Risk Assessment Checklist (Aligned with Appendix A to Part 748, Title 12)

1. Preparation and Planning
Aligned with: **Appendix A, Part II(A) and II(B)** – Information Security Program and Board Oversight

- **Define the Scope**:
  - Identify the systems, applications, processes, and **member data** included in the assessment, ensuring a focus on protecting **member information**.
  - Ensure the scope covers enterprise-wide or business unit-specific risk, including **administrative, technical, and physical safeguards**.
- **Identify Stakeholders**:
  - List relevant stakeholders, including IT, security, legal, compliance, and business units.
  - **Appendix A, Part II(A)(2)** – Include the **Board of Directors** for approval and oversight of the risk assessment and information security program.
- **Gather Documentation**:
  - Collect existing security policies, procedures, and past risk assessment reports.
  - **Appendix A, Part II(A)(3)** – Ensure documentation covers **safeguards for member data** and addresses administrative, technical, and physical measures in place to protect this information.

2. Asset Identification and Classification
Aligned with: **Appendix A, Part III(A)** – Risk Assessment

- **Identify Critical Assets**:
  - Identify and inventory all hardware, software, data, and processes, focusing on assets that contain or process **member information**.
  - **Appendix A, Part III(A)** – Prioritize protection of **member data** in the identification of critical assets.
- **Classify Assets**:
  - Determine the sensitivity and criticality of each asset (e.g., High, Medium, Low).
  - **Appendix A, Part III(A)(1)** – Include **data classification** based on the sensitivity of the information and the risks associated with unauthorized access, alteration, or destruction of **member information**.

3. Threat Identification
Aligned with: **Appendix A, Part III(A)(1) and (2)** – Identifying Potential Threats

- **Identify Internal Threats**:
  - Review potential threats from employees, contractors, or insiders, such as accidental data leakage or malicious insiders.
  - **Appendix A, Part III(A)(1)** – Focus on threats that could result in **unauthorized access to or misuse of member information**.
- **Identify External Threats**:
  - List possible threats from cybercriminals, competitors, or natural disasters, with a focus on threats targeting **member information**.
  - **Appendix A, Part III(A)(2)** – Consider cyber threats such as hacking, malware, and **advanced persistent threats** targeting **member data**.
- **Use Threat Intelligence**:
  - Incorporate threat intelligence and industry reports to identify new and evolving threats, particularly those that affect the **security of member information**.

4. Vulnerability Identification
Aligned with: **Appendix A, Part III(A)(3)** – Identifying Vulnerabilities

- **Identify Vulnerabilities in Systems**:
  - Conduct vulnerability scans and review past incident reports, with a focus on **systems that store or process member data**.
  - **Appendix A, Part III(A)(3)** – Evaluate whether existing controls are sufficient to address vulnerabilities related to **member information**.
- **Assess Process Vulnerabilities**:
  - Evaluate gaps in security policies, access controls, and data handling processes that affect **member information**.
  - **Appendix A, Part III(A)(3)** – Ensure that internal processes protect **member data** against unauthorized access or loss.
- **Review Third-Party Risks**:
  - Assess the security practices of vendors and partners who have access to **member information**.
  - **Appendix A, Part III(A)(4)** – Evaluate the risks posed by **third-party service providers**, especially those that handle sensitive **member data**.

5. Risk Analysis and Evaluation
Aligned with: **Appendix A, Part III(A)(5)** – Risk Assessment

- **Assess Likelihood**:
  - Estimate the likelihood of each identified threat exploiting a vulnerability, particularly those involving **member information**.

    - **Appendix A, Part III(A)(5)** – Use relevant data to analyze potential security risks.
- **Assess Impact**:
    - Determine the impact of each threat on critical assets, particularly the **operational, reputational, and financial impacts** related to the loss of **member data**.
    - **Appendix A, Part III(A)(5)** – Consider worst-case scenarios, such as large-scale breaches of **member information**.
- **Prioritize Risks**:
    - Use a risk matrix to rank risks, focusing on those directly affecting the security of **member information**.

6. Control Identification and Evaluation

Aligned with: **Appendix A, Part III(B)(1)** – Safeguards

- **Document Existing Controls**:
    - List current controls in place, such as **encryption, access controls, and authentication**, with a specific focus on **safeguarding member data**.
    - **Appendix A, Part III(B)(1)** – Ensure controls are in place to protect **member information** from unauthorized access or use.
- **Evaluate Control Effectiveness**:
    - Test the effectiveness of controls through audits and penetration testing.
    - **Appendix A, Part III(B)(2)** – Evaluate whether controls effectively address risks to **member information**.
- **Identify Gaps**:
    - Identify gaps where controls are insufficient or missing, prioritizing those that affect **member data security**.
    - **Appendix A, Part III(B)(2)** – Address any weaknesses that expose **member information** to risk.

7. Risk Treatment and Mitigation

Aligned with: **Appendix A, Part III(B)(2) and Part IV(A)(1)** – Risk Mitigation and Program Design

- **Identify Risk Mitigation Strategies**:
    - Develop strategies to mitigate risks, such as adding new controls or revising policies.
    - **Appendix A, Part III(B)(2)** – Include additional safeguards where needed to ensure **the security and confidentiality of member information**.
- **Develop a Risk Treatment Plan**:
    - Document mitigation strategies, with clear timelines and ownership, especially for **risks related to member data**.
    - Establish a risk appetite in policy
    - **Appendix A, Part IV(A)(1)** – Incorporate safeguards that mitigate identified risks to **member data** in a timely and effective manner.
- **Evaluate Residual Risk**:
    - Assess remaining risk after mitigation, ensuring that **residual risk to member information** is reduced to acceptable levels.
    - **Appendix A, Part IV(A)(1)** – Verify whether residual risk is acceptable or if further mitigation is necessary.

8. Monitoring and Reporting

Aligned with: **Appendix A, Part V(B)(2)** – Ongoing Monitoring

- **Establish Continuous Monitoring**:
    - Implement continuous monitoring to detect security events, particularly those affecting **member data**.
    - **Appendix A, Part V(B)(2)** – Ensure ongoing monitoring of security controls related to **member information**.
- **Report Findings**:
    - Prepare regular reports for stakeholders, including risk summaries related to **member information**.
    - **Appendix A, Part V(A)(2)** – Communicate findings to senior management and the **Board**.
- **Review and Update Regularly**:
    - Set regular intervals (e.g., quarterly or annually) to update the risk assessment, especially after changes in **IT systems or security environment**.
    - **Appendix A, Part V(A)(3)** – Ensure the program is regularly adjusted in response to changing risks to **member data**.

9. Documentation and Compliance

Aligned with: **Appendix A, Part VI(A)** – Documentation and Compliance

- **Document All Findings**:
    - Maintain records of all risks, assessments, and mitigation actions related to **member information**.
    - **Appendix A, Part VI(A)** – Ensure all findings are documented to demonstrate compliance with regulatory requirements.
- **Ensure Compliance**:
    - Cross-check the risk assessment against relevant regulations and standards (e.g., ISO 27001, NIST), ensuring alignment with **Appendix A to Part 748 and GLBA**.
    - **Appendix A, Part VI(A)** – Be prepared for audits by maintaining necessary documentation and evidence that show compliance, particularly regarding **the security of member information**.

Issues

Thursday, September 19, 2024 10:33 AM

1. Preparation and Planning

- **Potential Finding:** Incomplete definition of the scope of the risk assessment, missing critical systems, applications, or processes that handle member information.
  - **Reference: Appendix A, Part II(A) and II(B)** – Requires that the scope covers enterprise-wide risks and includes administrative, technical, and physical safeguards.
- **Potential Finding:** Failure to involve the Board of Directors in the approval and oversight of the risk assessment process.
  - **Reference: Appendix A, Part II(A)(2)** – The Board must oversee the Information Security Program and its risk assessments.
- **Potential Finding:** Lack of up-to-date security policies or incomplete documentation of past assessments.
  - **Reference: Appendix A, Part II(A)(3)** – Documentation must address safeguards for member data and cover the necessary measures to protect it.

2. Asset Identification and Classification

- **Potential Finding:** Failure to identify and inventory critical assets that store or process member information.
  - **Reference: Appendix A, Part III(A)** – Critical assets containing member information must be identified and safeguarded.
- **Potential Finding:** Inaccurate or incomplete classification of assets based on their sensitivity or criticality.
  - **Reference: Appendix A, Part III(A)(1)** – Information assets must be classified based on their importance and the risks related to unauthorized access, alteration, or destruction.

3. Threat Identification

- **Potential Finding:** Insufficient identification of internal threats, such as accidental data leakage or malicious insider activity.
  - **Reference: Appendix A, Part III(A)(1)** – The risk assessment must include internal threats that could lead to unauthorized access or misuse of member information.
- **Potential Finding:** Inadequate identification of external threats, such as cyberattacks or natural disasters.
  - **Reference: Appendix A, Part III(A)(2)** – External threats must be considered, especially those targeting member information (e.g., hacking, malware).
- **Potential Finding:** Failure to incorporate up-to-date threat intelligence into the assessment.
  - **Reference: Appendix A, Part III(A)(1) and III(A)(2)** – The risk assessment should account for emerging threats, using relevant threat intelligence.

4. Vulnerability Identification

- **Potential Finding:** Missing or outdated vulnerability scans, especially on systems that store or process member data.
  - **Reference: Appendix A, Part III(A)(3)** – Vulnerability assessments must evaluate whether existing controls sufficiently protect member information.
- **Potential Finding:** Weaknesses in internal processes, such as poor access controls or data handling procedures, that expose member information to risk.
  - **Reference: Appendix A, Part III(A)(3)** – Processes must be assessed for vulnerabilities that could lead to data loss or unauthorized access.
- **Potential Finding:** Inadequate review of third-party vendors' security practices, particularly those with access to member information.
  - **Reference: Appendix A, Part III(A)(4)** – Third-party risks must be evaluated, especially when sensitive member information is involved.

5. Risk Analysis and Evaluation

- **Potential Finding:** Failure to accurately assess the likelihood of identified threats exploiting vulnerabilities related to member information.
  - **Reference: Appendix A, Part III(A)(5)** – The assessment must estimate the likelihood of threats impacting the security of member information.
- **Potential Finding:** Inadequate assessment of the potential impact on critical assets, particularly those containing member information.
  - **Reference: Appendix A, Part III(A)(5)** – The risk assessment must include potential operational, reputational, and financial impacts of a breach.
- **Potential Finding:** Lack of prioritization of high-risk areas affecting member data security, leading to ineffective mitigation strategies.
  - **Reference: Appendix A, Part III(A)(5)** – The highest risks, especially those affecting member information, must be prioritized for mitigation.

6. Control Identification and Evaluation

- **Potential Finding:** Incomplete documentation of existing security controls or their effectiveness in safeguarding member data.
  - **Reference: Appendix A, Part III(B)(1)** – All current controls (e.g., encryption, access controls) must be documented to ensure they are effective in protecting member information.
- **Potential Finding:** Lack of regular testing or evaluation of controls (e.g., encryption, access controls) through audits or penetration testing.
  - **Reference: Appendix A, Part III(B)(2)** – The effectiveness of existing controls must be regularly evaluated, especially those protecting member data.
- **Potential Finding:** Gaps in security controls, leaving member information vulnerable to unauthorized access or loss.
  - **Reference: Appendix A, Part III(B)(2)** – Any weaknesses in controls that expose member data to risk must be addressed.

7. Risk Treatment and Mitigation

- **Potential Finding:** Lack of clear strategies for mitigating identified risks, particularly those related to member information.
  - **Reference: Appendix A, Part III(B)(2)** – Institutions must implement additional safeguards where necessary to protect member information.
- **Potential Finding:** Incomplete or unclear risk treatment plan, with missing timelines or ownership for risk mitigation actions.
  - **Reference: Appendix A, Part IV(A)(1)** – Risk mitigation strategies must be documented, with defined timelines and accountability.
- **Potential Finding:** Failure to evaluate residual risk after implementing mitigation strategies, leaving critical areas of member data at risk.
  - **Reference: Appendix A, Part IV(A)(1)** – Institutions must assess whether residual risk is acceptable and, if not, implement further mitigation.

8. Monitoring and Reporting

- **Potential Finding:** Lack of continuous monitoring of security events, particularly those involving member data.
  - **Reference: Appendix A, Part V(B)(2)** – Continuous monitoring must be in place to detect and respond to security events affecting member information.
- **Potential Finding:** Insufficient or incomplete reporting of risk assessment findings to senior management and the Board of Directors.
  - **Reference: Appendix A, Part V(A)(2)** – Risk assessment findings, particularly those related to member information, must be regularly reported to senior management and the Board.
- **Potential Finding:** Failure to regularly update the risk assessment, especially after significant changes in the IT environment or external threat landscape.
  - **Reference: Appendix A, Part V(A)(3)** – The risk assessment must be updated periodically and after significant changes to ensure ongoing protection of member information.

9. Documentation and Compliance

- **Potential Finding:** Incomplete documentation of the risk assessment process, including findings and mitigation actions.
  - **Reference: Appendix A, Part VI(A)** – All findings must be documented to demonstrate compliance with regulatory requirements.
- **Potential Finding:** Lack of alignment between the risk assessment and relevant regulatory standards (e.g., GLBA, ISO 27001).
  - **Reference: Appendix A, Part VI(A)** – Risk assessments must align with applicable regulations and standards to ensure the security of member information.

Remediation

Thursday, September 19, 2024 10:37 AM

1. Preparation and Planning

Finding: Incomplete definition of the scope of the risk assessment.

- **Remediation Steps:**
  1. **Review and expand the scope** to ensure all systems, applications, processes, and member data are included.
  2. **Conduct stakeholder meetings** to gather input on missing areas or assets.
  3. **Update the scope document** to reflect a complete, enterprise-wide assessment or specify business units and processes handling member data.

Finding: Failure to involve the Board of Directors in risk assessment approval.

- **Remediation Steps:**
  1. **Develop a formal process** for Board oversight and approval of the risk assessment.
  2. **Ensure that risk assessment results** and the overall Information Security Program are regularly presented to the Board for review and approval.
  3. **Incorporate feedback** from the Board into future risk assessments and security strategies.

Finding: Lack of up-to-date security policies or incomplete documentation.

- **Remediation Steps:**
  1. **Conduct a review of current policies and procedures** to ensure they address all areas of member data protection.
  2. **Update or create missing documentation** for security policies, ensuring it covers administrative, technical, and physical safeguards.
  3. **Implement a policy review schedule** to ensure regular updates.

2. Asset Identification and Classification

Finding: Failure to identify and inventory critical assets.

- **Remediation Steps:**
  1. **Perform a complete asset inventory audit** to identify all hardware, software, and processes handling member data.
  2. **Use asset discovery tools** and collaboration with IT, security, and operations teams to ensure all assets are accounted for.
  3. **Implement an asset management process** that ensures ongoing identification and classification of assets.

Finding: Incomplete classification of assets based on sensitivity or criticality.

- **Remediation Steps:**
  1. **Establish or update a data classification policy** that classifies assets based on the sensitivity of the information they store or process (e.g., High, Medium, Low).
  2. **Classify assets in the inventory** according to this policy, prioritizing those that store or handle member data.
  3. **Review classifications regularly** and update as necessary to ensure they reflect current business and security risks.

3. Threat Identification

Finding: Insufficient identification of internal threats.

- **Remediation Steps:**
  1. **Conduct a thorough analysis** of internal threats, including potential risks from employees, contractors, and partners.
  2. **Implement monitoring and alerting** for insider threat activities, such as unauthorized access or data leakage.
  3. **Provide internal threat awareness training** to employees to reduce accidental data breaches.

Finding: Inadequate identification of external threats.

- **Remediation Steps:**
  1. **Update the risk assessment process** to include a broader set of external threats, including cyberattacks, competitors, and natural disasters.
  2. **Incorporate third-party threat intelligence feeds** and industry reports into the risk assessment process to stay updated on evolving threats.
  3. **Conduct a threat modeling exercise** to understand how external actors could target the credit union's member data.

4. Vulnerability Identification

Finding: Missing or outdated vulnerability scans.

- **Remediation Steps:**
  1. **Schedule regular vulnerability scans** of all systems that store or process member data (e.g., quarterly or more frequently).
  2. **Conduct a comprehensive vulnerability assessment** of systems using tools like Nessus, Qualys, or others to identify weaknesses.
  3. **Address identified vulnerabilities** through patching, configuration changes, or additional controls.

Finding: Weaknesses in internal processes that expose member information.

- **Remediation Steps:**
  1. **Review and update internal security processes**, such as access control, authentication, and data handling procedures.
  2. **Conduct process audits** to identify gaps and implement stricter controls where necessary.
  3. **Provide training on secure processes** to relevant personnel.

Finding: Inadequate review of third-party vendors' security practices.

- **Remediation Steps:**
  1. **Perform a thorough review** of the security controls of all third-party vendors, focusing on those with access to member data.
  2. **Enforce contractual obligations** requiring vendors to adhere to security best practices, including regular audits.
  3. **Implement vendor risk management processes** to regularly assess vendor security postures.

5. Risk Analysis and Evaluation

Finding: Failure to assess the likelihood of identified threats exploiting vulnerabilities.

- **Remediation Steps:**
  1. **Update the risk analysis methodology** to include likelihood assessments for each threat-vulnerability pair.
  2. **Use data-driven methods** (e.g., historical incidents, threat intelligence) to evaluate the probability of attacks.
  3. **Document likelihood ratings** in the risk register for ongoing tracking.

Finding: Inadequate assessment of potential impacts on member data.

- **Remediation Steps:**
  1. **Expand the risk analysis** to include detailed impact assessments for member data breaches, considering operational, reputational, and financial effects.
  2. **Use worst-case scenario modeling** to assess the full impact of high-severity risks on member information security.
  3. **Update incident response plans** based on the impact analysis to ensure readiness for data breaches.

Finding: Lack of prioritization of high-risk areas.

- **Remediation Steps:**
  1. **Create a risk matrix** to prioritize risks based on likelihood and impact, ensuring that member data risks receive the highest priority.
  2. **Review and prioritize mitigation efforts** for high-risk areas to ensure timely implementation of additional controls.
  3. **Engage the Board and senior management** in reviewing the prioritization and approving mitigation strategies.

6. Control Identification and Evaluation

Finding: Incomplete documentation of existing security controls.

- **Remediation Steps:**
  1. **Conduct a controls inventory** to document all current administrative, technical, and physical controls in place to protect member data.
  2. **Ensure controls are documented** with details on their purpose, implementation, and effectiveness.
  3. **Align control documentation with regulatory requirements** to ensure coverage of all required areas.

Finding: Lack of regular testing or evaluation of controls.

- **Remediation Steps:**
  1. **Schedule regular audits and penetration tests** to assess the effectiveness of key security controls, especially those protecting member data.
  2. **Conduct control testing** for encryption, access control, and authentication mechanisms, ensuring they meet industry best practices.
  3. **Remediate any weaknesses identified** during the testing process and document improvements.

Finding: Gaps in security controls that expose member information.

- **Remediation Steps:**
    1. **Identify missing or weak controls** through vulnerability assessments, internal audits, and reviews of incidents.
    2. **Implement additional safeguards** such as stronger encryption, enhanced access controls, and multi-factor authentication where gaps are identified.
    3. **Monitor the effectiveness** of new controls to ensure they mitigate identified risks.

7. Risk Treatment and Mitigation

Finding: Lack of clear strategies for mitigating identified risks.

- **Remediation Steps:**
    1. **Develop risk mitigation strategies** for each identified risk, ensuring that those affecting member data receive priority.
    2. **Incorporate mitigation strategies** into the overall Information Security Program and communicate them to relevant stakeholders.
    3. **Track mitigation efforts** through a risk treatment plan, ensuring timelines and responsibilities are clearly defined.

Finding: Incomplete or unclear risk treatment plans.

- **Remediation Steps:**
    1. **Create a detailed risk treatment plan** that includes specific actions, timelines, and owners for addressing risks.
    2. **Review and update the treatment plan** regularly to reflect progress or changes in the risk environment.
    3. **Assign accountability** to senior management and stakeholders to ensure timely execution of the plan.

Finding: Failure to evaluate residual risk.

- **Remediation Steps:**
    1. **Conduct residual risk assessments** after implementing mitigation strategies to determine if further action is needed.
    2. **Document residual risk levels** and ensure they are acceptable to the organization's risk appetite.
    3. **Escalate significant residual risks** to the Board for further discussion and possible mitigation.

8. Monitoring and Reporting

Finding: Lack of continuous monitoring for security events.

- **Remediation Steps:**
    1. **Implement continuous monitoring tools** (e.g., SIEM systems) to track access and activities across critical systems containing member data.
    2. **Ensure alerts and notifications** are configured for suspicious or unauthorized activities.
    3. **Regularly review logs and incident reports** to ensure monitoring is effective and covers all critical assets.

Finding: Insufficient reporting of risk assessment findings to senior management.

- **Remediation Steps:**
    1. **Establish a regular reporting process** for communicating risk assessment findings to senior management and the Board.
    2. **Create summary reports** with clear action items, progress updates, and areas of concern.
    3. **Ensure risk assessment updates** are included in Board meetings and strategic discussions.

Finding: Failure to regularly update the risk assessment.

- **Remediation Steps:**
    1. **Schedule regular updates** (e.g., quarterly or annually) to the risk assessment, particularly after significant changes in the IT environment or securit y landscape.
    2. **Review the risk assessment** following any major incidents, acquisitions, or system changes to capture new risks.
    3. **Document changes** in the risk profile and update mitigation strategies accordingly.

9. Documentation and Compliance

Finding: Incomplete documentation of the risk assessment process.

- **Remediation Steps:**
    1. **Ensure all aspects of the risk assessment** (findings, actions, decisions) are documented, particularly those related to member data security.
    2. **Maintain records** of risk treatment, mitigation, and residual risk evaluations for audit purposes.
    3. **Conduct internal reviews** to ensure documentation meets regulatory requirements and is ready for audits.

Finding: Lack of alignment with relevant regulatory standards.

- **Remediation Steps:**
    1. **Cross-check the risk assessment** against applicable regulations (e.g., GLBA, ISO 27001, NIST) and standards to ensure compliance.
    2. **Update the risk assessment process** to address any gaps in alignment with these frameworks.
    3. **Prepare for external audits** by ensuring all documentation is complete and readily available.

By following these **remediation steps**, credit unions can address the potential findings from their risk assessment, ensuring compliance with **Appendix A to Part 748, Title 12** and enhancing the security of member information. These steps will help reduce risks, improve security controls, and ensure proper governance and oversight of the credit union's Information Security Program.

Compliance with **Appendix A to Part 748, Title 12** requires credit unions to implement a comprehensive **Risk Assessment** process as part of their overall **Information Security Program**. The goal is to protect member information and ensure that risks related to unauthorized access, data breaches, and security threats are identified, evaluated, and mitigated. Below are the compliance steps for conducting a risk assessment aligned with **Appendix A to Part 748, Title 12**.

1. Preparation and Planning

1.1 Define the Scope

- **Action:** Define the scope of the risk assessment, identifying the systems, applications, processes, and data that will be assessed, particularly those handling member information.
- **Reference: Appendix A, Part II(A)** – The risk assessment must cover all areas where member information is processed or stored, focusing on administrative, technical, and physical safeguards.

1.2 Identify Stakeholders

- **Action:** Involve key stakeholders in the risk assessment process, including IT, security, legal, compliance, and relevant business units. Include the **Board of Directors** for approval and oversight.
- **Reference: Appendix A, Part II(A)(2)** – The Board must approve and oversee the risk assessment and the overall information security program.

1.3 Gather Documentation

- **Action:** Collect and review existing security policies, procedures, and previous risk assessment reports as part of the preparation process.
- **Reference: Appendix A, Part II(A)(3)** – Ensure the documentation reflects safeguards for member information and covers administrative, technical, and physical measures.

2. Asset Identification and Classification

2.1 Identify Critical Assets

- **Action:** Identify and inventory all hardware, software, data, and processes, focusing on critical assets that store, process, or transmit member information.
- **Reference: Appendix A, Part III(A)** – Critical assets that could impact member data must be identified and safeguarded.

2.2 Classify Assets

- **Action:** Classify assets based on their sensitivity and criticality to the organization and the level of risk they present (e.g., High , Medium, Low).
- **Reference: Appendix A, Part III(A)(1)** – Assets should be classified based on the sensitivity of the information they handle, particularly member data.

3. Threat Identification

3.1 Identify Internal Threats

- **Action:** Identify potential internal threats, such as employee negligence, insider attacks, or misuse of privileges that could compromise member data.
- **Reference: Appendix A, Part III(A)(1)** – Internal threats must be considered to prevent unauthorized access to member information.

3.2 Identify External Threats

- **Action:** Identify external threats, including cybercriminals, competitors, or natural disasters, and assess how they could impact the security of member information.
- **Reference: Appendix A, Part III(A)(2)** – External threats, particularly those targeting member data (e.g., malware, hacking), must be accounted for.

3.3 Use Threat Intelligence

- **Action:** Incorporate threat intelligence and industry data to identify evolving and emerging threats, especially those affecting the credit union's security posture.
- **Reference: Appendix A, Part III(A)(2)** – The risk assessment should be informed by current threat intelligence to reflect up-to-date risk factors.

4. Vulnerability Identification

4.1 Identify Vulnerabilities in Systems

- **Action:** Conduct vulnerability scans and review past incident reports to identify vulnerabilities in systems and processes that

handle member data.
- **Reference: Appendix A, Part III(A)(3)** – Vulnerability assessments must evaluate whether existing security controls are sufficient to protect member information.

4.2 Assess Process Vulnerabilities
- **Action:** Review security policies, access controls, and data handling processes to identify any gaps or weaknesses that may expose member data.
- **Reference: Appendix A, Part III(A)(3)** – Internal processes should be evaluated for potential vulnerabilities that could lead to data breaches.

4.3 Review Third-Party Risks
- **Action:** Assess the security practices of third-party vendors and partners with access to member information to ensure they meet regulatory standards.
- **Reference: Appendix A, Part III(A)(4)** – The risks posed by third-party service providers must be included in the risk assessment.

5. Risk Analysis and Evaluation

5.1 Assess Likelihood
- **Action:** Estimate the likelihood of each identified threat exploiting a vulnerability, particularly those that could affect member dat a.
- **Reference: Appendix A, Part III(A)(5)** – The risk assessment must analyze the likelihood of threats impacting member information security.

5.2 Assess Impact
- **Action:** Evaluate the potential impact of each threat on critical assets, especially the financial, reputational, and operational consequences of a breach of member data.
- **Reference: Appendix A, Part III(A)(5)** – The impact assessment must consider worst-case scenarios involving member data breaches.

5.3 Prioritize Risks
- **Action:** Use a risk matrix or scoring system to prioritize risks based on their likelihood and impact, giving priority to risks that p ose a significant threat to member data.
- **Reference: Appendix A, Part III(A)(5)** – The highest risks to member data should be prioritized for mitigation.

6. Control Identification and Evaluation

6.1 Document Existing Controls
- **Action:** Identify and document all current security controls in place to safeguard member data, including encryption, access control, and authentication mechanisms.
- **Reference: Appendix A, Part III(B)(1)** – Security controls should be documented to ensure they protect member data from unauthorized access or use.

6.2 Evaluate Control Effectiveness
- **Action:** Test the effectiveness of these controls through audits, penetration testing, and other assessments.
- **Reference: Appendix A, Part III(B)(2)** – Regular evaluation of controls is necessary to ensure they effectively address risks to member information.

6.3 Identify Gaps
- **Action:** Identify gaps where controls are missing or insufficient, particularly those affecting the protection of member data.
- **Reference: Appendix A, Part III(B)(2)** – Any weaknesses or gaps in security controls that expose member information to risk must be addressed.

7. Risk Treatment and Mitigation

7.1 Develop Risk Mitigation Strategies
- **Action:** Create strategies to mitigate identified risks, such as implementing new security controls, updating policies, or enhancing monitoring.
- **Reference: Appendix A, Part III(B)(2)** – Risk mitigation strategies should focus on improving safeguards for member data.

7.2 Develop a Risk Treatment Plan
- **Action:** Document risk treatment plans with specific actions, timelines, and responsibilities for mitigating risks, particularly those related to member data.
- **Reference: Appendix A, Part IV(A)(1)** – A documented plan is essential for ensuring timely and effective risk mitigation.

7.3 Evaluate Residual Risk
- **Action:** Assess the residual risk after mitigation to determine if additional controls or actions are necessary to reduce risk to acceptable levels.

- **Reference: Appendix A, Part IV(A)(1)** – The remaining risk after mitigation must be evaluated to ensure it is acceptable to the credit union.

8. Monitoring and Reporting

8.1 Implement Continuous Monitoring

- **Action:** Set up continuous monitoring tools to detect security events and potential breaches, focusing on systems that handle member data.
- **Reference: Appendix A, Part V(B)(2)** – Continuous monitoring is necessary to detect and respond to security incidents affecting member information.

8.2 Report Findings to Stakeholders

- **Action:** Prepare and present regular reports on risk assessment findings, including identified risks, mitigation efforts, and ongoing monitoring results, to senior management and the Board.
- **Reference: Appendix A, Part V(A)(2)** – The Board and senior management must be regularly informed about risk assessment results and actions taken to protect member information.

8.3 Regularly Update the Risk Assessment

- **Action:** Schedule periodic updates to the risk assessment, particularly after significant changes in the IT environment, processes, or external threats.
- **Reference: Appendix A, Part V(A)(3)** – The risk assessment must be regularly updated to reflect changes in the business environment or technology landscape.

9. Documentation and Compliance

9.1 Document All Findings

- **Action:** Maintain comprehensive records of all findings, actions, and decisions related to the risk assessment, ensuring clear documentation for regulatory compliance.
- **Reference: Appendix A, Part VI(A)** – All aspects of the risk assessment must be documented to demonstrate compliance with regulatory requirements.

9.2 Ensure Alignment with Regulations

- **Action:** Cross-check the risk assessment process against relevant regulatory standards (e.g., GLBA, ISO 27001, NIST) to ensure compliance with Appendix A to Part 748 and other applicable regulations.
- **Reference: Appendix A, Part VI(A)** – Ensure that the risk assessment complies with regulatory requirements and industry standards to protect member information.

10. Board Oversight and Review

10.1 Obtain Board Approval

- **Action:** Ensure the Board reviews and approves the risk assessment process and findings, providing oversight and guidance on risk management strategies.
- **Reference: Appendix A, Part II(A)(2)** – The Board must approve and oversee the risk assessment and the overall information security program.

10.2 Engage the Board in Risk Discussions

- **Action:** Involve the Board in discussions about significant risks, mitigation strategies, and the residual risk posture, particularly those affecting member data.
- **Reference: Appendix A, Part II(A)(2)** – The Board should be actively involved in decisions related to the security and risk management of member information.

By following these **compliance steps**, credit unions can ensure that their **Risk Assessment** process aligns with the requirements of **Appendix A to Part 748, Title 12**. This will help mitigate risks, protect member information, and maintain regulatory compliance through a structured and ongoing risk management framework.

Resources

Friday, August 16, 2024 7:44 AM

Items for Review:
Verify Institution formally address the following as a part of the IT risk assessment process:

- Identification of critical service providers,
- Determination of threats, including likelihood and impact,
- Identification of inherent risk levels,
- Documentation of controls to reduce threat impact,
- Determination of the quality of controls (i.e., testing),
- Identification and evaluation of residual risk levels,
- Remediation program for unacceptable residual risk levels,
- Gathering of threat intelligence (e.g., NCU-ISAO, US-CERT, Infrared).

Strong	Satisfactory	Less Than Satisfactory	Deficient	Critically Deficient
☐ Formal IT risk assessment process includes ☐ determination of threats, including likelihood/impact; ☐ identification of inherent risk levels ☐ documentation of controls; ☐ determination of the quality of controls; ☐ identification of residual risk levels; ☐ Remediation program for unacceptable residual risk levels; ☐ identification of critical service providers; ☐ gathering of threat intelligence.	☐ Formal IT risk assessment process in place; ☐ Determination of threats, including likelihood/impact; ☐ Identification of inherent risk levels; ☐ Documentation of controls; ☐ Determination of the quality of controls; ☐ Identification of residual risk levels; ☐ Remediation program for unacceptable residual risk levels; ☐ Identification of critical service providers; ☐ No consistent gathering of threat intelligence.	☐ Formal IT risk assessment process in place; but ☐ Determination of threats, including likelihood/impact; ☐ No identification of inherent risk levels; ☐ No documentation of controls; ☐ No identification of residual risk levels; ☐ No remediation program for unacceptable residual risk levels; ☐ No determination of the quality of controls; ☐ No identification of critical service providers; ☐ No gathering of threat intelligence.	☐ IT risk assessment process is in place but not formalized; ☐ No determination of threats, including likelihood/impact; ☐ No identification of inherent risk levels; ☐ No documentation of controls; ☐ No identification of residual risk levels; ☐ No remediation program for unacceptable residual risk levels; ☐ No determination of the quality of controls; ☐ No identification of critical service providers; ☐ No gathering of threat intelligence.	☐ No IT risk assessment process in place.

Level	Description	Recommendations
0	There are no formal risk management practices.	• Pitch leadership on benefits of a formal program. • Establish risk management guidelines. • Host a risk awareness session/workshop and document the results in the risk register. • Start identifying key controls. • Report on incidents/losses.
1	The risk management processes and practices are reactive and rarely subject to accountability. Issues are addressed at a tactical level only and risk rarely gets management visibility.	• Establish the risk policy with roles/responsibilities defined. • Train key personnel. • Assess key risk scenarios. • Test key controls. • Establish key metrics. • Report on issues and action plans.
2	A complete set of risk management processes, activities and tools are applied to key risk areas according to the risk policy.	• Assess staffing needs. • Establish a risk committee. • Develop risk appetite statements. • Expand training/awareness. • Refine key metrics and expand monitoring. • Report on accepted risk.
3	The risk management process is defined with significant adoption, assessments are being updated, and there is regular reporting against risk appetite. The enterprise has a functioning risk committee that oversees the risk strategy and management process.	• Develop a risk and controls library. • Start adopting quantification methods to measure risk. • Reevaluate existing assessments. • Automate metrics.
4	The risk management process is integrated into business processes, quantitative assessments are informing decision-making, risk is reassessed based on a standard risk and controls library, and some automation is in place.	• Reevaluate the risk taxonomy. • Aggregate risk across parts of the enterprise and compare scenarios. • Automate control testing. • Expand metrics and monitoring.
5	A structured, enterprise-wide program is enforced and well-managed. Risk practices are consistent across the enterprise, including both bottom-up and top-down assessments. The risk management process is highly automated to reduce errors and inefficiencies and is quantitatively measured. There is continualreassessment of risk and inefficiencies in the program.	• Continue to invest in automation. • Calibrate risk appetite and risk models. • Clearly link risk management practices to strategy-setting.

Impact

Friday, August 16, 2024 9:42 AM

1. Define Impact Categories

- **Financial Impact:**
  - **Lost Revenue:** Calculate potential revenue loss due to downtime, service interruption, or loss of customers.
  - **Recovery Costs:** Estimate the costs associated with data recovery, system restoration, and other recovery activities.
  - **Litigation Costs:** Consider potential legal expenses, including the cost of defending against lawsuits and paying settlements or fines.
- **Operational Impact:**
  - **Downtime:** Measure the potential impact of system outages on operations, including delays in service delivery.
  - **Productivity Loss:** Assess how a threat could reduce employee productivity or disrupt business processes.
- **Reputational Impact:**
  - **Customer Trust:** Evaluate how a security breach could damage customer confidence and result in loss of business.
  - **Market Share:** Estimate the potential loss of market share due to negative publicity or customer attrition.
- **Regulatory Impact:**
  - **Fines and Penalties:** Identify potential fines or penalties from regulatory bodies due to non-compliance with data protection laws.
  - **Increased Oversight:** Assess the impact of increased regulatory scrutiny following a security incident.
- **Strategic Impact:**
  - **Long-Term Business Objectives:** Consider how a threat could derail strategic initiatives, such as expansion plans or mergers.
  - **Competitive Advantage:** Evaluate how a loss of intellectual property or other critical assets could weaken the organization's competitive position.

2. Choose a Measurement Method

- **Qualitative Measurement:**
  - **Impact Scales:** Use a predefined scale (e.g., Low, Medium, High) to categorize the impact.
  - **Scenario Analysis:** Develop scenarios where a threat is successfully exploited and assess the potential consequences.
- **Quantitative Measurement:**
  - **Monetary Valuation:** Assign a dollar value to the potential financial losses, including lost revenue, recovery costs, and legal expenses.
  - **Statistical Analysis:** Use historical data or statistical models to estimate the financial impact based on the probability of the threat occurring.
- **Hybrid Method:**
  - Combine qualitative and quantitative approaches by assigning financial values to key impact areas while also using qualitative assessments for non-monetary impacts, like reputational damage.

3. Gather Data for Impact Assessment

- **Financial Records:** Use financial statements, budget reports, and cost estimates for calculating potential monetary impacts.
- **Incident Reports:** Review past incident reports to understand the impact of similar threats.
- **Market Analysis:** Gather data on market trends, customer behavior, and competitor actions to assess potential reputational and strategic impacts.

4. Analyze the Potential Impact

- **Worst-Case Scenario Analysis:** Consider the worst possible outcome for each identified threat, and evaluate the maximum potential impact.
- **Likelihood of Impact:** Combine the impact assessment with the likelihood of threat occurrence to prioritize risks.
- **Aggregate Impact:** Calculate the total potential impact by aggregating the impact across different categories (financial, operational, reputational, etc.).

5. Document and Communicate Impact Findings

- **Impact Report:** Prepare a detailed report that includes both the qualitative and quantitative impact assessments.
- **Risk Heatmap:** Visualize the impact on a risk heatmap, where risks are plotted based on their likelihood and impact.
- **Stakeholder Communication:** Ensure that the findings are communicated to all relevant stakeholders, including executives and the board, to inform decision-making.

6. Review and Update Impact Assessment

- **Continuous Monitoring:** Regularly review and update the impact assessment to account for new threats, changes in the business environment, and emerging vulnerabilities.
- **Lessons Learned:** After any security incident, conduct a post-mortem analysis to refine the impact measurement process.

Measurement

Friday, August 16, 2024 9:44 AM

1. Qualitative Risk Measurement

Qualitative methods assess risks based on subjective criteria and descriptions rather than numerical data. They are often use d when precise data is unavailable or when a more general understanding of risk is sufficient.

- **Risk Scoring or Rating:**
  - **Low, Medium, High:** Risks are categorized into levels such as Low, Medium, or High based on their potential impact and likelihood.
  - **Impact and Likelihood Matrix:** Risks are plotted on a matrix where one axis represents likelihood (e.g., Unlikely to Certain) and the other represents impact (e.g., Insignificant to Catastrophic). Each combination results in a risk score or level.
- **Scenario Analysis:**
  - Develop hypothetical scenarios for various risks to understand potential outcomes.
  - Assess how different risks could impact the organization in different situations (e.g., a data breach leading to regulatory fines and loss of customer trust).
- **Risk Mapping:**
  - Visual tools (like heat maps) are used to represent risks graphically.
  - Risks are mapped on a grid, where the axes represent impact and likelihood, helping to prioritize risks visually.

2. Quantitative Risk Measurement

Quantitative methods involve numerical data and statistical models to assess risk, offering a more precise understanding of p otential losses.

- **Annualized Loss Expectancy (ALE):**
  - **Single Loss Expectancy (SLE):** Estimate the financial loss expected from a single occurrence of a risk event. SLE = Asset Value × Exposure Factor (percentage of asset loss).
  - **Annualized Rate of Occurrence (ARO):** Estimate the number of times a risk event is expected to occur in a year.
  - **ALE Calculation:** ALE = SLE × ARO. This method provides a monetary value of the expected annual loss due to specific risks.
- **Value at Risk (VaR):**
  - Commonly used in financial risk management, VaR estimates the potential loss in value of an asset or portfolio over a defined period for a given confidence interval.
  - VaR helps to quantify the maximum expected loss with a certain level of confidence (e.g., 95% VaR).
- **Monte Carlo Simulation:**
  - A computational algorithm that uses random sampling to estimate the probability distributions of different risk outcomes.
  - It provides a range of possible outcomes and probabilities, helping to understand the potential variability in risk.
- **Cost-Benefit Analysis:**
  - Assess the costs of implementing a security control against the potential benefits (i.e., reduction in risk).
  - Helps to determine if a control is financially justified based on the potential reduction in risk.

3. Semi-Quantitative Risk Measurement

This method blends qualitative and quantitative approaches, using numerical scales to rate qualitative assessments, which can then be used for further analysis.

- **Risk Matrix with Numerical Scoring:**
  - Use a scale (e.g., 1-5 or 1-10) to rate the impact and likelihood of risks.
  - Combine these scores to create a composite risk score that allows for ranking and prioritization.
- **Risk Indices:**
  - Create a risk index by assigning weights to different risk factors (e.g., financial impact, operational disruption, likelihood).
  - Combine these weighted factors into a single risk index that can be tracked over time.
- **Hybrid Models:**
  - Combine qualitative descriptions with quantitative data. For example, use ALE for financial risks while applying a qualitative risk matrix for operational risks.
  - This approach is useful when different types of risks require different measurement methods.

4. Other Methods

- **Delphi Technique:**
  - A structured communication technique that relies on a panel of experts. The experts provide estimates independently, and the process continues iteratively until a consensus is reached.
  - Useful for measuring risk in areas where hard data may be lacking.
- **Bow-Tie Analysis:**
  - Visual tool used to analyze the pathways from risk causes to consequences, with controls depicted as barriers in between.
  - Helps to identify the potential impact of a risk and the effectiveness of current controls.
- **Failure Mode and Effects Analysis (FMEA):**
  - Identify potential failure modes, their causes, and their effects on system operations.
  - Assign a Risk Priority Number (RPN) based on the severity, occurrence, and detection of each failure mode.

5. Hybrid Approaches

- **Combining Methods:**
  - Often, a combination of qualitative, quantitative, and semi-quantitative methods is used to gain a comprehensive understanding of risk.
  - For instance, an organization might use qualitative methods to initially identify and categorize risks, then apply quantitative methods to measure the financial impact of high-priority risks.

Choosing the Right Method:

- **Context and Data Availability:**
  - Choose qualitative methods when data is scarce or the goal is to provide a high-level overview.
  - Use quantitative methods when accurate data is available and precise measurements are needed.
- **Regulatory and Industry Requirements:**
  - Some industries or regulations may require specific risk measurement methods (e.g., financial services may require VaR calculations).

- **Resource Availability:**
  - Consider the time, expertise, and tools available. Quantitative methods may require specialized skills and tools, while qualitative methods may be more accessible.
- **Decision-Making Needs:**
  - If the goal is to make immediate decisions, simpler qualitative methods may suffice. For long-term planning and investment, more detailed quantitative analysis might be necessary.

Value at Risk

Friday, August 16, 2024 9:45 AM

What Is Value at Risk (VaR)?

Value at risk (VaR) is a statistic that quantifies the extent of possible financial losses within a firm, portfolio, or posit ion over a specific time frame. This metric is most commonly used by investment and commercial banks to determine the extent and probabilities of potential losses in their institutional portfolios.

Risk managers use VaR to measure and control the level of risk exposure. One can apply VaR calculations to specific positions or whole portfolios or use them to measure firm-wide risk exposure.

Key Takeaways

- Value at risk (VaR) is a way to quantify the risk of potential losses for a firm or an investment.
- This metric can be computed in three ways: the historical, variance-covariance, and Monte Carlo methods.
- Investment banks commonly apply VaR modeling to firm-wide risk due to the potential for independent trading desks to unintentionally expose the firm to highly correlated assets.

Understanding Value at Risk (VaR)

VaR modeling determines the potential for loss in the entity being assessed and the probability that the defined loss will oc cur. One measures VaR by assessing the amount of potential loss, the probability of occurrence for the amount of loss, and th e time frame. For example, a financial firm may determine an asset has a 3% one-month VaR of 2%, representing a 3% chance of the asset declining in value by 2% during the one-month time frame. The conversion of the 3% chance of occurrence to a daily ratio places the odds of a 2% loss at one day per month.

Using a firm-wide VaR assessment allows for the determination of the cumulative risks from aggregated positions held by different trading desks and departments within the institution. Using the data provided by VaR modeling, financial institutions can determine whether they have sufficient capital reserves in place to cover losses or whether higher-than-acceptable risks require them to reduce concentrated holdings.

VaR Methodologies

There are three main ways of computing VaR: the historical method, the variance-covariance method, and the Monte Carlo method.

Historical Method

The historical method looks at one's prior returns history and orders them from worst losses to greatest gains—following from the premise that past returns experience will inform future outcomes. See "Value at Risk (VaR) Example" below for the formula and how it's calculated.

Variance-Covariance Method

Rather than assuming that the past will inform the future, the variance-covariance method, also called the parametric method, instead assumes that gains and losses are normally distributed. This way, potential losses can be framed in terms of standard deviation events from the mean.

The variance-covariance method works best for risk measurement in which the distributions are known and reliably estimated. It is less rel iable if the sample size is very small.

Monte Carlo Method

A third approach to VaR is to conduct a Monte Carlo simulation. This technique uses computational models to simulate projected returns over hundreds or thousands of possible iterations. T hen, it takes the chances that a loss will occur—say, 5% of the time—and reveals the impact.

The Monte Carlo method can be used with a wide range of risk measurement problems and relies upon the assumption that the pro bability distribution for risk factors is known.

From <https://www.investopedia.com/terms/v/var.asp>

Power Apps | Apps

Annualized Loss Expectancy

Friday, August 16, 2024 10:59 AM

Understanding Annualized Loss Expectancy (ALE)

Annualized Loss Expectancy (ALE) is a key metric in risk management, particularly in the field of information security. It provides a quantifiable estimate of the potential annual financial loss that an organization might expect from a specific risk. ALE is a cornerstone of quantitative risk assessment and helps in making informed decisions about risk mitigation investments.

Components of ALE

ALE is calculated using two primary components:

1. **Single Loss Expectancy (SLE):**
   - **Definition:** SLE represents the financial loss expected from a single occurrence of a risk event.
   - **Calculation:** SLE = Asset Value (AV) × Exposure Factor (EF)
     - **Asset Value (AV):** The value of the asset at risk. This could be the cost to replace or repair a physical asset, or the value of data, intellectual property, etc.
     - **Exposure Factor (EF):** The percentage of the asset value that is lost if the risk event occurs. It is a measure of the extent of damage. For example, if a fire destroys 30% of a data center's capacity, the EF would be 0.3.
2. **Annualized Rate of Occurrence (ARO):**
   - **Definition:** ARO is the estimated frequency with which a specific risk event is expected to occur in a year.
   - **Determining ARO:**
     - **Historical Data:** ARO can be determined based on past occurrences of the event.
     - **Expert Judgment:** When historical data is not available, experts may estimate ARO based on industry knowledge or similar experiences.
     - **Environmental Factors:** Consideration of factors like location, industry, and the effectiveness of current controls also influences ARO.

Calculating ALE

The formula to calculate ALE is:

ALE=SLE×ARO\text{ALE} = \text{SLE} \times \text{ARO}ALE=SLE×ARO

Example Calculation of ALE

Scenario: Consider a company that has a database with customer information valued at $1,000,000. There's a risk of a data breach, which, based on expert opinion, could result in the loss of 50% of the data (EF = 0.5). Historical data and industry trends suggest that the probability of such a breach occurring in a given year is 0.1 (ARO = 0.1).

1. **Step 1: Calculate SLE**
   - Asset Value (AV): $1,000,000
   - Exposure Factor (EF): 0.5 (or 50%)
   - SLE = $1,000,000 × 0.5 = $500,000
2. **Step 2: Calculate ALE**
   - ARO: 0.1 (or once every 10 years)
   - ALE = SLE × ARO = $500,000 × 0.1 = $50,000

Interpretation: The ALE of $50,000 indicates that the company can expect an annual financial loss of $50,000 due to the potential data breach. This information can help the company decide how much to invest in risk mitigation (e.g., enhanced security controls, insurance).

Applications of ALE

1. **Risk Management Decisions:**
   - ALE helps determine the cost-effectiveness of implementing security controls. If the cost of implementing a control is less than the ALE, it might be considered a worthwhile investment.
2. **Budgeting and Resource Allocation:**
   - ALE provides a financial basis for budgeting security measures. It helps in prioritizing risks and allocating resources where they can have the most significant impact.
3. **Comparing Risks:**
   - Organizations can compare the ALE of different risks to determine which ones pose the greatest financial threat and should be addressed first.
4. **Insurance Planning:**
   - ALE can be used to determine the amount of coverage required for insurance policies, ensuring that potential losses are adequately covered.

Limitations of ALE

1. **Accuracy of Input Data:**
   - The accuracy of ALE depends on the reliability of the ARO and SLE estimates. If these inputs are based on incorrect assumptions or incomplete data, the ALE will be inaccurate.
2. **Assumes Linear Impact:**
   - ALE assumes that each occurrence of a risk event will have the same impact, which may not always be the case, especially with complex risks.
3. **Does Not Address Non-Financial Impacts:**
   - ALE focuses on financial losses and may not fully capture non-financial impacts, such as reputational damage, regulatory penalties, or loss of customer trust.
4. **Risk Interdependencies:**
   - ALE calculations typically do not account for the interdependencies between risks. In reality, one risk event can trigger or exacerbate others, leading to a cumulative effect that ALE alone may not capture.

Enhancing ALE Calculations

To make ALE more robust and reliable, consider the following enhancements:

1. **Use Monte Carlo Simulations:**
   - Incorporate Monte Carlo simulations to model a range of possible outcomes and probabilities. This can help address the uncertainty in ARO and SLE estimates.
2. **Regular Updates:**
   - Regularly update ALE calculations to reflect changes in the threat landscape, asset values, and effectiveness of security controls.
3. **Scenario Analysis:**
   - Conduct scenario analysis to understand how variations in ARO or SLE might impact ALE. This helps in preparing for worst-case scenarios.
4. **Complement with Qualitative Assessments:**
   - Use ALE in conjunction with qualitative assessments to capture a fuller picture of risk, including non-financial impacts and risk interdependencies.

Conclusion

ALE is a powerful tool for quantifying the financial risks an organization faces. When used correctly, it enables better decision-making in risk management, helping to balance the cost of security measures against potential losses. However, it's crucial to recognize its limitations and enhance its use with other risk assessment methods for a more comprehensive risk management strategy.

Threat Modeling

Friday, August 16, 2024 11:01 AM

Understanding Threat Modeling

Threat modeling is a proactive approach to identifying, understanding, and addressing potential security threats to a system. It involves systematically analyzing a system's architecture, identifying potential vulnerabilities, and evaluating the possi ble threats that could exploit these vulnerabilities. The goal of threat modeling is to anticipate and mitigate security risks before they are exploited, thereby enhancing the overall security posture of the system.

Key Components of Threat Modeling

1. **Assets:**
   - **Definition:** Anything valuable that needs protection, such as data, intellectual property, customer information, or system components.
   - **Examples:** User data, financial records, critical business applications, and servers.
2. **Attackers:**
   - **Definition:** Individuals or entities that pose a threat to the assets. Understanding the attacker's motivations, capabilities, and methods is crucial in threat modeling.
   - **Examples:** Cybercriminals, nation-state actors, disgruntled employees, or opportunistic hackers.
3. **Threats:**
   - **Definition:** Potential events or actions that could cause harm to the assets by exploiting vulnerabilities.
   - **Examples:** SQL injection, phishing attacks, distributed denial-of-service (DDoS) attacks, data breaches.
4. **Vulnerabilities:**
   - **Definition:** Weaknesses or flaws in a system that could be exploited by a threat to compromise security.
   - **Examples:** Unpatched software, weak passwords, inadequate access controls, misconfigured security settings.
5. **Mitigations:**
   - **Definition:** Security controls or countermeasures implemented to reduce or eliminate vulnerabilities and prevent threats from being realiz ed.
   - **Examples:** Encryption, firewalls, intrusion detection systems, security patches, and user education.

Threat Modeling Process

The threat modeling process typically involves the following steps:

1. **Define the Scope and Objectives:**
   - Determine the boundaries of the system or application to be modeled.
   - Set clear objectives for what the threat modeling exercise aims to achieve, such as identifying high-risk threats or understanding potential attack vectors.
2. **Identify and Prioritize Assets:**
   - List all assets within the scope and prioritize them based on their importance to the organization and the potential impact o f a security breach.
   - Consider both tangible and intangible assets.
3. **Create an Architectural Overview:**
   - Develop a high-level architecture diagram of the system, including data flow diagrams (DFDs) that show how data moves through the system.
   - Include all components such as servers, databases, APIs, and external interfaces.
4. **Identify Threats:**
   - **Use STRIDE:** One common methodology for identifying threats is the STRIDE model, which categorizes threats into six types:
     - **Spoofing:** Impersonating something or someone.
     - **Tampering:** Modifying data or code.
     - **Repudiation:** Denying actions without accountability.
     - **Information Disclosure:** Exposing sensitive information.
     - **Denial of Service (DoS):** Disrupting service availability.
     - **Elevation of Privilege:** Gaining unauthorized access.
   - **Apply Attack Trees:** Use attack trees to break down how an attacker might achieve a specific goal, mapping out the steps needed to exploit a vulne rability.
   - **Leverage Threat Libraries:** Utilize threat libraries, such as MITRE ATT&CK, to identify known threats relevant to your system or industry.
5. **Identify Vulnerabilities:**
   - Assess the system to identify existing vulnerabilities that could be exploited by the identified threats.
   - Use vulnerability scanning tools, code reviews, and penetration testing to find weaknesses.
6. **Analyze and Prioritize Threats:**
   - Evaluate the likelihood and potential impact of each identified threat.
   - Prioritize threats based on their risk level, focusing on those that could cause the most significant harm.
7. **Develop Mitigations:**
   - For each high-priority threat, develop security controls or countermeasures to reduce or eliminate the associated risk.
   - Ensure that mitigations address the root cause of the vulnerability.
8. **Validate and Iterate:**
   - Test the effectiveness of the proposed mitigations through security testing, red teaming, or penetration testing.
   - Revisit the threat model regularly, especially when there are significant changes to the system, to ensure it remains relevan t and accurate.

Threat Modeling Frameworks and Methodologies

Several frameworks and methodologies are widely used for threat modeling, each offering a different approach depending on the specific needs of the organization or system:

1. **STRIDE:**
   - **Description:** Developed by Microsoft, STRIDE is a mnemonic that stands for Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege.
   - **Use:** It helps in identifying threats based on the security properties they violate (e.g., confidentiality, integrity, availability).
2. **DREAD:**
   - **Description:** DREAD is a risk rating model used to prioritize threats based on five factors: Damage potential, Reproducibility, Exploitabil ity, Affected users, and Discoverability.
   - **Use:** DREAD provides a scoring mechanism to rank the severity of threats.
3. **Attack Trees:**
   - **Description:** Attack trees represent the paths an attacker might take to achieve a specific malicious goal. Each node in the tree represent s a potential attack step, and the leaves represent the goals.
   - **Use:** They help in visualizing and analyzing the different ways a system can be attacked.
4. **PASTA (Process for Attack Simulation and Threat Analysis):**
   - **Description:** PASTA is a risk-centric threat modeling methodology that focuses on aligning business objectives with security concerns. It involves multiple stages, from defining business objectives to modeling the system and identifying threats.
   - **Use:** PASTA is used for understanding threats in the context of the organization's business goals.
5. **OCTAVE (Operationally Critical Threat, Asset, and Vulnerability Evaluation):**
   - **Description:** OCTAVE is a risk-based threat modeling approach that focuses on organizational risk and security practices. It includes identifying critical a ssets, evaluating threats, and assessing vulnerabilities.
   - **Use:** Suitable for organizations looking to align threat modeling with enterprise risk management.
6. **LINDDUN:**
   - **Description:** LINDDUN is a privacy-focused threat modeling methodology. The acronym stands for Linkability, Identifiability, Non-repudiation, Detectability, Disclosure of information, Unawareness, and Non-compliance.
   - **Use:** LINDDUN is used for identifying and mitigating privacy threats in systems.
7. **VAST (Visual, Agile, and Simple Threat):**
   - **Description:** VAST is a threat modeling methodology that integrates with Agile development processes and provides visual representations fo r both developers and security teams.
   - **Use:** It supports scalable threat modeling in large organizations with multiple development teams.

Tools for Threat Modeling

Several tools can assist in automating and streamlining the threat modeling process:

1. **Microsoft Threat Modeling Tool:**
   - A free tool from Microsoft that helps create DFDs and identify threats using the STRIDE methodology.
2. **OWASP Threat Dragon:**
   - An open-source tool that provides a web-based platform for creating threat models and identifying threats using STRIDE.
3. **ThreatModeler:**
   - A commercial tool that automates the creation of threat models and integrates with DevSecOps pipelines.
4. **IriusRisk:**
   - A platform that facilitates automated threat modeling and security requirement generation, integrating with various developme nt tools.
5. **Trike:**
   - An open-source tool focused on risk management and providing a framework for threat modeling and risk assessment.

Benefits of Threat Modeling

- **Proactive Risk Management:** Threat modeling allows organizations to identify and mitigate potential threats before they can be exploited, reducing the ov erall risk.
- **Improved Security Design:** By understanding the threats and vulnerabilities during the design phase, organizations can build more secure systems from th e ground up.
- **Resource Allocation:** Threat modeling helps prioritize security investments based on risk, ensuring resources are allocated to the most critical ar eas.
- **Compliance and Auditing:** Many regulatory frameworks require organizations to perform regular threat assessments. Threat modeling provides a structured approach to meeting these requirements.
- **Enhanced Communication:** The process fosters collaboration between development, security, and business teams, ensuring a shared understanding of risks and security priorities.

Challenges in Threat Modeling

- **Complexity:** Large and complex systems can be challenging to model comprehensively, requiring significant time and expertise.
- **Evolving Threat Landscape:** Threats continuously evolve, requiring ongoing updates to the threat model to remain relevant.
- **Integration with Development Processes:** Integrating threat modeling with Agile or DevOps processes can be difficult without disrupting workflows.
- **Accuracy of Predictions:** The effectiveness of threat modeling depends on the accuracy of assumptions and predictions, which can be difficult to valida te.

Conclusion

Threat modeling is an essential practice for identifying, understanding, and mitigating potential security threats. By adopti ng a structured approach, organizations can build more resilient systems, reduce the likelihood of successful attacks, and en sure that security measures are aligned with business objectives. Although it presents challenges, the benefits of proactive threat management far outweigh the difficulties, making it a critical component of any robust secur ity strategy.

PASTA

Friday, August 16, 2024 11:02 AM

The **Process for Attack Simulation and Threat Analysis (PASTA)** is a risk-centric threat modeling methodology designed to align technical security analysis with business objectives. It provides a structured approach to identifying, analyzing, and prioritizing threats, ultimately helping organizations to mitigate risks effectively. Here are the key benefits of adopting the PASTA methodology:

1. Alignment with Business Objectives
- **Business-Centric Approach:** PASTA explicitly aligns security measures with business objectives and risk appetites, ensuring that the identified threats a nd corresponding mitigations are relevant to the organization's overall goals.
- **Risk Prioritization:** By focusing on business impact, PASTA helps organizations prioritize threats that could cause the most significant disruption to operations, financial performance, or reputation.

2. Comprehensive Threat Analysis
- **Multiple Perspectives:** PASTA considers threats from various perspectives, including the attacker's point of view, which helps in understanding the m otivations, tactics, and techniques that might be used against the system.
- **Layered Security Assessment:** The methodology looks at threats across multiple layers, including business, application, and infrastructure levels, providin g a thorough understanding of where vulnerabilities may exist.

3. Simulation of Real-World Attacks
- **Attack Simulation:** PASTA involves simulating potential attack scenarios, allowing organizations to see how their systems would fare against real -world threats. This simulation helps in identifying weaknesses that might not be evident through other methods.
- **Threat Scenarios:** It creates realistic attack scenarios that can help security teams anticipate potential threats and prepare appropriate respo nses.

4. Scalability and Flexibility
- **Adaptable Framework:** PASTA can be tailored to fit different organizational sizes, industries, and levels of complexity, making it a versatile appr oach suitable for various environments.
- **Iterative Process:** The methodology supports continuous improvement, allowing for regular updates and refinements as new threats emerge or as the system evolves.

5. Enhanced Communication and Collaboration
- **Cross-Functional Collaboration:** PASTA encourages collaboration between different teams, including business, security, and IT. This cross -functional approach ensures that all relevant stakeholders are involved in the threat modeling process.
- **Common Language:** By focusing on risk and business impact, PASTA helps bridge the communication gap between technical and non -technical stakeholders, making security considerations more accessible to business leaders.

6. Proactive Risk Management
- **Early Identification of Risks:** By integrating threat modeling early in the development lifecycle, PASTA enables the early identification and mitigation of r isks, reducing the likelihood of vulnerabilities being exploited.
- **Continuous Monitoring:** The iterative nature of PASTA supports ongoing risk assessment and threat monitoring, helping organizations stay ahead of evo lving threats.

7. Improved Decision-Making
- **Data-Driven Decisions:** PASTA provides a structured, data-driven approach to risk assessment, allowing decision-makers to evaluate threats and security investments based on quantifiable metrics.
- **Cost-Effective Security Investments:** By focusing on the most critical threats and aligning them with business priorities, PASTA helps organizations allocate resou rces more effectively, ensuring that security investments deliver maximum value.

8. Regulatory Compliance
- **Structured Process:** PASTA's structured approach to threat modeling can help organizations meet regulatory requirements related to risk assessment and management, particularly in industries with strict compliance obligations, such as finance, healthcare, and critical infr astructure.
- **Audit Readiness:** The detailed documentation and analysis provided by PASTA can be useful in audits and compliance reviews, demonstrating that the organization has a robust risk management process in place.

9. Enhanced Security Posture
- **Holistic Risk View:** PASTA provides a comprehensive view of the organization's risk landscape, enabling a more effective and holistic approach to security.
- **Focus on Mitigation:** By identifying high-priority threats and suggesting targeted mitigations, PASTA helps strengthen the organization's overall security posture agai nst potential attacks.

Conclusion

PASTA offers numerous benefits that make it a valuable methodology for organizations seeking to enhance their security through structured, business-aligned threat modeling. By focusing on both technical and business aspects, PASTA enables more effective risk management, ensuring that security measures are both relevant and impactful. This comprehensive approach not only helps in mitigating existing threats but also prepares organizations to anticipate and respond to future challenges.

PASTA Vs STRIDE

Friday, August 16, 2024 11:03 AM

PASTA (Process for Attack Simulation and Threat Analysis) and **STRIDE** are two distinct threat modeling methodologies, each with its own focus, approach, and use cases. Below is a comparative analysis of PASTA and STRIDE:

1. Focus and Objectives

- **PASTA:**
  - **Business-Centric:** PASTA is a risk-centric threat modeling methodology that focuses on aligning security efforts with business objectives and assessing risks from a business impact perspective. The primary goal is to prioritize threats based on their potential impact on business operations, financial performance, and reputation.
  - **Comprehensive:** PASTA emphasizes understanding the entire attack surface, including business processes, application layers, and infrastructure, to create a holistic view of potential threats.
- **STRIDE:**
  - **Security Property-Centric:** STRIDE is a threat modeling framework that focuses on identifying threats based on specific security properties: Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, and Elevation of Privilege. The primary goal is to ensure that each of these security properties is protected against potential threats.
  - **Technical:** STRIDE is more technical and is often used to identify and address security issues within the design and architecture of software systems.

2. Methodology and Process

- **PASTA:**
  - **Stages:** PASTA is a seven-stage process that includes defining business objectives, creating a detailed architecture diagram, identifying potential threats, simulating attacks, and assessing risks based on business impact.
  - **Iterative and Scalable:** The process is iterative, meaning it can be revisited as the system evolves, and it is scalable to fit different organizational needs.
- **STRIDE:**
  - **Threat Identification:** STRIDE is a threat enumeration framework that helps teams systematically identify potential threats to a system by analyzing different components of the system architecture (e.g., processes, data flows, data stores, and external entities).
  - **Direct Mapping:** Each of the six categories in STRIDE corresponds to a specific type of threat, making it straightforward to map potential security issues to the corresponding threat type.

3. Output and Deliverables

- **PASTA:**
  - **Risk-Centric Reports:** The output of PASTA is typically a detailed risk report that outlines the potential business impact of identified threats, prioritized by their severity and likelihood. This report includes recommended mitigation strategies aligned with business goals.
  - **Attack Scenarios:** PASTA often generates simulated attack scenarios that illustrate how threats could be realized in the real world.
- **STRIDE:**
  - **Threats List:** The primary output of STRIDE is a list of threats categorized by the STRIDE model. This list helps in understanding which security properties are at risk and where mitigations need to be applied.
  - **Mitigation Strategies:** STRIDE typically results in a set of security controls or design changes aimed at addressing the identified threats.

4. Complexity and Usability

- **PASTA:**
  - **Complex and Detailed:** PASTA is a more complex and detailed methodology that requires a significant understanding of both the business context and technical architecture. It is often used in larger organizations with mature security processes.
  - **Cross-Functional Involvement:** Due to its comprehensive nature, PASTA requires the involvement of multiple stakeholders, including business leaders, security experts, and IT professionals.
- **STRIDE:**
  - **Simpler and Focused:** STRIDE is simpler and more focused on technical aspects, making it easier to use in smaller projects or as part of the software development lifecycle. It is widely used by development teams and security professionals to address security concerns during design and development.
  - **Primarily Technical Audience:** STRIDE is often used by security architects, developers, and technical teams who are responsible for ensuring the security of system components.

5. Use Cases

- **PASTA:**
  - **Enterprise-Level Risk Management:** PASTA is well-suited for organizations looking to integrate security risk management with broader business risk management practices. It is particularly effective for complex systems with multiple layers and interdependencies.
  - **Proactive Security Strategy:** PASTA is useful for organizations that want to take a proactive approach to security by anticipating and simulating potential attacks before they occur.
- **STRIDE:**
  - **Software Development:** STRIDE is commonly used in the software development lifecycle (SDLC) to identify and mitigate security threats during the design and architecture phases. It is particularly useful in projects where security needs to be built into the system from the ground up.
  - **Component-Level Analysis:** STRIDE is effective for analyzing specific components of a system, such as a particular application or service, to ensure that it meets security requirements.

6. Flexibility and Adaptability

- **PASTA:**
  - **Flexible and Adaptable:** PASTA can be tailored to fit the specific needs of an organization, considering both technical and business contexts. It can be applied to various industries and different types of systems, including cloud-based and hybrid environments.
  - **Broad Scope:** The methodology's flexibility makes it suitable for a wide range of threat scenarios, from strategic (business-level) to operational (technical-level).
- **STRIDE:**
  - **Specific and Prescriptive:** STRIDE is more prescriptive, with a clear focus on specific threat types. While it is highly effective for its intended use cases, it may not provide the same level of flexibility or breadth as PASTA.
  - **Narrower Scope:** STRIDE is typically applied to specific systems or components, making it less adaptable to broader, organization-wide threat modeling efforts.

7. Integration with Other Processes

- **PASTA:**
  - **Integration with Risk Management:** PASTA is designed to integrate seamlessly with enterprise risk management processes, making it easier to communicate security risks in a language that business stakeholders understand.
  - **Support for Compliance:** Due to its comprehensive nature, PASTA can help organizations meet regulatory and compliance requirements by providing a thorough assessment of security risks.
- **STRIDE:**
  - **Integration with SDLC:** STRIDE is well-integrated with the software development lifecycle, making it a popular choice for developers and security teams working on system design and implementation.
  - **Complementary Use:** STRIDE can be used alongside other methodologies or tools for a more comprehensive threat modeling approach, particularly in projects where technical security is a primary concern.

Conclusion

PASTA and **STRIDE** serve different purposes within the realm of threat modeling, and the choice between them depends on the specific needs of the organization or project.

- **PASTA** is ideal for organizations seeking a comprehensive, risk-focused approach that aligns security with business objectives and provides a holistic view of threats across multiple layers. It's suited for complex systems where understanding the broader impact of threats is crucial.
- **STRIDE**, on the other hand, is more suitable for teams focused on identifying and mitigating specific security threats during the design and development of systems. Its technical focus makes it a powerful tool for ensuring that security properties are preserved in software and system components.

In practice, these methodologies can be complementary. Organizations might use STRIDE during the early stages of system design and development, and later apply PASTA to assess broader business risks and simulate potential attack scenarios as the system evolves.

Comments

Thursday, September 26, 2024 12:59 PM

1. Preparation and Planning

- **Finding**: "The risk assessment scope has been clearly defined to cover all systems, applications, processes, and data that handle member information. This ensures that the assessment comprehensively addresses both administrative, technical, and physical safeguards, as required by Appendix A, Part II(A)."
- **Finding**: "Key stakeholders, including IT, security, legal, compliance, and business units, have been actively involved in the risk assessment process, and the Board of Directors has approved and provided oversight, in compliance with Appendix A, Part II(A)(2)."

2. Asset Identification and Classification

- **Finding**: "The credit union has successfully identified and inventoried all critical assets, including hardware, software, and data processes that store or transmit member information. The asset classification reflects the sensitivity and criticality of these assets, ensuring that the highest priority is placed on safeguarding member data, in line with Appendix A, Part III(A)."
- **Finding**: "Assets are classified based on risk levels (High, Medium, Low), allowing the credit union to focus security efforts on the most sensitive information, as required by Appendix A, Part III(A)(1)."

3. Threat Identification

- **Finding**: "The risk assessment thoroughly identifies both internal and external threats, including employee negligence, insider threats, cyberattacks, and natural disasters. The credit union has incorporated current threat intelligence to ensure that the most up-to-date threats are considered, meeting the expectations of Appendix A, Part III(A)(1) and Part III(A)(2)."
- **Finding**: "The use of threat intelligence and industry data to identify emerging risks enhances the credit union’s preparedness for evolving cybersecurity threats, in compliance with Appendix A, Part III(A)(2)."

4. Vulnerability Identification

- **Finding**: "Regular vulnerability scans and reviews of past incident reports have been conducted to identify weaknesses in systems and processes. The risk assessment has identified both technical and process-related vulnerabilities, ensuring comprehensive risk mitigation, as outlined in Appendix A, Part III(A)(3)."
- **Finding**: "Third-party vendor security practices have been evaluated, and the risks posed by these service providers have been fully incorporated into the risk assessment, ensuring compliance with Appendix A, Part III(A)(4)."

5. Risk Analysis and Evaluation

- **Finding**: "The likelihood and potential impact of threats to member information have been carefully assessed. A risk matrix was used to prioritize risks based on likelihood and impact, ensuring that the highest-risk areas receive immediate attention, in compliance with Appendix A, Part III(A)(5)."
- **Finding**: "Impact assessments include potential financial, reputational, and operational consequences, with worst-case scenarios for member data breaches considered. This allows the credit union to prioritize resources effectively, as required by Appendix A, Part III(A)(5)."

6. Control Identification and Evaluation

- **Finding**: "The risk assessment process has documented all existing security controls, including encryption, access controls, and monitoring systems. Regular audits and penetration tests confirm the effectiveness of these controls, demonstrating compliance with Appendix A, Part III(B)(1) and Part III(B)(2)."
- **Finding**: "Identified gaps in controls, especially those impacting member data security, have been addressed with clear remediation plans, ensuring a proactive approach to mitigating risks as required by Appendix A, Part III(B)(2)."

7. Risk Treatment and Mitigation

- **Finding**: "Risk mitigation strategies have been developed for all identified risks, with a focus on implementing additional security controls, updating policies, and enhancing monitoring. A risk treatment plan with specific actions and timelines has been established, ensuring compliance with Appendix A, Part IV(A)(1)."
- **Finding**: "Residual risks have been assessed after mitigation efforts, ensuring that any remaining risk is within acceptable levels. Additional controls have been implemented where necessary to reduce risk, in accordance with Appendix A, Part IV(A)(1)."

8. Monitoring and Reporting

- **Finding**: "The credit union has implemented continuous monitoring tools to detect security events and breaches, particularly for systems that handle member data. This ensures timely detection and response, meeting the requirements of Appendix A, Part V(B)(2)."
- **Finding**: "Regular reports on risk assessment findings, mitigation efforts, and ongoing monitoring results are presented to senior management and the Board of Directors. This provides continuous oversight and aligns with the requirements of Appendix A, Part V(A)(2)."

9. Documentation and Compliance

- **Finding**: "All aspects of the risk assessment process have been thoroughly documented, ensuring that findings, actions, and decisions are available for regulatory review. This clear documentation demonstrates compliance with Appendix A, Part VI(A)."
- **Finding**: "The risk assessment process has been cross-checked against relevant regulatory standards, including GLBA, NIST, and ISO 27001, ensuring full alignment with Appendix A to Part 748 and other applicable regulations, as required by Appendix A, Part VI(A)."

10. Board Oversight and Review

- **Finding**: "The Board of Directors has reviewed and approved the risk assessment process and findings, providing oversight and guidance on risk mitigation strategies. This demonstrates compliance with Appendix A, Part II(A)(2)."
- **Finding**: "The Board is actively engaged in discussions regarding significant risks, mitigation strategies, and residual risks, ensuring ongoing governance and risk management in line with Appendix A, Part II(A)(2)."

Notes

Tuesday, September 3, 2024 7:04 AM

Risk assessment process. NIST CSF, NIST 800-30, Mitre Attack model. Using ACET as a tool but they not have an IS program document and a draft Risk Assessment. Will start the assessment as the process is implemented. Completed the pen testing report. Same Scope. Currently negotiating a Pen test team (red team test). Will be conducting a ransomware scenario. GT Risk Assessment, 2nd line NIST CEF assessment. GT IAM/PAM Assessment. Expensive for PCI DSS Compliance. Pretty much open ended right now because the IS process is trying to integrate into the ERM process.

ACET review by GT. Validated the 2023 baseline statements. Making excuses as to the people who left having knowledge that may have applied to the ACET. Not going to use the ACET anymore. General Controls Audit is not current.