testing program is regularly updated.
- **Reference: Section III(A)(3)** – Security processes must be kept up to date.

8. Validate Testing of Wireless Controls (Stmt 5.8)

- **Action:** Review wireless security testing reports to ensure coverage of wireless networks.
- **Reference: Section III(A)(4)** – Wireless controls must be regularly tested.
- **Action:** Verify that wireless vulnerability testing occurs at regular intervals.
- **Reference: Section III(A)(4)** – Regular monitoring of wireless controls is required.
- **Action:** Confirm that any issues found in wireless testing are remediated.
- **Reference: Section III(B)(1)(b)** – Corrective actions for wireless vulnerabilities must be implemented.

9. Validate Formal Audit Plan and Schedule (Stmt 5.9)

- **Action:** Review the formal audit plan to ensure critical controls are scheduled for regular testing.
- **Reference: Section III(A)(2)** – A formal audit plan must be in place.
- **Action:** Verify that audits are completed according to the schedule.
- **Reference: Section III(B)(1)** – Audits must be timely and comprehensive.

10. Validate Penetration Testing Program Characteristics (Stmt 5.10)

- **Action:** Ensure that the penetration testing program covers all critical areas and is documented.
- **Reference: Section III(A)(1)** – The scope of testing programs must be comprehensive.
- **Action:** Verify that documentation for the penetration testing program is maintained and up to date.
- **Reference: Section III(B)(1)(a)** – All security assessments must be properly documented.

11. Validate Outstanding Issues (Stmt 5.11)

- **Action:** Confirm that all outstanding issues from previous assessments are tracked.
- **Reference: Section III(B)(2)** – All issues must be documented and tracked until resolution.
- **Action:** Verify that the status of outstanding issues is regularly updated.
- **Reference: Section III(B)(2)** – Issues must be resolved in a timely manner.

12. Validate Application Penetration Testing (Stmt 5.12)

- **Action:** Review application penetration testing reports to ensure application-level risks are identified and tested.
- **Reference: Section III(A)(4)** – Guidelines for testing application security.
- **Action:** Confirm that vulnerabilities identified in application testing are remediated.
- **Reference: Section III(B)(1)(b)** – Corrective actions must be taken for application vulnerabilities.

Reporting

1. Compile Findings

- **Action:** Document all findings and provide actionable insights for stakeholders.
- **Reference: Section III(C)** – Findings must be documented and reported to management.

2. Prepare Report

- **Action:** Compile a comprehensive report detailing test results, audit findings, and issues.
- **Reference: Section III(B)(1)** – Reports should provide clear insights into the status of security controls.

3. Review and Approval

- **Action:** Present findings to senior management and the Board for review and approval.
- **Reference: Section III(C)** – The Board and senior management must be involved in reviewing audit results.

4. Follow-Up

- **Action:** Develop a follow-up plan to address identified gaps and monitor the implementation of corrective actions.
- **Reference: Section III(B)(2)** – Gaps must be addressed, and corrective actions must be monitored until resolved.

Issues

Thursday, September 19, 2024 10:48 AM

Validation Steps Findings

1. Validate IT Controls Audit (Stmt 5.1)

- **Finding:** Audit reports do not cover critical controls or do not align with regulatory requirements.
  - **Reference: Section III(B)(1)(a)** – Independent assessments must comprehensively cover the control environment.
- **Finding:** No regular audit schedule or misalignment between scheduled reviews and the organization's policies.
  - **Reference: Section III(A)(2)** – Periodic audits and reviews are required to ensure ongoing control effectiveness.

2. Validate Internal Vulnerability Scanning (Stmt 5.2)

- **Finding:** Internal vulnerability scans are incomplete, missing critical systems or assets, or are performed infrequently.
  - **Reference: Section III(A)(4)** – Regular internal scans must be performed to monitor vulnerabilities in critical systems.
- **Finding:** Lack of documented remediation actions following internal vulnerability assessments.
  - **Reference: Section III(B)(1)(b)** – Corrective action must be documented and taken to address identified vulnerabilities.

3. Validate External Vulnerability Scanning (Stmt 5.3)

- **Finding:** External vulnerability scans do not cover all external-facing systems or occur less frequently than required.
  - **Reference: Section III(A)(4)** – External threats must be regularly monitored through periodic external scans.
- **Finding:** Inadequate or missing remediation actions for vulnerabilities identified in external scans.
  - **Reference: Section III(B)(1)(b)** – Remediation of external vulnerabilities must be documented and addressed promptly.

4. Validate Internal Penetration Testing (Stmt 5.4)

- **Finding:** Internal penetration testing is not comprehensive or does not cover all critical internal systems.
  - **Reference: Section III(B)(1)(a)** – Independent assessments, including penetration tests, must evaluate critical systems to detect weaknesses.
- **Finding:** Penetration tests are not conducted in alignment with the policy or do not follow a consistent schedule.
  - **Reference: Section III(A)(4)** – Regular penetration testing is required to assess system defenses.
- **Finding:** Issues identified in penetration testing are not properly documented or remediated.
  - **Reference: Section III(B)(1)(b)** – Remediation processes must be implemented following penetration tests.

5. Validate External Penetration Testing (Stmt 5.5)

- **Finding:** External penetration testing does not adequately cover external-facing assets, or testing is not conducted as scheduled.
  - **Reference: Section III(A)(4)** – External-facing systems must undergo regular penetration testing to assess security controls.
- **Finding:** Remediation actions for vulnerabilities identified during external penetration tests are not tracked or implemented.
  - **Reference: Section III(B)(1)(b)** – Vulnerabilities found during penetration testing must be addressed with corrective measures.

6. Validate Social Engineering Testing (Stmt 5.6)

- **Finding:** Social engineering tests (e.g., phishing, pretexting) do not cover all relevant attack vectors or human vulnerabilities.
  - **Reference: Section III(A)(5)** – Testing must cover human factors in security, including social engineering risks.
- **Finding:** Social engineering test results are not integrated into employee training programs or awareness initiatives.
  - **Reference: Section III(B)(1)(c)** – Employee awareness programs must address human vulnerabilities based on testing results.

7. Validate Penetration Testing Program (Stmt 5.7)

- **Finding:** The penetration testing program is not tailored to the specific needs and risks of the credit union.
  - **Reference: Section III(A)(1)** – Security programs must be customized to the institution's risk profile and operational needs.
- **Finding:** The penetration testing program does not cover all relevant assets or is not updated regularly.
  - **Reference: Section III(A)(3)** – Security processes and testing programs must be kept up to date and comprehensive.

8. Validate Testing of Wireless Controls (Stmt 5.8)

- **Finding:** Wireless network security is not adequately tested, or reports do not address wireless vulnerabilities.
  - **Reference: Section III(A)(4)** – Wireless networks must undergo regular security testing to ensure compliance.
- **Finding:** Issues identified during wireless security testing are not properly remediated.
  - **Reference: Section III(B)(1)(b)** – Remediation of identified wireless control issues is necessary to maintain security.

9. Validate Formal Audit Plan and Schedule (Stmt 5.9)

- **Finding:** The audit plan does not cover all critical controls, or scheduled audits are not conducted in a timely manner.
  - **Reference: Section III(A)(2)** – Audit plans must include scheduling and testing of critical controls.
- **Finding:** The audit plan is not executed as scheduled, leading to delays in reviewing critical security areas.
  - **Reference: Section III(B)(1)** – Audits must be timely and follow the established schedule to ensure continuous monitoring.

10. Validate Penetration Testing Program Characteristics (Stmt 5.10)

- **Finding:** The penetration testing program does not comprehensively cover all critical systems and areas of potential risk.
  - **Reference: Section III(A)(1)** – Testing programs must be comprehensive to identify all relevant risks.
- **Finding:** Documentation for the penetration testing program is incomplete or not maintained properly.
  - **Reference: Section III(B)(1)(a)** – All security assessments, including penetration testing, must be properly documented.

11. Validate Outstanding Issues (Stmt 5.11)

- **Finding:** Outstanding issues from previous assessments are not properly tracked or documented, resulting in unresolved vulnerabilities.
  - **Reference: Section III(B)(2)** – All security issues must be tracked and resolved in a timely manner.
- **Finding:** The status of outstanding issues is not regularly updated, leaving risks unresolved.
  - **Reference: Section III(B)(2)** – Timely resolution of outstanding issues is essential for maintaining security.

12. Validate Application Penetration Testing (Stmt 5.12)

- **Finding:** Application penetration testing is not comprehensive, and some critical applications are not tested.
  - **Reference: Section III(A)(4)** – Applications handling sensitive member information must undergo regular security testing.
- **Finding:** Vulnerabilities identified in application penetration testing are not remediated or tracked properly.
  - **Reference: Section III(B)(1)(b)** – Corrective actions must be implemented for vulnerabilities found during application testing.

Reporting Findings

1. Compile Findings

- **Finding:** Incomplete documentation of findings, limiting the ability to provide actionable insights to management.
  - **Reference: Section III(C)** – All findings must be clearly documented and actionable.

2. Prepare Report

- **Finding:** The report is missing critical information about security test results or does not provide clear recommendations.
    - **Reference: Section III(B)(1)** – Reporting of test results and audit findings must be clear and comprehensive.

3. Review and Approval

- **Finding:** Failure to present findings to senior management and the Board for review and approval.
    - **Reference: Section III(C)** – The Board must review and approve findings from security assessments and audits.

4. Follow-Up

- **Finding:** Follow-up actions are not adequately documented, monitored, or resolved, leaving security gaps.
    - **Reference: Section III(B)(2)** – Corrective actions must be tracked and monitored to ensure issues are fully resolved.

Remediation

Thursday, September 19, 2024 10:52 AM

1. IT Controls Audit (Stmt 5.1)

Finding: Inadequate audit coverage or misalignment with policy.

- **Remediation Steps:**
    1. **Ensure all critical controls** are included in the scope of internal and external audits.
    2. **Review audit procedures** to align with regulatory requirements and best practices.
    3. **Establish an audit calendar** to schedule regular reviews, ensuring that audits are performed on time.

6. Internal Vulnerability Scanning (Stmt 5.2)

Finding: Incomplete scans or infrequent scanning.

- **Remediation Steps:**
    1. **Ensure comprehensive scanning** by reviewing scanning policies and procedures to cover all critical systems and applications.
    2. **Increase the frequency of scans** to align with regulatory guidance and internal risk management policies.
    3. **Document and track vulnerabilities** to ensure that they are remediated promptly, using a formal vulnerability management program.

7. External Vulnerability Scanning (Stmt 5.3)

Finding: External vulnerability scans are not comprehensive or scheduled regularly.

- **Remediation Steps:**
    1. **Expand the scope** of external vulnerability scans to include all external-facing systems and network entry points.
    2. **Schedule regular scans** based on the credit union's risk profile and regulatory requirements.
    3. **Implement automated tracking** for remediation of externally identified vulnerabilities to ensure timely corrective actions.

8. Internal and External Penetration Testing (Stmts 5.4 and 5.5)

Finding: Incomplete penetration testing or failure to remediate findings.

- **Remediation Steps:**
    1. **Review penetration testing programs** to ensure coverage of all critical internal and external systems.
    2. **Schedule regular penetration tests** and ensure testing aligns with the credit union's risk profile and regulatory requirements.
    3. **Document and prioritize remediation efforts** for all identified vulnerabilities, ensuring that high-risk issues are resolved immediately.

9. Social Engineering Testing (Stmt 5.6)

Finding: Inadequate scope or frequency of social engineering testing.

- **Remediation Steps:**
    1. **Expand social engineering tests** to include multiple vectors (e.g., phishing, pretexting) and ensure they target human vulnerabilities effectively.
    2. **Integrate testing results** into employee awareness programs, adjusting training based on identified weaknesses.
    3. **Schedule regular social engineering tests** to assess the effectiveness of security awareness programs.

10. Penetration Testing Program (Stmt 5.7)

Finding: The penetration testing program is not tailored or regularly updated.

- **Remediation Steps:**
    1. **Customize the penetration testing program** based on the specific threats and risks faced by the credit union.
    2. **Ensure all relevant systems are included** in the testing scope, including new applications or technologies introduced since the last test.
    3. **Update the program regularly** to reflect emerging threats and changes in the IT environment.

11. Wireless Controls Testing (Stmt 5.8)

Finding: Insufficient wireless security testing.

- **Remediation Steps:**
    1. **Ensure regular wireless network testing** is included in the security testing schedule.
    2. **Expand testing scope** to cover all wireless access points, guest networks, and internal wireless systems.
    3. **Document and remediate vulnerabilities** identified in wireless network testing, ensuring all issues are tracked until resolved.

12. Formal Audit Plan and Schedule (Stmt 5.9)

Finding: Missing or incomplete audit plans, or audits not conducted as scheduled.

- **Remediation Steps:**
    1. **Develop a formal audit plan** that outlines audit objectives, frequency, and scope for all critical systems.
    2. **Create an audit calendar** and assign accountability to ensure that audits are performed on schedule.
    3. **Review audit results** promptly and implement any recommended corrective actions.

13. Penetration Testing Program Characteristics (Stmt 5.10)

Finding: Penetration testing program lacks comprehensive scope or documentation.

- **Remediation Steps:**
    1. **Ensure the penetration testing program** covers all critical areas, including network, applications, and user behavior.
    2. **Maintain comprehensive documentation** for all penetration testing activities, including scope, results, and remediation actions.

3. **Regularly review and update the program** to reflect any changes in the IT environment or business operations.

14. Outstanding Issues Tracking (Stmt 5.11)

Finding: Failure to track or resolve outstanding issues.

- **Remediation Steps:**
  1. **Implement an issue tracking system** that captures all security issues identified during audits, vulnerability scans, or penetration tests.
  2. **Assign ownership for remediation** of each issue, with clear deadlines for resolution.
  3. **Regularly review the status of outstanding issues** to ensure timely resolution and mitigate potential risks.

15. Application Penetration Testing (Stmt 5.12)

Finding: Application penetration testing is not comprehensive, or vulnerabilities are not remediated.

- **Remediation Steps:**
  1. **Expand application penetration testing** to include all critical applications, especially those handling sensitive member information.
  2. **Document vulnerabilities** identified during testing and track their remediation.
  3. **Ensure timely remediation** of application vulnerabilities, particularly those that expose member information to risks.

Compliance

Thursday, September 19, 2024 10:58 AM

The compliance steps for **independent testing of controls** according to **Appendix A to Part 748, Title 12** are designed to ensure that credit unions conduct thorough, objective assessments of their information security controls. These independent assessments verify that the controls in place effectively protect member information from unauthorized access, misuse, or loss. Below are the **compliance steps** required to meet regulatory expectations:

1. Define the Scope of Independent Testing

1.1 Identify Critical Systems and Controls

- **Action:** Determine which systems, applications, processes, and controls will be tested, with a focus on those safeguarding member information.
- **Reference: Appendix A, Section III(B)(1)(a)** – Independent testing must assess critical systems and controls to ensure the protection of member information.

1.2 Tailor the Scope Based on Risk

- **Action:** Ensure the scope of testing reflects the specific risks and vulnerabilities identified in the institution's risk assessment,covering both administrative and technical controls.
- **Reference: Appendix A, Section III(A)(1)** – Testing should be aligned with the institution's risk profile and address areas that are most critical for data protection.

2. Engage Qualified Independent Parties

2.1 Ensure Independence of Testing

- **Action:** Engage independent auditors, third-party service providers, or internal auditors who are not involved in the design or operation of the controls being tested.
- **Reference: Appendix A, Section III(B)(1)(a)** – The testing must be conducted by parties independent of those responsible for managing the controls to ensure objectivity.

2.2 Verify Credentials of Testing Personnel

- **Action:** Ensure that the personnel conducting the testing are qualified and experienced in performing security assessments, audits, and vulnerability testing.
- **Reference: Appendix A, Section III(B)(1)(a)** – Testing personnel must have the necessary qualifications to conduct thorough and accurate assessments.

3. Review and Update Testing Policies

3.1 Develop or Update Testing Policies

- **Action:** Review and update the credit union's policies for independent control testing, ensuring they align with regulatory requirements and industry best practices.
- **Reference: Appendix A, Section III(A)(3)** – Policies must be regularly reviewed and updated to reflect changes in risk and emerging threats.

3.2 Align Policies with Risk Assessment

- **Action:** Ensure the independent testing policies are aligned with the risk assessment to target areas where the potential impact on member information security is highest.
- **Reference: Appendix A, Section III(B)(1)(a)** – Testing should prioritize high-risk areas identified in the risk assessment.

4. Conduct Independent Testing

4.1 Perform IT Audits

- **Action:** Conduct independent audits of IT systems, controls, and processes to ensure they are functioning as intended and effectivelymitigating risks to member information.
- **Reference: Appendix A, Section III(B)(1)(a)** – Independent audits must be comprehensive and include all critical controls and systems.

4.2 Perform Vulnerability Scans and Penetration Testing

- **Action:** Perform regular vulnerability scans and penetration tests on internal and external systems to identify potential weaknesses that could compromise member data.
- **Reference: Appendix A, Section III(A)(4)** – Vulnerability assessments and penetration testing must be conducted to identify and mitigate security gaps.

4.3 Test Physical and Administrative Controls

- **Action:** Test physical controls (e.g., facility access) and administrative controls (e.g., policies, procedures) to ensure they are preventing unauthorized access to member information.
- **Reference: Appendix A, Section III(A)(1)** – Physical and administrative controls must be part of the testing process to ensure a comprehensive security posture.

5. Document and Report Findings

5.1 Document Test Results

- **Action:** Record the results of independent testing, including any vulnerabilities, weaknesses, or control failures identified during the testing process.
- **Reference: Appendix A, Section III(C)** – Test results must be documented clearly to provide a complete picture of the control environment's effectiveness.

5.2 Provide Actionable Recommendations

- **Action:** Include recommendations for remediation and improvements in the test report, focusing on areas where controls were found to be ineffective or missing.
- **Reference: Appendix A, Section III(B)(1)(b)** – The institution must implement corrective actions based on the findings of the independent test.

5.3 Report Findings to Senior Management and the Board

- **Action:** Present the results of the independent testing to senior management and the Board of Directors for review and approval, ensuring they are fully informed of any risks or control gaps.
- **Reference: Appendix A, Section III(C)** – Senior management and the Board must be involved in the review of independent testing results to ensure proper oversight.

6. Implement Corrective Actions

6.1 Develop a Corrective Action Plan

- **Action:** Based on the findings of the independent testing, develop a corrective action plan that outlines specific steps, timelines, and responsibilities for remediating identified issues.
- **Reference: Appendix A, Section III(B)(1)(b)** – Corrective actions must be taken to address deficiencies and mitigate risks identified during the independent testing.

6.2 Prioritize High-Risk Issues

- **Action:** Ensure that issues identified as high-risk are prioritized in the corrective action plan and are addressed first to mitigate the most critical vulnerabilities.
- **Reference: Appendix A, Section III(B)(1)(b)** – High-risk areas must be remediated promptly to protect member information from unauthorized access or breaches.

6.3 Track and Monitor Remediation Progress

- **Action:** Track the progress of remediation efforts and ensure all corrective actions are completed within the designated time frame.
- **Reference: Appendix A, Section III(B)(2)** – The institution must follow up on corrective actions to ensure they are implemented effectively.

7. Revalidate Controls After Remediation

7.1 Conduct Follow-Up Testing

- **Action:** After implementing corrective actions, conduct follow-up independent testing to ensure that the identified weaknesses have been properly remediated and that controls are functioning as intended.
- **Reference: Appendix A, Section III(B)(2)** – Revalidation of controls is necessary to confirm that issues have been resolved and no new vulnerabilities have been introduced.

7.2 Update the Risk Assessment

- **Action:** Update the credit union's risk assessment to reflect the findings and improvements made as a result of the independent testing.
- **Reference: Appendix A, Section III(B)(1)(a)** – The risk assessment must be updated regularly to reflect the current state of controls and risks.

8. Continuous Monitoring and Improvement

8.1 Schedule Regular Independent Testing

- **Action:** Establish a regular schedule for independent testing of controls, ensuring that high-risk areas are tested more frequently, while lower-risk areas are tested periodically.
- **Reference: Appendix A, Section III(A)(2)** – Testing must be performed on a regular basis to ensure ongoing control effectiveness.

8.2 Incorporate Testing into the Continuous Monitoring Program

- **Action:** Integrate independent testing into the credit union's continuous monitoring program to proactively detect and address potential security weaknesses.
- **Reference: Appendix A, Section III(A)(5)** – Continuous monitoring should be in place to detect emerging risks and vulnerabilities in real time.

8.3 Review and Update Testing Policies Regularly

- **Action:** Regularly review and update the independent testing policies and procedures to reflect changes in the credit union's risk profile, IT environment, and regulatory requirements.
- **Reference: Appendix A, Section III(A)(3)** – Policies and procedures must be regularly updated to address changes in risk and emerging threats.

By following these **compliance steps for independent testing of controls**, credit unions can ensure their **Information Security Program** meets the requirements outlined in **Appendix A to Part 748, Title 12**. These steps help ensure that member information is properly safeguarded, risks are mitigated, and controls are regularly assessed and improved.

Tools

Friday, August 16, 2024 12:00 PM

Tools for Stmt 5 and Sub-Statements

1. **Information Technology Controls Audit (Stmt 5.1)**
    - **Audit Management Software**: Tools like **AuditBoard**, **TeamMate**, and **Pentana** help manage audit schedules, documentation, and findings.
    - **Compliance Management Tools**: Platforms such as **Qualys**, **Rapid7**, or **NIST** frameworks can assist in ensuring that controls meet regulatory and compliance requirements.
2. **Internal Vulnerability Scanning (Stmt 5.2)**
    - **Vulnerability Scanners**: Tools like **Nessus**, **OpenVAS**, and **Qualys** can identify vulnerabilities in internal systems.
    - **Network Scanners**: Tools like **Nmap** can help identify open ports and potential vulnerabilities within internal networks.
3. **External Vulnerability Scanning (Stmt 5.3)**
    - **External Scanners**: Tools such as **Qualys**, **Rapid7 InsightVM**, and **Nessus** are used to scan externally facing systems and services for vulnerabilities.
    - **Web Application Scanners**: Tools like **Acunetix** or **OWASP ZAP** focus specifically on web applications and external interfaces.
4. **Internal Penetration Testing (Stmt 5.4)**
    - **Penetration Testing Frameworks**: Tools like **Metasploit**, **Core Impact**, and **Burp Suite** are commonly used for conducting internal penetration tests.
    - **Testing Scripts**: Custom scripts or tools used in-house for specific penetration testing scenarios.
5. **External Penetration Testing (Stmt 5.5)**
    - **Penetration Testing Tools**: **Nessus**, **Kali Linux** (which includes various penetration testing tools), and **Burp Suite** are used for external testing.
    - **Third-Party Services**: Engaging with external security firms or services for comprehensive external penetration testing.
6. **Social Engineering Testing (Stmt 5.6)**
    - **Social Engineering Tools**: Tools like **PhishingBox**, **Gophish**, and **Social-Engineer Toolkit (SET)** can be used for conducting phishing and other social engineering tests.
    - **Simulation Platforms**: Platforms such as **KnowBe4** offer comprehensive social engineering and awareness training.
7. **Penetration Testing Program (Stmt 5.7)**
    - **Program Management Tools**: **Jira**, **Asana**, or **Trello** for tracking penetration testing activities and scheduling.
    - **Documentation**: Tools like **Confluence** for documenting the penetration testing program and its characteristics.
8. **Testing Wireless Controls (Stmt 5.8)**
    - **Wireless Network Scanners**: Tools like **Aircrack-ng**, **Kismet**, and **NetSpot** are used for assessing wireless network security.
    - **Wireless Security Assessors**: Tools for assessing the security of wireless protocols and configurations.
9. **Formal Audit Plan and Schedule (Stmt 5.9)**
    - **Audit Scheduling Tools**: **AuditBoard**, **TeamMate**, and **Engage** for creating and managing audit plans and schedules.
    - **Project Management Tools**: **Microsoft Project** or **Smartsheet** for tracking audit schedules and milestones.
10. **Penetration Testing Program Characteristics (Stmt 5.10)**
    - **Program Management Tools**: **Jira**, **Asana**, or **Trello** to track and manage the scope and characteristics of the penetration testing program.
    - **Documentation Tools**: **Confluence** or **SharePoint** for maintaining detailed documentation of the penetration testing program.
11. **Outstanding Issues (Stmt 5.11)**
    - **Issue Tracking Tools**: **Jira**, **ServiceNow**, or **Bugzilla** for tracking and managing unresolved issues.
    - **Compliance Management**: **Qualys** or **Rapid7** for tracking compliance-related issues and their resolution.
12. **Application Penetration Testing (Stmt 5.12)**
    - **Application Security Testing Tools**: **OWASP ZAP**, **Burp Suite**, and **AppScan** for conducting application penetration tests.
    - **Static Analysis Tools**: **SonarQube** or **Checkmarx** for static application security testing (SAST).

Additional Considerations

- **Documentation and Reporting**: Tools like **Microsoft Word**, **Excel**, or **Google Docs** can be used for documenting findings and preparing reports.
- **Integration with Existing Systems**: Ensure that the tools used integrate well with other systems and workflows within the organization.

Best Tools for CORE Statements

1. **Information Technology Controls Audit (Stmt 5.1)**
    - **Best Tool**: **AuditBoard**
        - **Why**: AuditBoard is widely used for managing audit processes, including tracking controls, managing audit schedules, and generating reports. It supports various audit methodologies and integrates well with other risk management tools.
2. **Internal Vulnerability Scanning (Stmt 5.2)**
    - **Best Tool**: **Qualys Vulnerability Management**
        - **Why**: Qualys is known for its comprehensive vulnerability scanning capabilities, ease of use, and robust reporting features. It provides detailed insights into internal vulnerabilities and integrates with other security management tools.
3. **External Vulnerability Scanning (Stmt 5.3)**
    - **Best Tool**: **Rapid7 InsightVM**
        - **Why**: Rapid7 InsightVM offers strong external vulnerability scanning features with actionable insights and remediation guidance. It is also known for its scalability and ease of integration with other security solutions.
4. **Internal Penetration Testing (Stmt 5.4)**
    - **Best Tool**: **Metasploit**
        - **Why**: Metasploit is a leading penetration testing framework that provides extensive exploit capabilities, customizable testing, and a large community of contributors. It is highly effective for conducting internal penetration tests.
5. **External Penetration Testing (Stmt 5.5)**
    - **Best Tool**: **Burp Suite Professional**
        - **Why**: Burp Suite Professional is a comprehensive web application security testing tool that excels in external penetration testing. It provides powerful scanning and attack simulation features for identifying vulnerabilities in external-facing applications.
6. **Social Engineering Testing (Stmt 5.6)**
    - **Best Tool**: **KnowBe4**
        - **Why**: KnowBe4 specializes in social engineering and phishing simulation, offering a range of tools to test and improve organizational security awareness and response to social engineering attacks.
7. **Penetration Testing Program (Stmt 5.7)**
    - **Best Tool**: **Cobalt Strike**
        - **Why**: Cobalt Strike provides a robust platform for managing and executing penetration testing engagements. It includes features for establishing a testing program, managing scope, and coordinating with other security tools.
8. **Testing Wireless Controls (Stmt 5.8)**
    - **Best Tool**: **Aircrack-ng**
        - **Why**: Aircrack-ng is a suite of tools focused on wireless network security. It is widely used for assessing the security of wireless networks, including encryption and authentication mechanisms.
9. **Formal Audit Plan and Schedule (Stmt 5.9)**
    - **Best Tool**: **TeamMate**
        - **Why**: TeamMate provides comprehensive audit management capabilities, including planning, scheduling, and tracking audit activities. It helps ensure that audit plans are well-documented and adhered to.
10. **Penetration Testing Program Characteristics (Stmt 5.10)**
    - **Best Tool**: **Tenable.io**
        - **Why**: Tenable.io offers extensive capabilities for managing the characteristics of a penetration testing program, including asset discovery, vulnerability assessment, and integration with other security tools.
11. **Outstanding Issues (Stmt 5.11)**
    - **Best Tool**: **Jira**
        - **Why**: Jira is a powerful issue and project tracking tool that helps manage and resolve outstanding issues. It is widely used for tracking issues across various domains, including IT and security.
12. **Application Penetration Testing (Stmt 5.12)**
    - **Best Tool**: **OWASP ZAP**
        - **Why**: OWASP ZAP (Zed Attack Proxy) is a highly effective, open-source tool for application penetration testing. It is known for its user-friendly interface and robust testing capabilities, making it suitable for testing both internal and externally developed applications.

Resources

Friday, August 16, 2024 12:02 PM

https://csf.tools/reference/nist-sp-800-53/r5/ca/ca-2/
https://mitre-attack.github.io/attack-navigator/#layerURL=https%3A%2F%2Fraw.githubusercontent.com%2Fcenter-for-threat-informed-defense%2Fattack-control-framework-mappings%2Fmain%2Fframeworks%2Fattack_12_1%2Fnist800_53_r4%2Flayers%2Fby_family%2FSecurity_Assessment_And_Authorization%2FCA-2.json

Best
Practices ...

Comments

Thursday, September 26, 2024 1:37 PM

1. Define the Scope of Independent Testing

- **Finding**: "The credit union has clearly defined the scope of independent testing, focusing on critical systems, applications, and pro cesses that safeguard member information. This scope aligns with the institution’s risk assessment, ensuring the most critical areas are prioritized, in compliance with Appendix A, Section III(B)(1)(a)."
- **Finding**: "Testing is tailored based on the institution’s risk profile, ensuring that systems with higher risk receive greater attent ion. This risk-based approach demonstrates adherence to Appendix A, Section III(A)(1)."

2. Engage Qualified Independent Parties

- **Finding**: "The independent testing is conducted by third-party auditors with no involvement in the design or management of the controls being tested, ensuring objectivity and independence as required by Appendix A, Section III(B)(1)(a)."
- **Finding**: "All testing personnel are qualified and certified, with extensive experience in conducting IT audits, vulnerability assess ments, and penetration tests, which meets the standards outlined in Appendix A, Section III(B)(1)(a)."

3. Review and Update Testing Policies

- **Finding**: "The credit union has a robust policy in place for independent testing, which is regularly reviewed and updated to reflect changes in risks, threats, and regulatory requirements, in alignment with Appendix A, Section III(A)(3)."
- **Finding**: "Testing policies are directly linked to the results of the risk assessment, ensuring that high-risk areas identified during the assessment are prioritized during testing, as required by Appendix A, Section III(B)(1)(a)."

4. Conduct Independent Testing

- **Finding**: "The credit union conducts comprehensive IT audits that cover all critical systems and processes, ensuring that controls ar e functioning as intended and effectively mitigating risks to member information, in compliance with Appendix A, Section III(B)(1)(a)."
- **Finding**: "Regular vulnerability scans and penetration tests are performed on internal and external systems, and the results are used to address potential weaknesses, in accordance with Appendix A, Section III(A)(4)."
- **Finding**: "Physical and administrative controls are regularly tested to ensure that access to sensitive data is properly restricted, both physically and procedurally, as required by Appendix A, Section III(A)(1)."

5. Document and Report Findings

- **Finding**: "Independent testing results are clearly documented, and any identified vulnerabilities or weaknesses are detailed comprehe nsively. This ensures transparency and compliance with Appendix A, Section III(C)."
- **Finding**: "The credit union provides actionable recommendations based on the test results, prioritizing areas where controls were fou nd to be insufficient or ineffective. These recommendations align with the requirements of Appendix A, Section III(B)(1)(b)."
- **Finding**: "Testing results are presented to senior management and the Board of Directors, ensuring appropriate oversight and informed decision-making regarding any necessary remediation actions, in compliance with Appendix A, Section III(C)."

6. Implement Corrective Actions

- **Finding**: "A detailed corrective action plan has been developed based on the results of independent testing, outlining specific steps and timelines for addressing identified issues, as required by Appendix A, Section III(B)(1)(b)."
- **Finding**: "The credit union prioritizes high-risk issues in the corrective action plan to ensure that critical vulnerabilities are addressed first, demonstrating complian ce with Appendix A, Section III(B)(1)(b)."
- **Finding**: "Remediation efforts are tracked and monitored, with all corrective actions completed within the designated timeframe, ensu ring compliance with Appendix A, Section III(B)(2)."

7. Revalidate Controls After Remediation

- **Finding**: "Follow-up independent testing is conducted after corrective actions are implemented to confirm that all identified vulnerabilities h ave been remediated, in compliance with Appendix A, Section III(B)(2)."
- **Finding**: "The risk assessment is regularly updated to reflect improvements and control changes based on independent testing results, ensuring that the credit union's risk profile remains accurate, as required by Appendix A, Section III(B)(1)(a)."

8. Continuous Monitoring and Improvement

- **Finding**: "Independent testing is scheduled regularly, with high-risk areas receiving more frequent testing and lower-risk areas being tested periodically, in alignment with Appendix A, Section III(A)(2)."
- **Finding**: "Independent testing is integrated into the credit union’s continuous monitoring program, ensuring that emerging risks and vulnerabilities are detected and addressed proactively, in compliance with Appendix A, Section III(A)(5)."
- **Finding**: "The credit union regularly reviews and updates its independent testing policies and procedures to address changes in risk, technology, and regulatory requirements, ensuring continuous improvement, in accordance with Appendix A, Section III(A)(3)."

Summary of Positive Findings

- **Effective Governance**: The credit union demonstrates strong governance and oversight by involving senior management and the Board of Directors in reviewing and acting upon independent testing results.
- **Comprehensive Testing**: The credit union’s independent testing program covers all critical systems, with regular audits, vulnerability assessments, penetration tests, and follow-up testing to ensure controls are effective and risks are mitigated.
- **Timely Corrective Action**: The credit union prioritizes high-risk issues, promptly implementing corrective actions and tracking remediation progress to completion.
- **Continuous Monitoring and Adaptation**: Regular independent testing and policy reviews are part of the credit union’s continuous improvement efforts, ensuring ongo ing compliance with regulatory requirements and emerging threats.

EF

Tuesday, December 17, 2024 11:40 AM

SBIR Process for Observing the Information Security Program Testing Gap

1. Situation (S)

During the evaluation of the credit union's **Information Security Program**, it was observed that a **formal testing plan** detailing the timing, frequency, and methods (internal vs. external) for critical security testing events had **not been documented**.

2. Behavior (B)

The organization did not have an established process or documented schedule for conducting essential security assessments, including:

- Internal and external audits
- Information Security Risk Assessments
- Penetration tests
- Vulnerability Assessments
- Phishing campaigns
- On-site social engineering tests
- Firewall reviews
- Active Directory reviews
- Physical device inventories

These tests were either conducted **ad hoc** or inconsistently, with no formal documentation to guide or measure the effectiveness of the security controls.

3. Impact (I)

The lack of a formal testing plan resulted in the following:

- **Gaps in Security Posture**: Without regular testing, vulnerabilities and weaknesses may go undetected, increasing the risk of unauthorized access or data breaches.
- **Regulatory Non-Compliance**: Failure to meet the independent testing requirements outlined in **Appendix A to Part 748, Title 12** exposes the credit union to compliance violations.
- **Limited Oversight**: Senior management and the Board of Directors lack visibility into the effectiveness of security controls and overall risk exposure.
- **Inefficient Resource Allocation**: Without a clear schedule or priorities, critical areas may be overlooked, while low-risk areas may consume unnecessary time and effort.

4. Resolution (R)

To address this gap, the following actionable steps are recommended:

1. **Develop a Formal Testing Plan**:
    - Document a comprehensive **Information Security Program Testing Plan** that includes:
        - **Timing**: Define specific schedules for internal and external security tests (e.g., annual penetration tests, quarterly vulnerability scans).
        - **Frequency**: Prioritize testing high-risk areas more frequently.
        - **Methods**: Clearly outline testing methods such as audits, vulnerability scans, phishing campaigns, and social engineering.
2. **Align Testing with Risk Assessments**:
    - Tailor the testing plan to focus on critical systems and controls based on the credit union's **risk assessment**.
3. **Engage Qualified Personnel**:
    - Use independent third parties or qualified internal auditors to ensure objectivity and expertise.
4. **Document Results and Report to the Board**:
    - Record testing results, identified vulnerabilities, and remediation efforts.
    - Present findings to **senior management** and the **Board** to ensure oversight and accountability.
5. **Implement Continuous Monitoring and Improvement**:
    - Integrate testing into a **continuous monitoring program** to detect and respond to emerging threats promptly.
    - Review and update the testing plan regularly to adapt to changes in the IT environment and evolving threats.

By implementing a structured and documented testing plan, the credit union will strengthen its security posture, achieve regulatory compliance, and ensure that vulnerabilities are identified and remediated effectively.

Notes

Tuesday, September 3, 2024 1:34 PM

Summary of Findings - IPMI 2.0 RAKP Authentication Remote Password Hash Retrieval Vulnerability

Issue	Description	Severi	Likeliho	Impac	Date	Owner	Action Plan	Target	Status	Resolut	MITRE

ID		ty	od of Exploit	t	Identified			Resolution Date		ion Date	ATT&CK Tactics/Techniques
001	IPMI 2.0 RAKP Authentication Remote Password Hash Retrieval Vulnerability	Medium	Medium	High	2024-12-12	IT Operations	Leave IPMI 2.0 open to allow admin password changes every 30 days using randomly generated passwords. Implement network isolation and access controls for IPMI interfaces.	2024-12-20	In Progress		**T1003.008 - Credential Dumping: DCSync**

Tracking Template

Issue ID	Description	Severity	Likelihood of Exploit	Impact	Date Identified	Owner	Action Plan	Target Resolution Date	Status	Resolution Date	MITRE ATT&CK Tactics/Techniques
001	External sharing of calendars	Medium	Medium	Medium	2024-12-12	IT Operations	Limit permissions, explore alternatives for scheduling, disable external sharing when alternatives are implemented.	2024-03-01	In Progress		**T1592 - Gather Victim Identity Information**
002	Self-service password reset not fully enabled	Medium	Low (post-MFA/FIDO)	Medium	2024-12-12	IT Security	Pilot self-service password reset; integrate with MFA and FIDO tokens; monitor and refine after rollout.	2024-06-01	In Progress		**T1110 - Brute Force**
003	Password expiration policy enforced	High	Medium (current) / Low (post-FIDO)	High	2024-12-12	IT Security	Retain expiration temporarily; transition to "never expire" policy post-FIDO implementation.	2024-12-31	In Progress		**T1110.003 - Brute Force: Password Spraying**

Evaluation of 365 Audit Findings with Recommended Action Plan

1. Ensure 'External Sharing' of Calendars is Not Available
Evaluation:

- **Current State:** External sharing of calendars is enabled, which could expose sensitive organizational details (e.g., schedules, relationships , availability) to external parties. This presents a risk of reconnaissance attacks or targeted phishing attempts.
- **Reason for Retention:** Users currently rely on external calendar sharing for scheduling, and alternative methods are under evaluation.

Risk Assessment:

- **Likelihood of Exploit:** Medium
- **Impact:** Medium

Recommended Plan of Action:

1. **Short-Term (Immediate):**
    - Limit external calendar sharing permissions to only trusted external domains if applicable.
    - Train users on securely sharing calendar details and recognizing social engineering attempts.
    - Conduct a review of currently shared calendars to identify sensitive information.
2. **Long-Term (1-3 Months):**
    - Implement a secure alternative for scheduling that meets user needs without enabling broad external sharing.
    - Disable external sharing once the alternative is in place and tested.

2. Ensure 'Self-Service Password Reset' is Enabled for All Users
Evaluation:

- **Current State:** Self-service password reset was previously disabled due to security concerns but has now been updated. The organization plans to implement this feature alongside MFA and a FIDO token project.
- **Planned Integration:** Combining self-service password reset with stronger authentication mechanisms like MFA and FIDO tokens is a sound approach to reduce associated risks.

Risk Assessment:

- **Likelihood of Exploit:** Low (post-MFA/FIDO implementation)
- **Impact:** Medium

Recommended Plan of Action:

1. **Short-Term (1-2 Months):**
    - Begin a pilot program for self-service password reset with a small group of users.
    - Ensure integration with MFA and FIDO tokens to secure the password reset process.
    - Conduct penetration testing to identify potential vulnerabilities in the process.
2. **Long-Term (3-6 Months):**
    - Roll out self-service password reset organization-wide after pilot testing.
    - Monitor and audit reset activities for anomalies and refine policies as needed.

3. Ensure the 'Password Expiration Policy' is Set to 'Never Expire'
Evaluation:

- **Current State:** Password expiration is currently enforced. The organization plans to transition to a "never expire" policy after the completion of the FIDO token project.
- **Planned Change:** Aligning the password policy with modern security practices (e.g., use of strong, unique passwords and MFA) is a reasonable approach to enhance security without relying on periodic expiration.

Risk Assessment:

- **Likelihood of Exploit:** Medium (current) / Low (post-FIDO implementation)
- **Impact:** High

Recommended Plan of Action:

1. **Short-Term (1-3 Months):**
    - Retain password expiration but ensure password strength requirements (e.g., length, complexity) are robust.
    - Enforce MFA on all critical accounts to mitigate risks associated with compromised passwords.
2. **Long-Term (6-12 Months):**
    - Transition to "never expire" policy once FIDO tokens are implemented.
    - Train users on the importance of secure password practices and MFA.

Summary of Findings - Tracking Template

Issue ID	Description	Severity	Likelihood of Exploit	Impact	Date Identified	Owner	Action Plan	Target Resolution Date	Status	Resolution Date	MITRE ATT&CK Tactics/Techniques
001	Contact folders shared with all domains	High	Medium	High	2024-12-12	IT Operations	Restrict contact folder sharing to specific domains; audit existing sharing policies.	2024-01-15	In Progress		**T1567 - Exfiltration Over Web Service**, **T1048 - Exfiltration Over Alternative Protocol**
002	Calendar details shared with all domains	High	Medium	High	2024-12-12	IT Operations	Restrict calendar sharing to specific domains; conduct a permissions audit; train users.	2024-01-15	In Progress		**T1567 - Exfiltration Over Web Service**, **T1048 - Exfiltration Over Alternative Protocol**

Implementation Plan

MS.EXO.6.1v1 - Restrict Contact Folder Sharing

1. Sign in to the Exchange admin center.
2. Navigate to **Organization > Sharing**.
3. Select **Individual Sharing** and manage domains for existing policies.
4. Ensure **Sharing with all domains** is not enabled for contact folders.

MS.EXO.6.2v1 - Restrict Calendar Sharing

1. Sign in to the Exchange admin center.
2. Navigate to **Organization > Sharing**.
3. Manage domains under existing calendar sharing policies.
4. Ensure **Sharing with all domains** is not enabled for calendars.

valuation

Policy MS.EXO.6.1v1: Contact Folders SHALL NOT Be Shared with All Domains

Findings:

- **Current Risk:** Contact folders often contain sensitive information (e.g., email addresses, phone numbers, organizational relationships) that can be leveraged by malicious actors for reconnaissance or phishing attacks. Sharing contact folders with all domains creates a significant data exfiltration risk.
- **Rationale:** Disabling sharing with all domains limits exposure to unauthorized entities while maintaining flexibility to enable sharing for specific trusted domains.

Recommendations:

1. **Immediate Actions:**
    - Restrict contact folder sharing to specific, pre-approved domains.
    - Audit existing sharing policies to identify and remediate instances where contact folders are shared with all domains.
2. **Ongoing Actions:**
    - Regularly review sharing permissions for contact folders.
    - Monitor for unauthorized sharing configurations through automated tools.

MITRE ATT&CK TTP Mapping:

- **T1567 - Exfiltration Over Web Service:** Attackers can exfiltrate contact folder data via web-based services.
- **T1048 - Exfiltration Over Alternative Protocol:** Data exfiltration through non-standard protocols could go undetected.

Policy MS.EXO.6.2v1: Calendar Details SHALL NOT Be Shared with All Domains

Findings:

- **Current Risk:** Calendar details often include sensitive scheduling information, such as meetings, locations, and attendee names. Sharing this information broadly could allow attackers to infer organizational operations, target key personnel, or plan social engineering attacks.
- **Rationale:** Restricting calendar sharing to specific domains reduces the risk of unauthorized access while supporting legitimate business needs.

Recommendations:

1. **Immediate Actions:**
    - Restrict calendar sharing to pre-approved, trusted domains.
    - Conduct an audit of existing sharing configurations to ensure compliance with this policy.
2. **Ongoing Actions:**
    - Train users on securely sharing calendar information.
    - Use monitoring tools to detect and alert on unauthorized calendar sharing configurations.

MITRE ATT&CK TTP Mapping:

- **T1567 - Exfiltration Over Web Service:** Attackers can exfiltrate sensitive calendar information using shared web-based services.
- **T1048 - Exfiltration Over Alternative Protocol:** Calendar data exfiltration can occur through alternative protocols not actively monitored.