The information security training program includes the following:

Friday, August 16, 2024 12:11 PM

Preparation

1. Understand Requirements
- **Action:** Review each sub-statement (Stmt 7.1 to Stmt 7.12) to understand the specific training requirements.
- **Reference: Appendix A, Section III(B)(1)** – Each credit union must develop, implement, and maintain an information security program that includes training employees on security policies and procedures to protect member information.

2. Gather Documentation
- **Action:** Collect relevant documentation related to the information security training program, including training materials, attendance records, policies, and training schedules.
- **Reference: Appendix A, Section III(C)(1)** – The program must ensure that all employees are aware of security risks and the importance of protecting member information.

3. Identify Stakeholders
- **Action:** Identify key stakeholders, such as the training department, IT security team, compliance officers, and HR personnel, involved in administering and overseeing training.
- **Reference: Appendix A, Section III(C)(1)(b)** – Training should involve all key personnel responsible for implementing the information security program.

4. Plan Validation
- **Action:** Develop a detailed plan outlining the steps, resources, and timelines for validating each sub-statement and ensuring compliance.
- **Reference: Appendix A, Section III(B)(3)** – The information security program must be tested regularly, and its effectiveness evaluated, including the adequacy of training and personnel awareness.

Validation Steps

1. Validate New Employee Training and Background Checks (Stmt 7.1)
- **Action:** Review the training program to ensure new employees receive comprehensive information security training as part of their onboarding process.
- **Action:** Verify that background checks are conducted for new employees.
- **Reference: Appendix A, Section III(C)(2)** – The program must ensure the proper training and screening of employees to reduce risks related to unauthorized access to member information.

2. Validate Employee Training for All Employees (Stmt 7.2)
- **Action:** Check records to ensure that all employees receive regular, ongoing security training.
- **Action:** Review the content of the training to ensure it covers relevant security topics, such as data protection and compliance.
- **Reference: Appendix A, Section III(C)(1)** – The information security program must include regular training for all employees on security policies, procedures, and the importance of protecting member information.

3. Validate Incident Response, Current Cyber Threats, and Emerging Issues Training (Stmt 7.3)
- **Action:** Review training materials to ensure the content includes incident response procedures, current cyber threats, and emerging security risks.
- **Action:** Verify the frequency of training sessions focused on these critical topics.
- **Reference: Appendix A, Section III(C)(1)(c)** – Training must include the detection, prevention, and response to security incidents, including emerging threats and issues.

4. Validate Social Engineering Training (Stmt 7.4)
- **Action:** Ensure that training covers social engineering threats such as phishing, pretexting, and spear phishing.
- **Action:** Verify training records to ensure all employees have participated in this training.
- **Reference: Appendix A, Section III(C)(1)(c)** – The program should include awareness training on social engineering tactics that could compromise member information.

5. Validate Documented Training Records (Stmt 7.5)
- **Action:** Review records to confirm that all training sessions are properly documented and maintained.
- **Action:** Ensure the accuracy of these records and that they are up-to-date.
- **Reference: Appendix A, Section III(C)(2)(c)** – Training records must be maintained to demonstrate the effectiveness of the program and ensure compliance.

6. Validate Training Staff on Authentication Best Practices (Stmt 7.6)
- **Action:** Ensure that training includes best practices for authentication, including multi-factor authentication and password management.
- **Action:** Check that relevant staff, especially those in IT and security roles, have completed this training.
- **Reference: Appendix A, Section III(C)(1)(c)** – Employees responsible for information system access must receive specific training on authentication and other technical security controls.

7. Validate Member Security Awareness Materials (Stmt 7.7)
- **Action:** Review materials provided to members to raise awareness about security best practices, such as protecting online banking information.
- **Action:** Verify that these materials are distributed effectively and made accessible to all members.
- **Reference: Appendix A, Section III(C)(1)(e)** – The institution should develop security awareness programs for its members to help them safeguard their accounts and personal information.

8. Validate Annual Board Member Training (Stmt 7.8)
- **Action:** Ensure that board members receive annual security training tailored to their roles and responsibilities.
- **Action:** Verify attendance records to confirm that all board members have participated in the required training sessions.
- **Reference: Appendix A, Section III(C)(2)(b)** – Board members must be adequately trained on their role in overseeing the information security program and understanding risks related to member information.

9. Validate Staff Training on Data Leak Prevention Best Practices (Stmt 7.9)
- **Action:** Ensure that data leak prevention best practices are included in training materials for all relevant staff.
- **Action:** Confirm that staff have completed this training and that it is reflected in the training records.
- **Reference: Appendix A, Section III(C)(1)(c)** – Training must include awareness of data loss prevention techniques to mitigate risks to member information.

10. Validate Staff Training to Recognize and Report Security Incidents (Stmt 7.10)
- **Action:** Review the training content to ensure that it includes procedures for recognizing and reporting security incidents.
- **Action:** Verify that staff have been trained in these procedures and that records reflect their participation.
- **Reference: Appendix A, Section III(C)(1)(c)** – Employees must be trained on recognizing security incidents and the importance of timely reporting.

11. Validate Role-Specific Security Awareness and Skills Training (Stmt 7.11)
- **Action:** Ensure that the training program is tailored to specific roles, addressing the unique responsibilities and risks associated with each position.
- **Action:** Confirm that employees receive role-specific training and that attendance is documented.
- **Reference: Appendix A, Section III(C)(1)(b)** – Training must be customized to the specific roles and responsibilities of employees to address the unique risks they may encounter.

12. Validate Security Awareness and Training for Credit Union Officials (Stmt 7.12)
- **Action:** Ensure that credit union officials are required to attend security awareness training sessions.
- **Action:** Verify that training records confirm the participation of officials in these sessions.
- **Reference: Appendix A, Section III(C)(2)(b)** – Credit union officials must receive appropriate security awareness training in accordance with their role in overseeing the information security program.

Reporting and Documentation

1. Compile Findings
- **Action:** Document all findings from the validation process, including any gaps or deficiencies in the training program.
- **Action:** Provide actionable recommendations to address any areas of non-compliance.
- **Reference: Appendix A, Section III(C)(2)(c)** – Maintain documentation of training and any corrective actions taken to address deficiencies in the program.

2. Provide Report to Senior Management and Board

- **Action:** Present the findings and recommendations to senior management and the Board of Directors.
- **Action:** Ensure that any identified issues are addressed and integrated into the organization's risk management and training programs.
- **Reference: Appendix A, Section III(C)(2)(b)** – The Board and senior management must receive regular updates on the effectiveness of the information security training program.

Issues

Thursday, September 19, 2024 11:24 AM

Potential Findings for Validation Steps According to Appendix A to Part 748, Title 12
When conducting validation steps for the **Information Security Training Program**, several findings can emerge related to compliance gaps, deficiencies, and areas for improvement. Below are the **potential findings** for each validation step along with their alignment to **Appendix A to Part 748, Title 12**.

1. Validate New Employee Training and Background Checks (Stmt 7.1)
Potential Findings:
- **Lack of Comprehensive Security Training for New Employees:**
  - **Impact:** Employees may not fully understand security policies and procedures, leading to improper handling of sensitive information.
  - **Reference: Section III(C)(2)** – The program must ensure that all new employees receive proper training on security risks and practices.
- **Inconsistent or Missing Background Checks for New Employees:**
  - **Impact:** Hiring individuals without conducting appropriate background checks increases the risk of unauthorized access to member information.
  - **Reference: Section III(C)(2)** – Background checks are crucial for screening employees who may have access to sensitive data.

2. Validate Employee Training for All Employees (Stmt 7.2)
Potential Findings:
- **Training Not Provided Regularly:**
  - **Impact:** Employees may not stay updated on evolving security threats and changes in security policies, which increases the risk of data breaches.
  - **Reference: Section III(C)(1)** – Regular training on security policies and procedures is required for all employees.
- **Training Content Lacks Coverage of Key Security Topics:**
  - **Impact:** Incomplete or inadequate training may leave employees unprepared to handle data protection responsibilities.
  - **Reference: Section III(C)(1)** – Training must cover relevant security topics, including data protection and compliance.

3. Validate Incident Response, Current Cyber Threats, and Emerging Issues Training (Stmt 7.3)
Potential Findings:
- **Outdated or Incomplete Training on Incident Response and Cyber Threats:**
  - **Impact:** Employees may not be prepared to respond to incidents or emerging cyber threats, which can result in delays in identifying and containing breaches.
  - **Reference: Section III(C)(1)(c)** – The program must include training on incident response, current cyber threats, and emerging issues.
- **Infrequent Training on Critical Topics:**
  - **Impact:** Delays in providing updated training may result in employees being unaware of the latest threats and response procedures.
  - **Reference: Section III(C)(1)(c)** – Regular and updated training is required to ensure preparedness.

4. Validate Social Engineering Training (Stmt 7.4)
Potential Findings:
- **Lack of Emphasis on Social Engineering Threats:**
  - **Impact:** Employees may be vulnerable to phishing, pretexting, and other social engineering attacks.
  - **Reference: Section III(C)(1)(c)** – Training should include awareness of social engineering tactics.
- **Not All Employees Have Completed Social Engineering Training:**
  - **Impact:** Incomplete participation in training leaves parts of the workforce unprepared to recognize and mitigate these threats.
  - **Reference: Section III(C)(1)(c)** – All employees must be trained on social engineering risks.

5. Validate Documented Training Records (Stmt 7.5)
Potential Findings:
- **Training Records Are Incomplete or Not Maintained:**
  - **Impact:** Lack of proper records can result in compliance failures and make it difficult to verify the effectiveness of training programs.
  - **Reference: Section III(C)(2)(c)** – Training records must be maintained to ensure program compliance and effectiveness.
- **Records Are Not Updated After Each Training Session:**
  - **Impact:** Outdated records make it difficult to track which employees have received the necessary training.
  - **Reference: Section III(C)(2)(c)** – Accurate records are required for audit and compliance purposes.

6. Validate Training Staff on Authentication Best Practices (Stmt 7.6)
Potential Findings:
- **Insufficient Coverage of Authentication and Password Management in Training:**
  - **Impact:** Employees may fail to implement strong authentication practices, increasing the risk of unauthorized access to systems.
  - **Reference: Section III(C)(1)(c)** – Training must cover critical topics like multi-factor authentication and password management.
- **Relevant IT and Security Staff Have Not Completed This Training:**
  - **Impact:** Failure to train key staff on authentication best practices may lead to vulnerabilities in system security.
  - **Reference: Section III(C)(1)(c)** – Employees responsible for system access must receive adequate training on authentication practices.

7. Validate Member Security Awareness Materials (Stmt 7.7)
Potential Findings:
- **Member Awareness Materials Are Outdated or Ineffective:**
  - **Impact:** Members may be unaware of security best practices, making them more vulnerable to account compromises and fraud.
  - **Reference: Section III(C)(1)(e)** – The institution should provide security awareness programs for members.
- **Materials Are Not Being Distributed Effectively:**
  - **Impact:** Without proper distribution, members may not receive critical information that helps them protect their accounts.
  - **Reference: Section III(C)(1)(e)** – Awareness materials must be accessible to all members.

8. Validate Annual Board Member Training (Stmt 7.8)
Potential Findings:
- **Board Members Are Not Receiving Required Annual Training:**
  - **Impact:** Board members may not fully understand their roles in overseeing the information security program, which can hinder effective governance.
  - **Reference: Section III(C)(2)(b)** – Board members must receive annual training on their roles in overseeing the security program.
- **Attendance Records for Board Training Are Missing or Incomplete:**
  - **Impact:** Inadequate tracking of board member training may result in non-compliance with regulatory requirements.
  - **Reference: Section III(C)(2)(b)** – Records must verify that all board members participate in training.

9. Validate Staff Training on Data Leak Prevention Best Practices (Stmt 7.9)
Potential Findings:
- **Training Does Not Cover Data Leak Prevention Techniques:**
  - **Impact:** Employees may be unaware of how to prevent data leaks, which increases the risk of accidental or intentional data exposure.
  - **Reference: Section III(C)(1)(c)** – Training must include data loss prevention techniques to protect member information.
- **Training Records Do Not Show Completion of This Training for All Staff:**
  - **Impact:** Without complete participation, some staff may not be equipped to prevent data leaks.
  - **Reference: Section III(C)(1)(c)** – All relevant staff must complete data leak prevention training.

10. Validate Staff Training to Recognize and Report Security Incidents (Stmt 7.10)
Potential Findings:
- **Incident Reporting Procedures Are Not Included in Training:**
  - **Impact:** Employees may not know how to recognize or report security incidents, which delays response efforts.
  - **Reference: Section III(C)(1)(c)** – Training must include procedures for recognizing and reporting security incidents.
- **Records Do Not Show Participation in Incident Response Training:**
  - **Impact:** Without adequate training, employees may not effectively handle security incidents.
  - **Reference: Section III(C)(1)(c)** – All staff must be trained on incident recognition and reporting.

11. Validate Role-Specific Security Awareness and Skills Training (Stmt 7.11)
Potential Findings:
- **Role-Specific Training Is Not Provided:**
  - **Impact:** Employees may not have the specialized knowledge required to handle security risks specific to their roles.

- **Reference: Section III(C)(1)(b)** – Training must be tailored to the roles and responsibilities of employees.
- **Training Records Do Not Reflect Role-Specific Training Participation:**
  - **Impact:** Without role-specific training, employees may lack the necessary skills to perform their duties securely.
  - **Reference: Section III(C)(1)(b)** – Role-specific training must be documented for all employees.

12. Validate Security Awareness and Training for Credit Union Officials (Stmt 7.12)

Potential Findings:

- **Credit Union Officials Have Not Attended Required Training:**
  - **Impact:** Lack of training may prevent officials from effectively overseeing the security program.
  - **Reference: Section III(C)(2)(b)** – Officials must receive appropriate training on their role in the information security program.
- **Attendance Records for Officials Are Incomplete:**
  - **Impact:** Failure to track participation may result in non-compliance with training requirements.
  - **Reference: Section III(C)(2)(b)** – Officials' training must be documented and verified.

Reporting and Documentation

1. Compile Findings

- **Potential Finding:** Failure to Document Training Gaps or Deficiencies
  - **Impact:** Incomplete documentation may result in non-compliance during regulatory audits.
  - **Reference: Section III(C)(2)(c)** – Document and address any deficiencies found in the training program.

2. Provide Report to Senior Management and Board

Potential Finding: Failure to Regularly Report Training Status to Senior Management or Board

- **Impact:** Lack of oversight by senior management may result in unaddressed gaps in the training program.
- **Reference: Section III(C)(2)(b)** – Senior management and the Board must receive updates on the effectiveness of the training program.

By identifying and addressing these potential findings, credit unions can ensure compliance with **Appendix A to Part 748, Title 12** and maintain an effective information security training program that protects member data and enhances organizational security.

Remediation

Thursday, September 19, 2024 11:33 AM

Remediation Steps for Potential Findings (Validation of Information Security Training Program)
Below are the **remediation steps** for addressing the potential findings identified during the validation of the **Information Security Training Program** aligned with **Appendix A to Part 748, Title 12**.

1. Validate New Employee Training and Background Checks (Stmt 7.1)

Finding: Lack of Comprehensive Security Training for New Employees

- **Remediation Steps:**
  1. **Revise the onboarding process** to include mandatory comprehensive information security training for all new hires.
  2. **Develop or update training materials** covering the basics of information security, including data protection, access controls, and the importance of safeguarding member information.
  3. **Ensure mandatory completion** of training before granting system access to new employees.

Finding: Inconsistent or Missing Background Checks for New Employees

- **Remediation Steps:**
  1. **Implement a standardized background check policy** as part of the onboarding process for all employees, particularly those with access to sensitive member information.
  2. **Verify the process for conducting background checks** is consistently followed and documented.

2. Validate Employee Training for All Employees (Stmt 7.2)

Finding: Training Not Provided Regularly

- **Remediation Steps:**
  1. **Establish a regular training schedule** (e.g., annual or semi-annual) for all employees to refresh their knowledge on security policies and procedures.
  2. **Implement a training tracking system** to ensure all employees complete mandatory training by designated deadlines.

Finding: Training Content Lacks Coverage of Key Security Topics

- **Remediation Steps:**
  1. **Review and revise training materials** to ensure they cover essential topics such as data protection, compliance with security policies, and current security threats.
  2. **Incorporate real-world case studies** and examples of security breaches to increase engagement and awareness.

3. Validate Incident Response, Current Cyber Threats, and Emerging Issues Training (Stmt 7.3)

Finding: Outdated or Incomplete Training on Incident Response and Cyber Threats

- **Remediation Steps:**
  1. **Update the training program** to include current cyber threats, such as ransomware, malware, and social engineering attacks.
  2. **Include detailed incident response procedures** and protocols in the training, ensuring that employees understand their roles during a breach.

Finding: Infrequent Training on Critical Topics

- **Remediation Steps:**
  1. **Implement quarterly or bi-annual training updates** to ensure employees are aware of the latest cybersecurity threats and responses.
  2. **Monitor attendance and participation** in incident response training to ensure all employees are engaged.

4. Validate Social Engineering Training (Stmt 7.4)

Finding: Lack of Emphasis on Social Engineering Threats

- **Remediation Steps:**
  1. **Enhance training content** to emphasize social engineering threats, including phishing, pretexting, and spear phishing, with real-world examples.
  2. **Conduct simulated phishing exercises** to assess employee awareness and response to social engineering tactics.

Finding: Not All Employees Have Completed Social Engineering Training

- **Remediation Steps:**
  1. **Ensure that all employees complete mandatory social engineering awareness training** through an online or in-person program.
  2. **Implement a tracking mechanism** to flag employees who have not completed the training and follow up to ensure compliance.

5. Validate Documented Training Records (Stmt 7.5)

Finding: Training Records Are Incomplete or Not Maintained

- **Remediation Steps:**
  1. **Implement a centralized tracking system** to record all training sessions, participation, and completion status.
  2. **Conduct an internal audit** to review current training records and ensure they are complete, accurate, and up-to-date.

Finding: Records Are Not Updated After Each Training Session

- **Remediation Steps:**
  1. **Establish a policy to update training records immediately** after each session, with designated personnel responsible for record maintenance.
  2. **Set automated reminders** for HR or the training department to ensure records are updated promptly.

6. Validate Training Staff on Authentication Best Practices (Stmt 7.6)

Finding: Insufficient Coverage of Authentication and Password Management in Training

- **Remediation Steps:**
  1. **Update training content** to include best practices for authentication (e.g., multi-factor authentication) and secure password management.
  2. **Ensure that authentication training** is mandatory for all employees, especially IT and security staff.

Finding: Relevant IT and Security Staff Have Not Completed This Training

- **Remediation Steps:**
  1. **Identify gaps in training completion** and ensure all IT and security staff are enrolled in mandatory authentication training.
  2. **Schedule follow-up training sessions** to address any missed sessions or incomplete training.

7. Validate Member Security Awareness Materials (Stmt 7.7)

Finding: Member Awareness Materials Are Outdated or Ineffective

- **Remediation Steps:**
  1. **Revise and update member security awareness materials** to reflect current cybersecurity best practices.
  2. **Collaborate with marketing and communications teams** to design engaging and accessible materials for members.

Finding: Materials Are Not Being Distributed Effectively

- **Remediation Steps:**
  1. **Develop a distribution strategy** (e.g., email newsletters, website updates, social media posts) to ensure all members receive important security information.

2. **Track and monitor distribution** to confirm that materials are effectively reaching all members.

8. Validate Annual Board Member Training (Stmt 7.8)

Finding: Board Members Are Not Receiving Required Annual Training

- **Remediation Steps:**
    1. **Schedule mandatory annual training for board members** on information security risks, governance, and their oversight responsibilities.
    2. **Ensure board members are notified in advance** and that participation is tracked and enforced.

Finding: Attendance Records for Board Training Are Missing or Incomplete

- **Remediation Steps:**
    1. **Implement a formal process** for recording board member attendance and completion of training.
    2. **Designate personnel responsible for tracking attendance** and maintaining accurate records.

9. Validate Staff Training on Data Leak Prevention Best Practices (Stmt 7.9)

Finding: Training Does Not Cover Data Leak Prevention Techniques

- **Remediation Steps:**
    1. **Enhance training materials** to include data leak prevention techniques such as encryption, access controls, and secure data transfer.
    2. **Ensure data leak prevention training** is a required component for all employees handling sensitive information.

Finding: Training Records Do Not Show Completion of This Training for All Staff

- **Remediation Steps:**
    1. **Identify employees who have not completed this training** and enroll them in mandatory sessions.
    2. **Ensure future compliance** by incorporating data leak prevention into the core training curriculum.

10. Validate Staff Training to Recognize and Report Security Incidents (Stmt 7.10)

Finding: Incident Reporting Procedures Are Not Included in Training

- **Remediation Steps:**
    1. **Revise training materials** to include clear procedures for recognizing and reporting security incidents.
    2. **Conduct regular incident response drills** to reinforce these procedures and ensure employees are familiar with the reporting process.

Finding: Records Do Not Show Participation in Incident Response Training

- **Remediation Steps:**
    1. **Track and verify completion of incident response training** for all employees.
    2. **Follow up with employees who have missed training sessions** to ensure they receive the required instruction.

11. Validate Role-Specific Security Awareness and Skills Training (Stmt 7.11)

Finding: Role-Specific Training Is Not Provided

- **Remediation Steps:**
    1. **Develop role-specific training modules** that address the unique risks and responsibilities of different job functions.
    2. **Tailor content to the specific needs** of each department, ensuring that specialized staff (e.g., IT, compliance) receive targeted training.

Finding: Training Records Do Not Reflect Role-Specific Training Participation

- **Remediation Steps:**
    1. **Audit training records** to ensure role-specific training is accurately documented.
    2. **Flag employees who are missing this training** and schedule catch-up sessions.

12. Validate Security Awareness and Training for Credit Union Officials (Stmt 7.12)

Finding: Credit Union Officials Have Not Attended Required Training

- **Remediation Steps:**
    1. **Mandate security awareness training** for all officials with oversight responsibilities, ensuring they are equipped to manage and mitigate security risks.
    2. **Incorporate security training into the official onboarding process** and require annual refreshers.

Finding: Attendance Records for Officials Are Incomplete

- **Remediation Steps:**
    1. **Ensure attendance is recorded** for all training sessions attended by credit union officials.
    2. **Conduct audits** to verify training completion and follow up on missing records.

To ensure compliance with **Appendix A to Part 748, Title 12**, particularly in relation to the **Information Security Training Program**, credit unions must adopt a structured approach to managing, monitoring, and validating their training efforts. Below are the key steps and best practices for ensuring compliance:

1. Develop a Comprehensive Information Security Training Program

1.1 Align the Training Program with Regulatory Requirements

- **Action:** Ensure the training program covers all aspects outlined in **Appendix A to Part 748, Title 12**. This includes general security awareness, incident response, social engineering, and role-specific training.
- **Compliance Measure:** Review the training program to ensure it aligns with the regulatory requirements outlined in **Section III(C)(1)**.

1.2 Include All Employees, Board Members, and Officials

- **Action:** Develop training that applies to all levels of the organization, from new hires to senior management and the Board of Directors. Specific training for officials, IT personnel, and other specialized roles should also be included.
- **Compliance Measure:** Ensure training programs cover all roles as per **Section III(C)(1)(b)** and **Section III(C)(2)(b)**.

2. Implement an Ongoing Training Program

2.1 Provide Regular and Updated Training

- **Action:** Conduct regular training sessions that address current cyber threats, emerging security risks, and updates in security policies. Training should be held at regular intervals, such as annually or semi-annually.
- **Compliance Measure:** Document and track the frequency and content of training to ensure it meets the standards in **Section III(C)(1)(c)**.

2.2 Ensure Training is Tailored to Specific Roles

- **Action:** Tailor security training to the specific roles and responsibilities of employees to ensure they understand the security risks relevant to their duties.
- **Compliance Measure:** Verify role-specific training content and attendance in compliance with **Section III(C)(1)(b)**.

3. Conduct Audits and Reviews of the Training Program

3.1 Perform Regular Internal Audits

- **Action:** Conduct periodic audits of the training program to assess its effectiveness and ensure all training requirements are met.
- **Compliance Measure:** Use internal audits to identify gaps in training and address them as per **Section III(B)(3)**, which requires regular testing and evaluation of the program.

3.2 Engage External Auditors for Independent Review

- **Action:** Engage third-party auditors to independently review and validate the effectiveness of the information security training program.
- **Compliance Measure:** Use external audit findings to make necessary improvements, ensuring compliance with **Section III(C)(2)**.

4. Maintain Accurate Documentation and Records

4.1 Keep Detailed Training Records

- **Action:** Ensure that training sessions, attendance records, content materials, and certifications are well-documented and stored securely.

- **Compliance Measure:** Maintain training records that demonstrate employee and official participation, as required in **Section III(C)(2)(c)**.

4.2 Document Exceptions and Remediate Issues

- **Action:** If there are gaps in training attendance or exceptions, document these and develop a corrective action plan to address them.
- **Compliance Measure:** Ensure exceptions are documented and remediated according to **Section III(B)(3)**, which calls for corrective measures to address deficiencies.

5. Monitor and Track Training Effectiveness

5.1 Implement Metrics to Measure Training Success

- **Action:** Develop metrics to assess the effectiveness of training programs, such as employee assessments, incident response improvements, and phishing test results.
- **Compliance Measure:** Track training performance metrics to ensure continuous improvement and compliance with **Section III(C)(1)(c)**.

5.2 Use Feedback to Update and Improve Training Content

- **Action:** Solicit feedback from employees and management on the effectiveness and relevance of training materials.
- **Compliance Measure:** Regularly update training content based on feedback, audit findings, and emerging threats, ensuring alignment with **Section III(A)(3)**.

6. Report to Senior Management and the Board

6.1 Provide Regular Compliance Updates to the Board

- **Action:** Regularly report the status of the training program, audit results, and any corrective actions to senior management and the Board.
- **Compliance Measure:** Ensure the Board is aware of any training gaps and improvements as required by **Section III(C)(2)(b)**, which mandates oversight by senior management.

6.2 Use Training Reports in Risk Assessments

- **Action:** Integrate training performance and compliance reports into the overall risk assessment and information security program review.
- **Compliance Measure:** Ensure training and awareness programs are factored into the broader risk assessment as per **Section III(A)(1)**.

7. Foster a Culture of Security Awareness

7.1 Promote a Culture of Ongoing Security Awareness

- **Action:** Continuously promote a security-first mindset across the organization through regular communication, newsletters, and awareness programs.
- **Compliance Measure:** Ensure that ongoing security awareness aligns with **Section III(C)(1)(e)**, which requires member and employee security awareness programs.

7.2 Reinforce Training Through Simulated Attacks

- **Action:** Implement phishing simulations and social engineering exercises to reinforce training content and ensure employees can recognize and respond to threats.
- **Compliance Measure:** Document and analyze the results of these simulations to track progress and compliance with **Section III(C)(1)(c)**.

8. Update Training Based on Emerging Threats and Regulations

8.1 Stay Current with Regulatory Changes

- **Action:** Regularly review updates to regulatory requirements and incorporate any changes into the training program.
- **Compliance Measure:** Ensure the training program is aligned with current regulations as required by **Section III(A)(3)**, which mandates updates to the information security program based on evolving risks.

8.2 Update Content Based on New Threats

- **Action:** Revise training materials based on emerging cyber threats and changes in the organization's risk environment.
- **Compliance Measure:** Ensure content is refreshed regularly to meet the standards in **Section III(C)(1)(c)**.

9. Establish Clear Communication Channels for Reporting Incidents

9.1 Provide Training on Reporting Security Incidents

- **Action:** Ensure employees are trained on how to report security incidents promptly and efficiently through designated channels.
- **Compliance Measure:** Verify that incident reporting procedures are included in training materials as required by **Section III(C)(1)(c)**.

9.2 Ensure Incident Reporting Channels are Accessible

- **Action:** Make sure that all employees know how and where to report security incidents and potential breaches.
- **Compliance Measure:** Maintain clear communication channels for incident reporting, ensuring compliance with **Section III(C)(1)(c)**.

By following these steps, credit unions can ensure that their **Information Security Training Program** complies with the requirements of **Appendix A to Part 748, Title 12**, enhancing overall security awareness, minimizing risks, and protecting member information effectively. This structured approach ensures ongoing compliance through regular monitoring, documentation, and improvements based on emerging risks and regulatory updates.

Tools

Friday, August 16, 2024 12:17 PM

1. Document and Records Management

- **Document Management Systems (DMS):**
  - **SharePoint:** For managing and storing training materials and records.
  - **Google Workspace:** For creating, sharing, and managing documents.
- **Learning Management Systems (LMS):**
  - **Moodle:** For delivering and tracking training programs.
  - **Cornerstone OnDemand:** For managing employee training and certifications.

2. Training Content Evaluation

- **Content Review Tools:**
  - **Microsoft Word/Google Docs:** For reviewing and editing training materials.
  - **Adobe Acrobat:** For reviewing and annotating PDF training documents.
- **Training and Simulation Tools:**
  - **PhishMe/KnowBe4:** For simulating phishing attacks and training employees on recognizing social engineering.
  - **CybSafe:** For interactive security training and behavioral analytics.

3. Employee Knowledge and Assessment

- **Survey Tools:**
  - **SurveyMonkey/Google Forms:** For conducting surveys to assess employee understanding and effectiveness of training.
- **Quiz and Assessment Tools:**
  - **Quizlet:** For creating and administering quizzes on training content.
  - **Kahoot!:** For interactive quizzes and assessments.
- **Knowledge Testing Platforms:**
  - **TestGorilla:** For conducting pre-employment and ongoing skill assessments.

4. Incident Response and Awareness Training

- **Incident Simulation Tools:**
  - **SANS Institute's Cybersecurity Training Tools:** For incident response training and simulations.
  - **IBM's X-Force Red:** For testing incident response plans with real-world scenarios.
- **Awareness Materials Creation:**
  - **Canva:** For designing member security awareness materials.
  - **Piktochart:** For creating infographics and visual training content.

5. Documentation and Reporting

- **Reporting Tools:**
  - **Microsoft Excel/Google Sheets:** For creating and managing training records and reporting.
  - **Tableau/Power BI:** For advanced data visualization and reporting on training compliance and effectiveness.
- **Audit Management Tools:**
  - **AuditBoard:** For managing audit processes and tracking compliance.
  - **Netwrix Auditor:** For auditing training records and tracking changes.

6. Training Program Management

- **Project Management Tools:**
  - **Asana/Trello:** For managing training program tasks, schedules, and milestones.
  - **Jira:** For tracking tasks and issues related to training program implementation.
- **Compliance Tracking Tools:**
  - **GRC Platforms (Governance, Risk, and Compliance):**
    - **MetricStream:** For tracking compliance with security training requirements.
    - **RSA Archer:** For managing risk and compliance processes related to training.

7. Communication and Coordination

- **Collaboration Tools:**
  - **Microsoft Teams/Slack:** For coordinating with team members and stakeholders involved in the training program.
  - **Zoom/Webex:** For conducting virtual training sessions and meetings.
- **Email and Notification Tools:**
  - **Mailchimp/SendGrid:** For sending training materials and updates to employees.

8. Specialized Tools for Role-Specific Training

- **Role-Specific Training Platforms:**
  - **Pluralsight:** For technical and role-specific training.
  - **LinkedIn Learning:** For a broad range of professional development topics including security.
- **Security Awareness Platforms:**
  - **SANS Security Awareness Training:** For role-specific and organization-wide security training.

Resources

Friday, August 16, 2024 12:18 PM

Strong	Satisfactory	Less Than Satisfactory	Deficient	Critically Deficient
☐ Formal security awareness training program in place; ☐ Periodic training of all staff, including the Board ☐ Communication of acceptable use expectations ☐ Trained to identify social engineering attacks ☐ Trained on utilizing secure authentication. ☐ Customer awareness program	☐ Formal security awareness training program in place; ☐ Periodic training of all staff, including the Board ☐ Communication of acceptable use expectations ☐ Trained to identify social engineering attacks ☐ Trained on utilizing secure authentication. ☐ No member awareness program	☐ Security awareness training program in place but not formalized. ☐ Periodic training of all staff does not include the Board ☐ No communication of acceptable use expectations ☐ Not trained to identify social engineering attacks ☐ Not trained on utilizing secure authentication. ☐ No member awareness program.	☐ Security awareness training program in place but not formalized; ☐ No periodic training of all staff and does not including the Board ☐ No communication of acceptable use expectations ☐ Not trained to identify social engineering attacks ☐ Not trained on utilizing secure authentication. ☐ No member awareness program.	☐ No information security training program in place.

KPI

Wednesday, September 18, 2024 2:59 PM

1. New Employee Training and Background Checks

Metrics:

- Completion rate of background checks before onboarding.
- Completion rate of initial security training within the first month of employment.
- Pass rate of initial security assessment tests.

Assessment Methods:

- Verify completion of background checks.
- Track attendance and completion of initial training sessions.
- Administer and evaluate security knowledge tests.

KPIs:

- 100% completion of background checks.
- 100% completion of initial training.
- At least 90% pass rate on initial security assessment tests.

2. Employee Training Provided to All Employees

Metrics:

- Frequency of training sessions (quarterly, bi-annually, etc.).
- Attendance rate of mandatory training sessions.
- Improvement in security knowledge scores over time.

Assessment Methods:

- Track attendance and participation.
- Conduct pre- and post-training assessments.
- Collect feedback through surveys.

KPIs:

- 95% attendance rate for mandatory training.
- 80% of employees show improvement in post-training assessments.
- High satisfaction scores (e.g., above 4 on a 5-point scale) in feedback surveys.

3. Incident Response, Current Cyber Threats, and Emerging Issues

Metrics:

- Frequency of incident response drills and updates on current threats.
- Employee awareness of recent threats and incident response protocols.

Assessment Methods:

- Conduct regular incident response drills and tabletop exercises.
- Quiz employees on recent threats and response procedures.

KPIs:

- Conduct at least two incident response drills annually.
- 90% of employees can correctly identify and respond to recent threats in assessments.

4. Social Engineering Training (Phishing Scams, Pretexting, Spear Phishing)

Metrics:

- Number of phishing simulation tests conducted annually.
- Click rate on simulated phishing emails.
- Incident reports from employees on suspected social engineering attempts.

Assessment Methods:

- Regular phishing simulation campaigns.
- Monitor and record responses to phishing simulations.
- Encourage reporting of suspected phishing attempts and track the number of reports.

KPIs:

- Conduct at least four phishing simulation tests annually.
- Reduce click rate on simulated phishing emails to below 5%.
- Increase the number of reported phishing attempts by employees by 20% annually.

5. Documented Training Records

Metrics:

- Completeness and accuracy of training records.
- Availability of training records for audit and review.

Assessment Methods:

- Regular audits of training records.
- Use of a centralized Learning Management System (LMS) to track training completion and records.

KPIs:

- 100% of training records are up-to-date and accurate.
- Training records are available for audit within 24 hours of request.

Implementation Steps

1. **Set Up a Learning Management System (LMS):** Use an LMS to automate tracking, reminders, and documentation of training sessions.
2. **Regular Audits:** Conduct periodic audits to ensure training records are complete and accurate.
3. **Feedback Mechanism:** Implement a feedback mechanism for employees to provide input on training effectiveness and areas for improvement.
4. **Continuous Improvement:** Use the data collected to continually improve training content and delivery methods.

Examiner Finding

Thursday, December 12, 2024 2:42 PM

Finding Using SBIR Format with Awareness Initiative Policy Integration

1. Situation (S):

During the examination of the credit union's Information Security Training Program, the review included an assessment of its alignment with Appendix A to Part 748, Title 12, and its adherence to the internal **Awareness Initiative Policy**. The policy outlines required roles and responsibilities, cross-training modules, and procedures for updating and maintaining training topics, as well as tracking employee participation.

2. Behavior (B):

Although the **Awareness Initiative Policy** specifies comprehensive training requirements, the review revealed the following:

- Records indicate that only phishing training sessions were conducted, while other critical topics outlined in the policy, such as data sensitivity, encryption, acceptable use, and emergency procedures, were not addressed.
- There is no documentation to demonstrate the development, delivery, or tracking of cross-training modules for hardware/software usage, regulatory compliance, security policies, or other topics defined by the Information Security Officer.
- While the policy mandates that employees sign into training sessions and Human Resources log attendance records, there is no evidence of these records for sessions beyond phishing training.
- The Information Security Officer is tasked with maintaining training topics, but no updates to the training program addressing evolving threats or policy requirements were documented.

3. Impact (I):

The limited implementation of the **Awareness Initiative Policy** has resulted in:

- Non-compliance with regulatory requirements in Appendix A to Part 748, Title 12, which mandates comprehensive training for all employees, board members, and officials.
- Increased risk exposure due to inadequate coverage of critical security topics, such as encryption, regulatory compliance, and emergency procedures.
- Weak documentation and record-keeping, which hinder the credit union's ability to demonstrate accountability and preparedness.
- Missed opportunities to enhance employee awareness and preparedness against a broader range of security threats.

4. Resolution (R):

To address these issues, the credit union should take the following actions:

1. **Expand Training Coverage:** Develop and deliver training modules for all topics outlined in the **Awareness Initiative Policy**, including acceptable use, data sensitivity, regulatory compliance, and emergency procedures.
2. **Document Training Activities:** Ensure that attendance records and content materials are created and maintained for all training sessions, as mandated by the policy. Leverage Human Resources to centralize and standardize record-keeping.
3. **Conduct Comprehensive Audits:** Perform periodic internal audits to verify that all policy-mandated training modules are delivered and documented effectively.
4. **Update Training Content:** Task the Information Security Officer with regularly

reviewing and updating training topics to address emerging cyber threats and organizational changes.

5. **Monitor Compliance with Policy:** Establish a process for regularly monitoring adherence to the **Awareness Initiative Policy** and take corrective actions for gaps in implementation.
6. **Enhance Reporting to Management:** Provide detailed reports on training activities, participation, and effectiveness to senior management and the Board of Directors.

Notes

Tuesday, September 3, 2024 7:03 AM

The review process for Stmt 7.1 to 7.6 validated that the credit union's employee training program included comprehensive onboarding training for new hires and confirmed that background checks were conducted to mitigate risks related to unauthorized access to member information. It verified that all employees received regular, ongoing security training covering relevant topics such as data protection, compliance, incident response procedures, emerging cyber threats, and social engineering tactics. The review also ensured that training materials incorporated best practices for authentication, including multi-factor authentication and password management, particularly for IT and security personnel. Additionally, training records were reviewed to confirm they were accurate, up-to-date, and adequately maintained to demonstrate compliance and effectiveness, ensuring alignment with regulatory requirements outlined in Appendix A, Section III of Part 748.