6.The process for tracking formal issues, exceptions, and/or corrective actions includes the following:

Friday, August 16, 2024 12:03 PM

Checklist for Stmt 6: Process for Tracking Formal Issues, Exceptions, and Corrective Actions
Aligned with Appendix A to Part 748, Title 12
This checklist outlines the process for tracking, resolving, and documenting issues, exceptions, and corrective actions as pa rt of a credit union's compliance with **Appendix A to Part 748, Title 12**. It ensures that identified risks, vulnerabilities, and control gaps are appropriately addressed, tracked, and resolved in a timely manner.

Stmt 6.1: A Process for Resolving Identified Issues, Exceptions, and/or Corrective Actions

1. Documented Process Review
- **Action:** Verify that a formal process is documented for resolving identified issues, exceptions, and corrective actions.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(d)** – A documented process is required to ensure proper handling of issues.
- **Checklist:**
  - Obtain the documented process for issue resolution.
  - Review it to ensure it includes:
    - Roles and responsibilities for handling issues.
    - Timelines and procedures for addressing issues and exceptions.
    - Steps to resolve both internal and external issues.
  - Confirm that it covers escalation procedures and authority for final approval.

2. Process Implementation
- **Action:** Evaluate how the documented process is implemented in practice and ensure adherence to it.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(d)** – The process must be properly implemented to ensure issues are resolved.
- **Checklist:**
  - Observe the issue resolution process in action.
  - Review recent logs of identified issues, exceptions, and corrective actions.
  - Ensure that issues are logged, tracked, and resolved according to the documented process.
  - Verify that all steps, from issue identification to resolution, are documented in detail.

Stmt 6.2: Methods for Tracking and Reporting Issues to Resolution

1. Tracking System Verification
- **Action:** Confirm that there is a system in place to track and report issues until they are resolved.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(c)** – A system must be in place to track issues from identification through resolution.
- **Checklist:**
  - Review the issue tracking system or tool being used.
  - Ensure it logs all critical information, including:
    - Issue description, status, and severity.
    - Assigned owner(s).
    - Deadlines and due dates.
  - Verify that the system allows for progress tracking and generates reports.

2. Reporting Mechanisms
- **Action:** Validate that there are effective reporting methods to track issue resolution and provide updates to stakeholders.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(c)** – Reporting mechanisms must ensure transparency in issue resolution.
- **Checklist:**
  - Review the methods used to report on issue resolution status to stakeholders (e.g., management, the Board).
  - Ensure that reports are accurate and provide regular updates.
  - Review sample reports for completeness and adherence to established reporting standards.
  - Confirm that critical issues are flagged and included in periodic risk reports.

Stmt 6.3: Number of Current and Historical Events or Issues

1. Event Tracking Review
- **Action:** Review the system for tracking both current and historical events or issues to ensure accuracy.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(b)** – Both current and historical issues must be tracked and documented.
- **Checklist:**
  - Obtain a report of both current and historical issues.
  - Ensure that the tracking system includes:
    - Date of issue discovery.
    - Description of the issue/event.
    - Resolution status and historical context.
  - Verify that external and internal issues are documented properly.

2. Analysis of Deviations
- **Action:** Confirm that deviations from control standards are properly documented, tracked, and analyzed.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(b)** – Significant deviations from control standards must be flagged and addressed.
- **Checklist:**
  - Review how deviations from internal control standards are categorized and analyzed.
  - Ensure that significant deviations are documented and reported.
  - Verify that corrective actions or mitigating controls are implemented for any deviation.
  - Confirm that recurring deviations are flagged for deeper analysis.

Stmt 6.4: Penetration Testing Program Characteristics

1. Penetration Testing Scope and Frequency
- **Action:** Validate that the penetration testing program defines the scope and frequency of testing to align with risk levels.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(e)** – Penetration testing must include detailed scope and frequency based on the institution's risk profile.
- **Checklist:**
  - Review documentation detailing the scope of penetration testing (e.g., attack vectors, target systems).
  - Confirm the frequency of testing aligns with the organization's risk management framework.
  - Ensure that limitations on testing (e.g., hours, excluded attack types) are clearly defined.
  - Verify that coordination with a point of contact is included in the testing program.

2. Remediation and Retrospective Requirements
- **Action:** Ensure that the penetration testing program includes a remediation process for findings and retrospective analysis of control s.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(e)** – The program must define remediation and retrospective processes for identified vulnerabilities.
- **Checklist:**
  - Review the documented remediation process for penetration testing findings.
  - Verify that remediation steps are tracked and documented.
  - Confirm that retrospective reviews are conducted to assess the effectiveness of previous tests and improvements made.
  - Ensure that findings from penetration tests are included in future risk assessments.

Stmt 6.5: Documentation of Unresolved or Accepted Issues in Risk Assessment

1. Risk Assessment Documentation
- **Action:** Confirm that unresolved or accepted issues are documented in the risk assessment.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(f)** – Unresolved or accepted issues must be reflected in the risk assessment.
- **Checklist:**
  - Review the latest risk assessment to verify it includes unresolved issues or exceptions.
  - Ensure that the risk assessment describes the impact of unresolved or accepted issues.
  - Verify that risks associated with accepted issues are clearly stated and justified.

2. Follow-Up on Documentation
- **Action:** Ensure that the risk assessment process includes regular follow-ups on unresolved issues and accepted risks.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(f)** – Follow-up mechanisms must be in place for ongoing review of unresolved risks.
- **Checklist:**
  - Confirm that there are procedures for regularly updating the risk assessment with the status of unresolved issues.
  - Verify that mechanisms are in place for periodic reviews and updates to the risk assessment.
  - Ensure that unresolved or accepted risks are revisited to determine whether additional mitigation is required.

By following this **Checklist for Stmt 6**, credit unions can ensure that they have effective processes for tracking, managing, and resolving formal issues, exceptions , and corrective actions. This alignment with **Appendix A to Part 748, Title 12** helps protect member information and strengthens overall risk management.

Issues

Thursday, September 19, 2024 11:08 AM

Stmt 6.1: A Process for Resolving Identified Issues, Exceptions, and/or Corrective Actions

1. Documented Process Review

- **Potential Finding:** Lack of a documented process for resolving identified issues, exceptions, and corrective actions.
  - **Impact:** Without formal documentation, there may be inconsistent issue resolution practices and unassigned accountability for corrective actions.
  - **Reference: Section III(B)(3)(d)** – A documented process for resolving issues is required for compliance.
- **Potential Finding:** Incomplete process documentation, missing key components such as roles, responsibilities, and timelines.
  - **Impact:** Lack of clarity in who is responsible for addressing issues, leading to delays in resolution.

2. Process Implementation

- **Potential Finding:** Process is documented but not followed in practice, with issues not being tracked, logged, or resolved systematically.
  - **Impact:** Issues could go unaddressed, leading to increased risk exposure.
  - **Reference: Section III(B)(3)(d)** – Implementation of the documented process is essential to ensure that issues are properly managed.
- **Potential Finding:** Inconsistent implementation of the issue resolution process across departments or teams.
  - **Impact:** Some teams may resolve issues promptly while others may experience delays, creating security vulnerabilities.

Stmt 6.2: Methods for Tracking and Reporting Issues to Resolution

1. Tracking System Verification

- **Potential Finding:** No system or tool in place to track issues from identification to resolution.
  - **Impact:** Issues may not be consistently tracked, making it difficult to manage and report on their resolution.
  - **Reference: Section III(B)(3)(c)** – A formal system for tracking issues is required to ensure transparency and accountability.
- **Potential Finding:** The tracking system lacks essential information, such as issue descriptions, deadlines, or responsible parties.
  - **Impact:** Incomplete records can cause confusion and delays in resolving security risks.

2. Reporting Mechanisms

- **Potential Finding:** Reports on issue resolution are not regularly generated or shared with stakeholders.
  - **Impact:** Senior management and the Board may not be aware of unresolved issues or potential risks.
  - **Reference: Section III(B)(3)(c)** – Regular reporting is necessary for transparency and effective oversight.
- **Potential Finding:** Reports lack accuracy or completeness, leading to an incomplete picture of the organization's risk posture.
  - **Impact:** This can result in unresolved issues persisting unnoticed, increasing the organization's vulnerability.

Stmt 6.3: Number of Current and Historical Events or Issues

1. Event Tracking Review

- **Potential Finding:** Current and historical issues are not documented consistently, or records are incomplete.
  - **Impact:** Inadequate tracking of past and current issues may hinder the ability to learn from previous incidents and prevent future occurrences.
  - **Reference: Section III(B)(3)(b)** – Documentation of current and historical issues is necessary for proper oversight and analysis.
- **Potential Finding:** Internal and external events are not properly distinguished or recorded.
  - **Impact:** This can lead to a lack of visibility into how external threats (e.g., third-party vulnerabilities) impact the organization.

2. Analysis of Deviations

- **Potential Finding:** Deviations from control standards are not properly categorized or documented, leading to underreported risks.
  - **Impact:** Failure to track and address significant deviations increases the likelihood of control failures.
  - **Reference: Section III(B)(3)(b)** – Deviations from control standards must be documented and addressed.
- **Potential Finding:** Repeated deviations are not flagged or addressed in a timely manner.
  - **Impact:** This can lead to a recurring weakness that might be exploited by malicious actors or lead to operational inefficiencies.

Stmt 6.4: Penetration Testing Program Characteristics

1. Penetration Testing Scope and Frequency

- **Potential Finding:** The scope of penetration testing is too narrow or does not cover critical systems and assets.
  - **Impact:** Key vulnerabilities may be missed, leaving critical systems exposed to threats.
  - **Reference: Section III(B)(3)(e)** – Penetration testing must be comprehensive, covering all relevant systems based on risk.
- **Potential Finding:** Penetration tests are not conducted at regular intervals or are not aligned with the institution's risk profile.
  - **Impact:** Infrequent testing can result in security gaps that are not detected in a timely manner.

2. Remediation and Retrospective Requirements

- **Potential Finding:** Penetration test findings are not remediated promptly or are not tracked to completion.
  - **Impact:** Unresolved vulnerabilities identified during penetration tests can leave the institution exposed to security breaches.
  - **Reference: Section III(B)(3)(e)** – Remediation of findings from penetration testing must be documented and monitored.
- **Potential Finding:** No retrospective review is conducted to evaluate the effectiveness of past penetration tests and improvements made.
  - **Impact:** Without retrospective analysis, the organization may fail to understand the effectiveness of security improvements.

Stmt 6.5: Documentation of Unresolved or Accepted Issues in Risk Assessment

1. Risk Assessment Documentation

- **Potential Finding:** Unresolved or accepted issues are not reflected in the risk assessment.
  - **Impact:** Failure to document these issues could result in a misleading risk assessment that does not accurately reflect the organization's security posture.
  - **Reference: Section III(B)(3)(f)** – Unresolved or accepted issues must be included in the risk assessment for a complete understanding of risks.
- **Potential Finding:** The risk assessment does not include an analysis of the potential impact of unresolved or accepted issues.
  - **Impact:** This may lead to an underestimation of the organization’s risk exposure, impacting decision-making.

2. Follow-Up on Documentation

- **Potential Finding:** No formal process is in place for regularly updating the risk assessment with the status of unresolved issues.
  - **Impact:** Without regular follow-up, unresolved issues may persist, leading to long-term vulnerabilities.
  - **Reference: Section III(B)(3)(f)** – A process for periodic updates to the risk assessment is essential to ensure that risks are continually reassessed.
- **Potential Finding:** Mechanisms for reviewing and updating the risk assessment do not include input from all relevant stakeholders.
  - **Impact:** Incomplete input could lead to inaccurate assessments of risks or incomplete coverage of significant issues.

General Findings Across All Statements

- **Finding:** Lack of accountability for tracking and resolving issues, leading to delays in remediation.
  - **Impact:** This can result in prolonged periods of vulnerability and increase the likelihood of a security incident.
- **Finding:** Insufficient coordination between teams (e.g., IT, security, risk management) in addressing and resolving issues.
  - **Impact:** Poor communication can lead to inconsistencies in addressing and closing out issues, potentially increasing risks.

These **potential findings** highlight areas where credit unions may face non-compliance with **Appendix A to Part 748, Title 12**. Identifying these issues is critical for maintaining the security of member information, ensuring proper risk management, and adhering to regulatory requirements. Addressing these findings through corrective actions will help reduce vulnerabilities and improve overall risk governance.

Remediation

Thursday, September 19, 2024 11:14 AM

Stmt 6.1: A Process for Resolving Identified Issues, Exceptions, and/or Corrective Actions

Finding 1: Lack of a Documented Process for Issue Resolution

- **Remediation Steps:**
    1. **Develop and document a formal issue resolution process** that includes detailed procedures for identifying, tracking, and resolving issues, exceptions, and corrective actions.
    2. **Ensure the process covers key elements** such as roles and responsibilities, timelines, and escalation procedures.
    3. **Train relevant staff** on the new process to ensure consistent understanding and implementation.

Finding 2: Process Is Not Followed in Practice

- **Remediation Steps:**
    1. **Conduct a review of current practices** to identify why the documented process is not being followed.
    2. **Implement staff training** and awareness sessions to ensure all stakeholders understand the importance of adhering to the process.
    3. **Introduce regular audits** to monitor compliance with the issue resolution process and hold teams accountable for following procedures.

Stmt 6.2: Methods for Tracking and Reporting Issues to Resolution

Finding 1: No System in Place for Tracking Issues

- **Remediation Steps:**
    1. **Implement an issue tracking system** or software solution to log, track, and manage issues from identification to resolution.
    2. **Ensure the system captures all necessary data** (issue description, owner, deadlines, status) and allows for detailed reporting.
    3. **Integrate the tracking system** into the broader risk management framework to ensure all issues are properly managed.

Finding 2: Inadequate Reporting Mechanisms

- **Remediation Steps:**
    1. **Develop a formal reporting process** to provide regular updates to relevant stakeholders on the status of open issues and corrective actions.
    2. **Create standardized reporting templates** that include key information such as issue status, resolution timelines, and potential impact.
    3. **Schedule regular reporting intervals** (e.g., monthly or quarterly) to keep senior management and the Board informed about ongoing issues and their resolution progress.

Stmt 6.3: Number of Current and Historical Events or Issues

Finding 1: Inconsistent or Incomplete Tracking of Current and Historical Issues

- **Remediation Steps:**
    1. **Conduct an audit of past and current issue records** to identify gaps in tracking and documentation.
    2. **Ensure both current and historical issues** are logged in a centralized system that tracks key details, including resolution status and historical context.
    3. **Implement periodic reviews** to ensure that all issues, internal and external, are accurately documented and managed.

Finding 2: Deviations from Control Standards Are Not Properly Documented

- **Remediation Steps:**
    1. **Develop a deviation tracking system** that flags and categorizes deviations from internal controls.
    2. **Establish a process for documenting and analyzing deviations** to ensure they are addressed and mitigated appropriately.
    3. **Ensure significant deviations are escalated** to senior management for prompt attention and corrective action.

Stmt 6.4: Penetration Testing Program Characteristics

Finding 1: The Scope of Penetration Testing Is Too Narrow

- **Remediation Steps:**
    1. **Expand the penetration testing scope** to include all critical systems, applications, and network segments, especially those handling sensitive member data.
    2. **Tailor the frequency of testing** based on the risk level of each system, ensuring high-risk areas are tested more frequently.
    3. **Ensure the testing program is regularly updated** to include new threats, technologies, and changes in the IT environment.

Finding 2: Penetration Test Findings Are Not Properly Remediated

- **Remediation Steps:**
    1. **Establish a formal remediation process** to address vulnerabilities identified during penetration tests, with specific timelines and assigned responsibilities.
    2. **Track all findings in the issue management system** and regularly report on remediation progress to senior management.
    3. **Conduct follow-up testing** after remediation to verify that the vulnerabilities have been fully resolved.

Stmt 6.5: Documentation of Unresolved or Accepted Issues in Risk Assessment

Finding 1: Unresolved or Accepted Issues Are Not Documented in the Risk Assessment

- **Remediation Steps:**
    1. **Review the risk assessment process** and ensure that unresolved or accepted issues are included as part of the documentation.
    2. **Update the risk assessment** to reflect all current unresolved or accepted risks, detailing their potential impact and justifying any accepted risks.
    3. **Create a process for regularly reviewing the status** of unresolved or accepted issues and updating the risk assessment as needed.

Finding 2: No Formal Process for Following Up on Unresolved Issues

- **Remediation Steps:**
    1. **Develop a formal follow-up process** for monitoring unresolved or accepted risks, with scheduled review dates and assigned responsibilities.
    2. **Ensure that unresolved risks** are regularly revisited and reassessed to determine whether further mitigation actions are needed.
    3. **Document follow-up actions** in the risk assessment and ensure that updates are shared with senior management and the Board.

General Remediation for All Statements

Finding: Lack of Accountability for Tracking and Resolving Issues

- **Remediation Steps:**
    1. **Assign clear ownership and accountability** for all identified issues, ensuring that responsible parties are held accountable for resolving them.
    2. **Create escalation procedures** for unresolved issues to ensure that critical risks are promptly addressed by higher levels of management.
    3. **Monitor progress regularly** through status meetings, dashboards, and automated reminders in the tracking system.

Finding: Insufficient Coordination Between Teams

- **Remediation Steps:**
    1. **Establish cross-functional teams** involving IT, risk management, internal audit, and compliance to ensure collaboration in issue resolution.

2. **Implement regular meetings** between these teams to discuss ongoing issues, exceptions, and corrective actions.
3. **Improve communication channels** through shared platforms, collaborative tools, and centralized documentation to ensure that all teams are aligned.

Compliance

Thursday, September 19, 2024 11:18 AM

To ensure compliance with **Appendix A to Part 748, Title 12**, credit unions must establish a robust process for **tracking formal issues, exceptions, and corrective actions**. This process is critical to maintaining effective oversight of the institution's information security program and safeguarding member information. Below are the **compliance steps** that credit unions should follow for tracking issues, exceptions, and corrective actions:

1. Establish a Documented Process for Issue Resolution

1.1 Develop a Formal Issue Tracking and Resolution Process

- **Action:** Document a formal process for identifying, logging, tracking, and resolving issues, exceptions, and corrective actions.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(d)** – A documented process for resolving identified issues and exceptions is required to ensure issues are addressed properly.
- **Compliance Steps:**
  - Create a written procedure that outlines how issues and exceptions are identified and escalated.
  - Include detailed steps on logging issues, assigning responsibilities, and defining resolution timelines.
  - Ensure the process includes internal controls for both proactive issue identification and reactive issue management.

1.2 Ensure Accountability and Role Assignment

- **Action:** Assign roles and responsibilities for managing, tracking, and resolving issues and corrective actions.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(d)** – Clearly defined roles ensure accountability throughout the issue resolution process.
- **Compliance Steps:**
  - Define the roles of staff responsible for logging, managing, and resolving issues.
  - Assign a central coordinator or team to oversee the issue management process.
  - Ensure that staff are trained on the process and understand their roles.

2. Implement an Issue Tracking System

2.1 Establish a Centralized Tracking System

- **Action:** Implement a centralized system for tracking all identified issues, exceptions, and corrective actions.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(c)** – A formal tracking system is necessary to monitor the status of issues and exceptions.
- **Compliance Steps:**
  - Implement a software solution or tracking tool to log and track all issues from identification through resolution.
  - Ensure the system tracks critical information such as issue descriptions, assigned owners, deadlines, status updates, and resolution steps.
  - Integrate the tracking system with other risk management processes to provide real-time updates on issue status.

2.2 Monitor Progress and Ensure Timely Resolution

- **Action:** Use the tracking system to monitor progress and ensure issues are resolved within set timelines.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(c)** – The tracking system must support timely issue resolution and reporting.
- **Compliance Steps:**
  - Establish deadlines for resolving issues based on their severity and potential impact on the security program.
  - Set up automated notifications and reminders for staff responsible for resolving issues.
  - Regularly review the status of all tracked issues to ensure they are progressing toward resolution.

3. Define Reporting and Escalation Mechanisms

3.1 Develop Reporting Mechanisms

- **Action:** Create formal reporting procedures for escalating unresolved issues and providing updates to stakeholders.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(c)** – Reporting mechanisms must be in place to provide transparency and allow for effective oversight.
- **Compliance Steps:**
  - Define the frequency and format of issue resolution reports for senior management and the Board of Directors.
  - Ensure reports include details of open, resolved, and pending issues, along with status updates, action plans, and resolution deadlines.
  - Create a reporting structure that highlights high-risk issues and tracks exceptions that could impact the credit union's risk posture.

3.2 Escalate Critical Issues

- **Action:** Establish escalation procedures for unresolved or critical issues that require higher-level attention.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(c)** – Escalation is necessary for unresolved or high-risk issues that could impact the credit union's information security.
- **Compliance Steps:**
  - Create an escalation policy to define when and how issues should be escalated to senior management or the Board.
  - Include thresholds for escalation based on the severity of the issue and its impact on the information security program.
  - Ensure that the process for escalating issues is clearly documented and communicated to relevant staff.

4. Track and Manage Exceptions

4.1 Document Exceptions to Security Controls

- **Action:** Ensure that any exceptions to security controls or processes are formally documented, reviewed, and approved.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(d)** – Exceptions must be managed with appropriate documentation and oversight to ensure they do not introduce unmitigated risks.
- **Compliance Steps:**
  - Establish a process for documenting exceptions to security controls, including justification and impact analysis.
  - Ensure that exceptions are approved by authorized personnel and that they are periodically reviewed to assess whether they should be renewed or closed.
  - Include all approved exceptions in the risk assessment and track them until they are resolved or remediated.

4.2 Assess and Approve Exceptions Based on Risk

- **Action:** Evaluate exceptions based on their potential risk to member information security and the overall risk posture of the credit union.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(d)** – Exceptions should be approved based on a risk-based analysis and documented accordingly.
- **Compliance Steps:**
  - Perform a risk analysis for each exception to assess its potential impact on the organization's security and operations.
  - Ensure the assessment includes an analysis of compensating controls to mitigate risks introduced by the exception.
  - Document the approval process and ensure that each exception has a clearly defined expiration or review date.

5. Conduct Regular Reviews and Audits

5.1 Schedule Regular Reviews of Open Issues

- **Action:** Conduct periodic reviews of all open issues, exceptions, and corrective actions to ensure they are being addressed.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(f)** – Regular reviews of unresolved or accepted issues ensure continuous monitoring and management.
- **Compliance Steps:**
  - Set up a schedule for reviewing the status of unresolved issues and exceptions, ensuring they are regularly revisited.
  - Include senior management in the review process to ensure appropriate oversight.
  - Conduct follow-up reviews to confirm that corrective actions have been implemented and are effective.

5.2 Conduct Independent Audits

- **Action:** Include the issue tracking and resolution process in independent audits to assess compliance with regulatory requirements.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(d)** – Independent audits help ensure the process is functioning effectively and in compliance with regulatory standards.
- **Compliance Steps:**
  - Include the issue tracking system in the scope of internal and external audits to assess its effectiveness.
  - Review how well the process is functioning and whether corrective actions are being completed in a timely and effective manner.
  - Address audit findings by implementing recommended improvements to the tracking process.

6. Integrate with Risk Assessment

6.1 Incorporate Unresolved or Accepted Issues in Risk Assessment

- **Action:** Ensure that unresolved or accepted issues are documented in the risk assessment, and their potential impact is considered.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(f)** – Unresolved issues and exceptions must be included in the risk assessment to provide an accurate view of the organization's risk posture.
- **Compliance Steps:**
  - Document all unresolved or accepted issues in the risk assessment and ensure they are categorized based on risk level.
  - Evaluate the potential impact of unresolved issues on member data security and overall operations.
  - Ensure that risk assessments are updated regularly to reflect the current status of open issues.

6.2 Revisit Accepted Risks Regularly

- **Action:** Conduct regular follow-ups on accepted risks to determine whether they remain acceptable or require additional mitigation.
- **Reference: Appendix A, Part 748, Title 12, Section III(B)(3)(f)** – Ongoing review of accepted risks ensures they are managed effectively.
- **Compliance Steps:**
  - Set specific review dates for all accepted risks and exceptions.
  - Ensure that risk acceptance decisions are revisited periodically based on changes in the business, technology, or threat landscape.

- Reassess whether additional compensating controls are needed or whether previously accepted risks should be mitigated.

By following these **compliance steps for tracking formal issues, exceptions, and corrective actions**, credit unions can meet the requirements of **Appendix A to Part 748, Title 12**, ensuring that issues are properly managed, risks are mitigated, and member information is protected. This structured approach helps maintain regulatory compliance, improve oversight, and enhance overall risk management.

Tools

Friday, August 16, 2024 12:08 PM

1. Issue Tracking and Management
- **Jira:** A widely used tool for issue and project tracking, particularly in Agile development environments.
- **ServiceNow:** A platform for IT service management that includes issue tracking, incident management, and workflow automation.
- **Bugzilla:** An open-source tool for bug tracking and issue management.
- **Redmine:** A flexible project management web application that includes issue tracking.
- **Asana:** A task and project management tool that also supports issue tracking.

2. Project Management
- **Trello:** A visual project management tool that uses boards, lists, and cards to manage tasks and issues.
- **Microsoft Project:** A comprehensive project management tool for scheduling, resource management, and issue tracking.
- **Basecamp:** A project management and team collaboration tool that includes to-do lists, milestone management, and issue tracking.
- **Monday.com:** A work operating system that helps teams plan, track, and manage projects and tasks.

3. Customer Relationship Management (CRM)
- **Salesforce:** A leading CRM platform that provides tools for tracking customer issues, managing support tickets, and analyzing customer interactions.
- **Zoho CRM:** A CRM tool that includes features for tracking customer issues, managing sales, and automating processes.
- **HubSpot CRM:** A CRM platform with issue tracking and customer support functionalities integrated into its sales and marketing tools.

4. Quality Management Systems (QMS)
- **ISO 9001:** A standard for quality management systems that can be supported by various software tools for tracking quality issues.
- **Sparta Systems TrackWise:** A QMS tool for managing compliance, quality issues, and regulatory requirements.
- **MasterControl:** A quality management software for tracking and managing quality issues, document control, and compliance.

5. IT Service Management (ITSM)
- **BMC Helix ITSM:** An IT service management tool that includes incident management, problem management, and change management.
- **Ivanti Service Management:** An ITSM solution for tracking issues, managing service requests, and automating workflows.
- **Cherwell:** An IT service management platform that includes issue tracking, incident management, and change management.

6. Security Incident Management
- **Splunk:** A platform for monitoring, searching, and analyzing security data and incidents.
- **Qualys:** A cloud-based tool for vulnerability management, security incident tracking, and compliance.
- **AlienVault (AT&T Cybersecurity):** A security management tool for tracking and responding to security incidents and threats.

7. Risk Management
- **RiskWatch:** A risk management tool for identifying, assessing, and tracking risks.
- **LogicManager:** A risk management platform that includes tools for tracking and managing risks, issues, and compliance.
- **RSA Archer:** A comprehensive risk management solution for tracking and managing enterprise risks and compliance issues.

8. Environmental Health and Safety (EHS)
- **Enablon:** An EHS software platform for managing safety issues, compliance, and risk management.
- **Sphera:** A tool for managing environmental, health, and safety risks, including issue tracking and compliance management.
- **Gensuite:** An EHS software solution for tracking safety issues, compliance, and incident management.

9. Financial Management
- **Oracle Financial Services Analytical Applications:** A suite of tools for managing financial operations, including tracking financial issues and discrepancies.
- **SAP ERP:** An enterprise resource planning system with modules for financial management and issue tracking.
- **QuickBooks:** An accounting software for managing financial transactions and tracking issues related to finances.

10. General Task Management
- **Todoist:** A task management tool for tracking individual tasks and issues.
- **Microsoft To Do:** A task management application for tracking personal and professional tasks and issues.
- **ClickUp:** A task management and productivity tool that includes features for issue tracking and project management.

11. Document and Workflow Management
- **DocuSign:** An electronic signature and document management tool that can be used for tracking document-related issues.
- **SharePoint:** A collaboration and document management platform that includes features for tracking issues and managing workflows.

12. Communication and Collaboration
- **Slack:** A team communication tool that integrates with various issue tracking and management systems.
- **Microsoft Teams:** A collaboration platform that includes chat, file sharing, and integration with project and issue tracking tools.

Process

Wednesday, September 18, 2024 2:46 PM

1. Issue Identification and Documentation

- **Audit Findings:** Document all issues identified during the audit, including a detailed description of each issue.
- **Categorization:** Categorize issues by type (e.g., policy violation, technical vulnerability, procedural gap).
- **Severity and Impact:** Assign a severity level (e.g., critical, high, medium, low) and assess the potential impact on the organization.

2. Tracking System

- **Use a Centralized System:** Implement a centralized tracking system, such as a GRC (Governance, Risk, and Compliance) tool, an issue tracking system (e.g ., JIRA, ServiceNow), or a dedicated audit management software.
- **Unique Identifiers:** Assign a unique identifier to each issue to facilitate tracking and reference.
- **Fields to Track:** Ensure the system captures key details, including:
    - Issue description
    - Date identified
    - Severity and impact
    - Responsible party/owner
    - Action plan
    - Target resolution date
    - Status (e.g., open, in progress, resolved, closed)

3. Metrics and KPIs

Establish metrics and KPIs to measure the progress and effectiveness of issue resolution. Key metrics may include:

- **Total Number of Issues:** Count of all identified issues.
- **Issues by Severity:** Breakdown of issues by severity level.
- **Average Time to Resolution:** Time taken to resolve issues from identification to closure.
- **Overdue Issues:** Number and percentage of issues past their target resolution date.
- **Repeat Issues:** Number of issues that have reoccurred after being resolved.
- **Compliance Rate:** Percentage of issues resolved within the agreed timeline.

4. Regular Monitoring and Reporting

- **Dashboards:** Create dashboards in the tracking system to visualize metrics and KPIs. Use graphical representations such as charts and grap hs for easy interpretation.
- **Regular Reports:** Generate regular reports (e.g., monthly, quarterly) for different stakeholders, including executive management, IT teams, and auditors.
- **Trend Analysis:** Analyze trends over time to identify recurring issues, improvements, or areas needing attention.

5. Root Cause Analysis and Action Plans

- **Root Cause Analysis:** Conduct root cause analysis for significant or recurring issues to understand the underlying causes.
- **Action Plans:** Develop and document action plans to address each issue, including specific steps, responsible parties, and timelines.

6. Accountability and Follow-Up

- **Assign Responsibility:** Assign clear ownership for each issue to ensure accountability for resolution.
- **Follow-Up:** Regularly follow up on the progress of issue resolution, providing reminders and support as needed.
- **Escalation Procedures:** Establish procedures for escalating issues that are not being addressed in a timely manner.

7. Continuous Improvement

- **Feedback Loop:** Incorporate feedback from audits and issue resolution processes to continuously improve security controls and practices.
- **Lessons Learned:** Document lessons learned from resolved issues and use them to enhance policies, procedures, and training.

Sample Tracking Template (Example Fields)

Issue ID	Description	Severity	Impact	Date Identified	Owner	Action Plan	Target Resolution Date	Status	Resolution Date
001	Weak password policy	High	Critical	2024-07-01	IT Security	Update password policy, enforce MFA	2024-07-15	In Progress	
002	Unpatched server	Medium	High	2024-07-02	IT Operations	Apply latest patches, review patch management process	2024-07-10	Closed	2024-07-08

By implementing these best practices, you can effectively track and manage issues uncovered in information security audits, e nsuring timely resolution and continuous improvement of your security

Resources

Friday, August 16, 2024 12:10 PM

Strong	Satisfactory	Less Than Satisfactory	Deficient	Critically Deficient
☐ Management takes action on IT audit findings and recommendations; ☐ Action on IT audit findings and recommendations is appropriate and timely; ☐ IT audit reviews or test management's resolution of findings and recommendations; ☐ Management consistently reports the action taken on IT audit findings or recommendations to the board of directors or audit committee.	☐ Management takes action on IT audit findings and recommendations; ☐ Action on IT audit findings and recommendations is appropriate and timely; ☐ IT audit reviews or test management's resolution of findings and recommendations; ☐ Management does not consistently report the action taken on IT audit findings or recommendations to the board of directors or audit committee.	☐ Management takes action on IT audit findings and recommendations; ☐ Action on IT audit findings and recommendations is either not appropriate or not timely; ☐ IT audit does not review or test management's resolution of findings and recommendations; ☐ Management does not report the action taken on IT audit findings or recommendations to the board of directors or audit committee.	☐ Management takes action on IT audit findings and recommendations; ☐ Action on IT audit findings and recommendations is not appropriate and not timely; ☐ IT audit does not review or test management's resolution of findings and recommendations; ☐ Management does not report the action taken on IT audit findings or recommendations to the board of directors or audit committee.	☐ Management does not take action on IT audit findings and recommendations.

Summary of Findings - Tracking Template with MITRE ATT&CK Alignment and Likelihood of Exploit

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	LDAP signing not required	Medium	High	High	2024-12-12	IT Security	Enforce LDAP signing and audit configurations regularly	2024-12-20	In Progress		**T1557.002 - Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning**
002	SMB signing not required	Medium	High	High	2024-12-12	IT Security	Require SMB signing, test configurations	2024-12-20	In Progress		**T1550.002 - Use Alternate Authentication Material: NTLM Relay**
003	IPMI 2.0 RAKP authentication vulnerability	Medium	Medium	Medium	2024-12-12	IT Operations	Restrict IPMI access; implement robust password policies	2024-12-20	In Progress		**T1003.008 - Credential Dumping: DCSync**
004	Password spraying across services (FTP, SSH, etc.)	High	High	Critical	2024-12-12	IT Security	Tune detection solutions; implement account lockout policies	2024-12-18	In Progress		**T1110.003 - Brute Force: Password Spraying**
005	Active Directory password spraying	High	High	Critical	2024-12-12	IT Security	Configure AD monitoring; implement MFA	2024-12-18	In Progress		**T1110.003 - Brute Force: Password Spraying**

Likelihood of Exploit Assessment

1. **LDAP Signing Not Required:**
   - **Likelihood:** High
   - **Reason:** Exploitation is feasible for attackers with network access to intercept and relay LDAP authentication traffic due to the lack of cryptographic signing.
2. **SMB Signing Not Required:**
   - **Likelihood:** High
   - **Reason:** NTLM relay attacks are well-documented and commonly exploited in environments where SMB signing is disabled.
3. **IPMI 2.0 Vulnerability:**
   - **Likelihood:** Medium
   - **Reason:** IPMI vulnerabilities require specific network conditions and access, but the exploitation method is publicly available.
4. **Password Spraying (Services):**
   - **Likelihood:** High
   - **Reason:** Password spraying attacks are easy to conduct using automated tools and rely on weak password policies, making them a common tactic.
5. **Password Spraying (Active Directory):**
   - **Likelihood:** High
   - **Reason:** Active Directory environments are a frequent target of password spraying, particularly when MFA is not enforced.

Conclusion:

The likelihood of exploitation for the identified issues is predominantly **High**, indicating an urgent need for mitigation. The tracking template provides actionable steps, aligned with the MITRE ATT&CK framework, to address vulnerabilities and reduce the risk of exploitation effectively.

Examiner Findings

Thursday, December 12, 2024 2:29 PM

1. Situation (S):
During the FFIEC audit, it was observed that the organization's process for tracking and resolving identified issues, exceptions, and corrective actions lacked consistency and alignment with **Appendix A, Part 748, Title 12** requirements. Logs for issues, such as vulnerability scanning results, business continuity gaps, and port security concerns, were inconsistently maintained across different systems. These gaps hindered effective resolution and proper reporting to stakeholders, including management and the Board.

2. Behavior (B):
The review identified the following patterns:
Inconsistent Documentation:
- Issue logs lacked essential details, including resolution status, timelines, assigned owners, and escalation paths.

Fragmented Tracking Systems:
- Different systems (manual logs, standalone tools) created duplication and monitoring gaps, reducing visibility.

Lack of Reporting Mechanisms:
- Reports to stakeholders were incomplete, irregular, and lacked standardized formats.

Limited Historical Context:
- Historical issues were inadequately documented, making it challenging to analyze recurring patterns or assess corrective action effectiveness.

3. Impact (I):
These behaviors led to the following consequences:
Delayed Resolution:
- Lack of ownership and follow-ups caused prolonged issue resolution timelines.

Increased Risk Exposure:
- Critical vulnerabilities and control gaps remained unresolved, exposing the organization to potential breaches or operational disruptions.

Reduced Transparency:
- Stakeholders lacked visibility into the resolution status of critical issues, undermining confidence in the organization's risk management efforts.

Missed Opportunities for Improvement:
- The absence of historical tracking prevented the identification of recurring issues and proactive risk mitigation.

4. Resolution (R):
To address these gaps, the organization should implement the following actions, aligned with **Appendix A, Part 748, Title 12**:

4.1. Documented Process Review
- **Action:** Verify that a formal process is documented for resolving identified issues, exceptions, and corrective actions.
- **Reference:** Appendix A, Part 748, Title 12, Section III(B)(3)(d).
- **Checklist:**
  - Obtain and review the documented process for issue resolution.
  - Ensure it includes:
    - Roles and responsibilities for handling issues.
    - Timelines and procedures for addressing issues and exceptions.
    - Steps for resolving internal and external issues.
    - Escalation procedures and authority for final approval.

4.2. Process Implementation
- **Action:** Evaluate how the documented process is implemented in practice and ensure adherence.
- **Reference:** Appendix A, Part 748, Title 12, Section III(B)(3)(d).
- **Checklist:**
  - Observe the issue resolution process in action.
  - Review recent logs to ensure adherence to documented processes.
  - Verify detailed documentation for issue identification, tracking, and resolution steps.

4.3. Tracking System Verification
- **Action:** Confirm that a centralized system is in place to track issues from identification to resolution.
- **Reference:** Appendix A, Part 748, Title 12, Section III(B)(3)(c).
- **Checklist:**
  - Review the issue tracking system or tool being used.
  - Ensure it logs:
    - Issue description, severity, and status.
    - Assigned owner(s).
    - Deadlines and due dates.
  - Verify that the system allows progress tracking and generates standardized reports.

4.4. Reporting Mechanisms
- **Action:** Validate that effective reporting methods are in place for issue resolution updates.
- **Reference:** Appendix A, Part 748, Title 12, Section III(B)(3)(c).
- **Checklist:**
  - Review the methods for reporting issue resolution to stakeholders.
  - Ensure reports are complete, accurate, and timely.
  - Review sample reports for adherence to reporting standards, including highlighting critical issues.

Finding: Improving Issue Tracking Using the SBIR Process

1. Situation (S):
During the FFIEC audit, it was observed that the organization's process for tracking and resolving identified issues, exceptions, and corrective actions lacked consistency and alignment with Appendix A to Part 748, Title 12 requirements. Logs of identified issues—such as vulnerability scanning results, business continuity gaps, and port security concerns—were inconsistently maintained across different systems. This inconsistency hindered proper resolution and reporting.

2. Behavior (B):
The review identified the following patterns:
- **Inconsistent Documentation:**
  Logs failed to consistently capture critical details, such as resolution status, timelines, or ownership.
- **Fragmented Tracking Systems:**
  Some issues were tracked manually, while others used disparate tools, leading to duplication and gaps in monitoring.
- **Lack of Reporting Mechanisms:**
  Reporting to stakeholders, including management and the Board, was irregular and incomplete.
- **Limited Historical Context:**
  Historical issues were inadequately documented, reducing the organization's ability to identify recurring problems or evaluate corrective action effectiveness.

3. Impact (I):
The observed behaviors led to several adverse outcomes:
- **Delayed Resolution:**
  Issues were not resolved in a timely manner due to unclear ownership or insufficient follow-ups.
- **Increased Risk Exposure:**
  Vulnerabilities and control gaps went unaddressed for extended periods, heightening the risk of breaches or operational disruptions.
- **Reduced Transparency:**
  Stakeholders lacked visibility into the status of critical issues, eroding confidence in risk management processes.
- **Missed Opportunities for Improvement:**
  The absence of historical tracking prevented identifying recurring issues or trends that could guide proactive measures.

4. Resolution (R):
To address these shortcomings, the following actionable steps are recommended:
1. **Develop and Implement a Centralized Tracking System:**
   - Use a centralized system (e.g., ticketing software or GRC tool) to log all identified issues, exceptions, and corrective actions. Ensure the system captures:
     - Issue description, status, and severity.
     - Assigned owner(s) and due dates.
     - Progress updates and resolution documentation.
2. **Formalize the Issue Resolution Process:**
   - Create a documented process that includes:
     - Clearly defined roles and responsibilities for issue resolution.
     - Timelines for addressing issues based on severity.
     - Escalation procedures for unresolved issues.
3. **Enhance Reporting Mechanisms:**
   - Develop a standardized reporting format for providing updates to management and the Board. Reports should include:
     - Status of critical issues.
     - Historical trends and recurring issues.
     - Progress on corrective actions.
4. **Conduct Regular Audits and Reviews:**
   - Schedule periodic reviews of the tracking system to ensure issues are logged, tracked, and resolved according to policy.
   - Use review findings to refine and improve the process.
5. **Integrate with Risk Assessments:**
   - Document unresolved or accepted issues in risk assessments.
   - Regularly revisit these issues to determine whether additional mitigation is necessary.

4.5. Event Tracking and Historical Context

- **Action:** Review tracking systems to ensure they document both current and historical issues accurately.
- **Reference:** Appendix A, Part 748, Title 12, Section III(B)(3)(b).
- **Checklist:**
    - Obtain reports of current and historical issues.
    - Ensure logs capture:
        - Date of discovery.
        - Description of the issue/event.
        - Resolution status and historical context.
    - Verify that deviations from control standards are flagged, analyzed, and addressed.

4.6. Integration with Risk Assessment

- **Action:** Ensure unresolved or accepted issues are included in risk assessments.
- **Reference:** Appendix A, Part 748, Title 12, Section III(B)(3)(f).
- **Checklist:**
    - Review the latest risk assessments for unresolved issues or exceptions.
    - Verify documentation of the impact and justification of accepted risks.
    - Confirm periodic updates and reassessment of unresolved issues.

Notes

Monday, September 16, 2024 4:39 PM

The validation of **Stmt 6**assessed the credit union's processes for tracking and resolving issues, exceptions, and corrective actions, ensuring alignment with **Appendix A to Part 748, Title 12**. The review included establishing a formal, documented issue resolution process with clear procedures for logging, tracking, and resolving issues, alongside defined roles and accountability for staff. The implementation and functionality of a centralized tracking system were evaluated to ensure comprehensive monitoring and timely resolution of issues. Reporting and escalation mechanisms were reviewed to provide transparency, including regular updates to senior management and the Board of Directors. Processes for documenting, assessing, and approving exceptions based on risk were validated, ensuring they were included in the risk assessment and periodically revisited. Regular reviews and audits were examined to confirm ongoing oversight and the effectiveness of corrective actions. Finally, the integration of unresolved or accepted issues into risk assessments ensures a comprehensive understanding of the organization's risk posture, supporting continuous improvement and regulatory compliance.

Summary of Findings - Tracking Template with MITRE ATT&CK Alignment and Likelihood of Exploit

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	LDAP signing not required	Medium	High	High	2024-12-12	IT Security	Enforce LDAP signing and audit configurations regularly	2024-12-20	In Progress		**T1557.002 - Adversary-in-the-Middle: LLMNR/NBT-NS Poisoning**
002	SMB signing not required	Medium	High	High	2024-12-12	IT Security	Require SMB signing, test configurations	2024-12-20	In Progress		**T1550.002 - Use Alternate Authentication Material: NTLM Relay**
003	IPMI 2.0 RAKP authentication vulnerability	Medium	Medium	Medium	2024-12-12	IT Operations	Restrict IPMI access; implement robust password policies	2024-12-20	In Progress		**T1003.008 - Credential Dumping: DCSync**
004	Password spraying across services (FTP, SSH, etc.)	High	High	Critical	2024-12-12	IT Security	Tune detection solutions; implement account lockout policies	2024-12-18	In Progress		**T1110.003 - Brute Force: Password Spraying**
005	Active Directory password spraying	High	High	Critical	2024-12-12	IT Security	Configure AD monitoring; implement MFA	2024-12-18	In Progress		**T1110.003 - Brute Force: Password Spraying**

Likelihood of Exploit Assessment

1. **LDAP Signing Not Required:**
   - **Likelihood:** High
   - **Reason:** Exploitation is feasible for attackers with network access to intercept and relay LDAP authentication traffic due to the lackof cryptographic signing.
2. **SMB Signing Not Required:**
   - **Likelihood:** High
   - **Reason:** NTLM relay attacks are well-documented and commonly exploited in environments where SMB signing is disabled.
3. **IPMI 2.0 Vulnerability:**
   - **Likelihood:** Medium
   - **Reason:** IPMI vulnerabilities require specific network conditions and access, but the exploitation method is publicly available.
4. **Password Spraying (Services):**
   - **Likelihood:** High
   - **Reason:** Password spraying attacks are easy to conduct using automated tools and rely on weak password policies, making them a commontactic.
5. **Password Spraying (Active Directory):**
   - **Likelihood:** High
   - **Reason:** Active Directory environments are a frequent target of password spraying, particularly when MFA is not enforced.

Conclusion:

The likelihood of exploitation for identified issues is assessed to guide prioritization and resource allocation for mitigation. The tracking template provides actionable steps, aligned with the MITRE ATT&CK framework, to address vulnerabilities and reduce the risk of exploitation effectively.

Evaluation of Proposed Solution for Issue 002: Manually Disabling Unused Ports

Current Solution Overview

- **Current Practice:** Ports that are not in use, particularly in public areas, are manually disabled. This reduces the risk of unauthorized access through idle or unsecured ports.
- **Planned Project:** Automating port security (e.g., configuring ports to authenticate approved devices) is considered a lower priority due to physical access requirements and the presence of other mitigating defenses.

Strengths of the Current Solution

1. **Basic Risk Mitigation:**
   - Manually disabling unused ports reduces the attack surface and prevents unauthorized devices from easily connecting to the network.
2. **Focus on High-Risk Areas:**
   - Prioritizing ports in public areas addresses the most vulnerable locations where unauthorized physical access is more likely.
3. **Defensive Depth:**
   - Other defenses (e.g., firewalls, intrusion detection/prevention systems) can provide additional layers of security, compensating for the manual approach.

Weaknesses of the Current Solution

1. **Scalability Challenges:**
   - Manually managing port security is labor-intensive and prone to human error, especially in large or dynamic environments.
   - Ports in private or less visible areas might be overlooked, leaving gaps in security.
2. **Delayed Automation:**
   - Postponing automated solutions (e.g., Network Access Control [NAC]) prolongs the risk of unauthorized access through active but unsecured ports.
3. **Physical Access Dependency:**
   - The reliance on physical access for port configuration creates operational inefficiencies and delays in implementing changes.
4. **Limited Threat Mitigation:**
   - Manual disabling does not address the risk of rogue devices connecting to ports that remain enabled or re-enabled due to oversight.

Risk Assessment

- **Likelihood of Exploit:** Medium
  - Exploitation requires physical access to the network, but unsecured ports in public areas present an attractive target for attackers.

- **Impact:** High
    - Unauthorized access via compromised ports could lead to network infiltration, lateral movement, data exfiltration, or malware installation.

Recommendations

Short-Term (Immediate):

1. **Strengthen Manual Process:**
    - Regularly audit all network ports to ensure unused ones are disabled, especially in sensitive and public areas.
    - Implement a checklist or automated logging system to track which ports are disabled and identify gaps.
2. **Increase Physical Security:**
    - Enhance physical security in public and sensitive areas to reduce the likelihood of unauthorized physical access to network ports.
    - Use tamper-evident port covers or lockable Ethernet ports in vulnerable locations.

Mid-Term (3-6 Months):

1. **Deploy Partial Automation:**
    - Begin deploying NAC solutions in high-risk areas to automate the authentication of devices connecting to the network.
    - Use VLAN segmentation to isolate unknown or unauthorized devices attempting to connect to open ports.
2. **Leverage Existing Defenses:**
    - Integrate port security with firewalls and monitoring systems to detect and alert on suspicious activity originating from network ports.

Long-Term (6-12 Months):

1. **Full Port Security Implementation:**
    - Roll out NAC or similar automated solutions across the organization to enforce device authentication consistently.
    - Configure ports to disable automatically when not in use and re-enable only after authentication.
2. **Policy and Training:**
    - Develop a formal policy for port management and train IT staff on best practices for securing network access.
3. **evised Tracking for Issue 002**

Issue ID	Description	Severity	Likelihood of Exploit	Impact	Date Identified	Owner	Action Plan	Target Resolution Date	Status	Resolution Date	MITRE ATT&CK Tactics/Techniques
002	Ethernet ports not configured to authenticate devices	High	Medium	High	2024-12-12	Network Admin	Continue manual disabling; enhance physical security; deploy NAC in high-risk areas; automate port security organization-wide.	2025-06-30	In Progress		**T1078 - Valid Accounts**, **T1070.004 - Indicator Removal on Host**

The current solution of manually disabling unused ports is a reasonable short-term measure but is not sufficient to address the scalability and effectiveness challenges in the long term. Prioritizing the implementation of automated port security solutions, starting with high-risk areas, will significantly reduce the risk of unauthorized network access while improving operational efficiency. The proposed plan balances immediate risk mitigation with long-term security enhancements.

Evaluation of Proposed Solution for Issue 003: Scheduled In-Depth Test of DNA Hosts

Current Solution Overview

- **Plan:** The organization plans to conduct a more in-depth test of its DNA hosts in October as part of its business continuity testing.
- **Objective:** The scheduled test aims to assess the resilience of critical DNA hosts and improve preparedness for potential disruptions.

Strengths of the Proposed Solution

1. **Focus on Critical Systems:**
   - Testing DNA hosts ensures that the organization's business continuity plan (BCP) addresses the most critical infrastructure components.
2. **Proactive Approach:**
   - Scheduling an in-depth test demonstrates a commitment to evaluating and improving the organization's BCP.
3. **Opportunity for Improvement:**
   - The test provides an opportunity to identify weaknesses in the current BCP and take corrective actions based on findings.

Weaknesses of the Proposed Solution

1. **Limited Scope:**
   - Focusing solely on DNA hosts may not address broader business continuity risks, such as recovery times for non-DNA systems, communication protocols, or employee preparedness.
2. **Delayed Implementation:**
   - If the test is not conducted until October, the organization remains exposed to untested scenarios for several months.
3. **Lack of Regular Testing:**
   - Conducting a single in-depth test does not meet the FFIEC guideline for regular testing of the BCP, which is typically recommended at least annually or semi-annually.
4. **Absence of Comprehensive Plan Validation:**
   - The proposed test does not explicitly include broader components such as tabletop exercises, communication protocols, or supply chain continuity.

Risk Assessment

- **Likelihood of Exploit:** Medium
  - Business disruptions (e.g., cyberattacks, natural disasters) can occur at any time, leaving the organization unprepared if testing is delayed.
- **Impact:** High
  - Without regular and comprehensive testing, gaps in the BCP may go unnoticed, leading to prolonged downtime and operational disruptions.

Recommendations

Short-Term (Before October):

1. **Interim Testing:**
   - Conduct a tabletop exercise or limited-scope simulation for non-DNA components to evaluate broader BCP readiness.
   - Focus on critical areas such as communication protocols, staff roles, and data recovery processes.
2. **Document and Address Current Gaps:**
   - Review existing BCP documentation to identify potential weaknesses that do not require in-depth testing to address.

During October Testing:

1. **Expand Scope:**
   - Include additional critical systems beyond DNA hosts to ensure the BCP is tested comprehensively.
   - Simulate real-world scenarios, such as ransomware attacks or power outages, to evaluate preparedness.
2. **Engage Key Stakeholders:**
   - Involve representatives from all relevant departments to validate cross-functional readiness.

Long-Term (Post-October):

1. **Schedule Regular Tests:**
   - Establish a schedule for annual or semi-annual business continuity testing that includes full-scale simulations, tabletop exercises, and functional recovery tests.
2. **Review and Update the BCP:**
   - Incorporate findings from the October test into the BCP and address identified gaps promptly.
   - Ensure the BCP remains aligned with FFIEC guidelines and evolving organizational needs.

3. **Revised Tracking for Issue 003**

Issue ID	Description	Severity	Likelihood of Exploit	Impact	Date Identified	Owner	Action Plan	Target Resolution Date	Status	Resolution Date	MITRE ATT&CK Tactics/Techniques
003	Business continuity testing not conducted regularly	High	Medium	High	2024-12-12	IT Operations	Conduct October test on DNA hosts; add interim tabletop exercises; schedule regular annual tests.	2024-10-31	In Progress		**T1489 - Service Stop**, **T1490 - Inhibit System Recovery**

While the scheduled October test is a positive step, relying solely on this event leaves gaps in broader business continuity preparedness. Expanding the test scope to include additional systems and conducting interim exercises before October will help address these gaps. Long-term, establishing a regular testing schedule ensures compliance with FFIEC guidelines and continuous improvement of the BCP.