

# CORE Validation

Tuesday, August 13, 2024 3:43 PM

## 1. Governance and Oversight

- **Core Assessment:**
  - Verified whether the Board of Directors has formally approved the ISP.
  - Date of last review
  - Reviewed meeting minutes or board resolutions to ensure alignment with regulatory and organizational goals.
- **Positive Finding:** "The Board of Directors formally approves the ISP annually, demonstrating strong governance and oversight, in compliance with Appendix A, Section III(C)(1)."
- **Negative Finding:** "The ISP has not been formally approved by the Board of Directors, with no evidence of approval in meeting minutes or resolutions, reflecting insufficient governance."
- **Questions:**
  - Has the Board of Directors formally approved the information security program?
    - **Evidence:** Review meeting minutes or board resolutions for formal approval. Reference: Appendix A, Section III(C)(1).
- **Document Request:**
  - Meeting minutes or board resolutions approving the ISP.
  - Policies or reports presented to the Board for approval.

## 2. Access Controls and Authentication

- **Core Assessment:**
  - Evaluated access controls and authentication mechanisms, including multi-factor authentication (MFA).
- **Positive Finding:** "Access controls for all systems handling member information are well-documented, with MFA and role-based permissions implemented, ensuring compliance with Appendix A, Section III(C)(1)(a)."
- **Negative Finding:** "Access control policies are outdated, and several systems lack robust authentication mechanisms, such as MFA, increasing the risk of unauthorized access."
- **Questions:**
  - Are access controls documented and in place for systems and applications handling member information?
    - **Evidence:** Review system access control documentation. Reference: Appendix A, Section III(C)(1)(a).
  - Are authentication mechanisms for users (e.g., MFA) robust and compliant with industry best practices?
    - **Key Check:** Ensure only authorized individuals have access to sensitive information.
- **Document Request:**
  - Policies and procedures for access controls.
  - User access management reports (e.g., access lists, role definitions).
  - Records of MFA implementation and audit logs.

## 3. Physical Access Restrictions

- **Core Assessment:**
  - Assessed physical security measures, including secure premises and surveillance systems.
- **Positive Finding:** "Physical access controls, including secure premises, surveillance systems, and restricted entry, are effectively implemented and regularly reviewed, meeting Appendix A, Section III(C)(1)(b)."
- **Negative Finding:** "Physical security measures are insufficient, with outdated surveillance systems and missing access logs for critical areas, exposing sensitive information to unauthorized physical access."
- **Questions:**
  - Are physical access restrictions (e.g., secure premises, surveillance systems) documented and effective?
    - **Evidence:** Review documentation of physical security measures. Reference: Appendix A, Section III(C)(1)(c).
  - Do physical safeguards ensure that member information is protected from unauthorized physical access?
- **Document Request:**
  - Physical security policies and procedures.
  - Inventory of physical safeguards.
  - Logs and reports of physical access incidents.

## 4. Data Encryption

- **Core Assessment:**

- Reviewed encryption protocols, such as AES-256, for data at rest and in transit.
- **Positive Finding:** "Encryption protocols are consistently applied using AES-256, ensuring the confidentiality and integrity of member information, as required by Appendix A, Section III(C)(1)(c)."
- **Negative Finding:** "Encryption protocols are inconsistent, with some systems using outdated algorithms, and data at rest is not always encrypted, exposing sensitive information to potential breaches."
- **Questions:**
  - Is data encryption applied to protect member information at rest and in transit?
    - **Evidence:** Review encryption protocols (e.g., AES-256 for both storage and transmission). Reference: Appendix A, Section III(C)(1)(c).
  - Are encryption methods aligned with industry standards sufficient to protect customer information?
- **Document Request:**
  - Encryption policies and procedures.
  - Evidence of encryption implementation (e.g., certificates, configuration screenshots).
  - Compliance audit reports.

## 5. Testing Key or Critical Controls

- **Core Assessment:**
  - Assessed schedules, penetration testing reports, and audits to ensure effective testing of security controls.
- **Positive Finding:** "Critical security controls are regularly tested, with schedules and follow-up actions documented, adhering to Appendix A, Section III(C)(3)."
- **Negative Finding:** "Critical security controls are not tested regularly, and follow-up actions from previous tests are poorly documented, increasing the risk of undetected vulnerabilities."
- **Questions:**
  - Is there a documented schedule and process for regularly testing critical security controls, systems, and procedures?
    - **Evidence:** Review testing documentation (e.g., penetration testing reports, system audits). Reference: Appendix A, Section III(C)(3).
  - Are tests conducted frequently enough to address potential risks, and are the results documented for follow-up?
- **Document Request:**
  - Testing schedules for critical controls.
  - Reports from recent penetration tests and audits.
  - Records of remediation actions based on testing results.

## 6. Segregation of Duties

- **Core Assessment:**
  - Reviewed segregation of duties documentation and access permissions.
- **Positive Finding:** "The segregation of duties is clearly documented, minimizing risks of conflicts of interest and supporting compliance with Appendix A, Section III(C)(1)(e)."
- **Negative Finding:** "Segregation of duties is poorly defined, with some employees having excessive control over sensitive systems, increasing the risk of unauthorized access."
- **Questions:**
  - Is the segregation of duties documented, and are responsibilities clearly separated to prevent unauthorized access or conflicts of interest?
    - **Evidence:** Review roles and access permissions documentation. Reference: Appendix A, Section III(C)(1)(e).
  - Does the segregation of duties ensure that no individual has excessive control or oversight over sensitive systems and data?
- **Document Request:**
  - Role-based responsibilities and access permissions documentation.
  - Logs demonstrating adherence to segregation of duties policies.

## 7. Data Destruction and Media Sanitization

- **Core Assessment:**
  - Assessed data destruction policies and procedures for effectiveness.
- **Positive Finding:** "Data destruction and media sanitization processes are well-documented and effectively executed, ensuring irretrievable disposal of member information, as required by Appendix A, Section III(C)(4)."
- **Negative Finding:** "Data destruction methods are inconsistently applied, with some records improperly disposed of, creating a risk of member information being recoverable."

- **Questions:**
  - Are procedures for secure data destruction and media sanitization documented and implemented effectively?
    - **Evidence:** Review data destruction policies and procedures. Reference: Appendix A, Section III(C)(4).
  - Are data destruction methods sufficient to ensure that member information cannot be recovered once disposed of?
- **Document Request:**
  - Data destruction policies and procedures.
  - Records of data destruction activities and audit logs.

## 8. Security Program Responsibility

- **Core Assessment:**
  - Verified whether roles and responsibilities for the ISP are clearly defined and assigned.
- **Positive Finding:** "Clear responsibility for the ISP is assigned, with documented roles and accountability demonstrating effective oversight, in compliance with Appendix A, Section III(A)(2)."
- **Negative Finding:** "Roles and responsibilities for the ISP are unclear or undocumented, leading to gaps in oversight and accountability for key security tasks."
- **Questions:**
  - Is there a clearly documented assignment of responsibility for implementing and maintaining the security program?
    - **Evidence:** Review organizational charts or role definitions. Reference: Appendix A, Section III(A)(2).
  - Are roles and responsibilities adequately defined, and is there a designated person or team overseeing the security program?
- **Document Request:**
  - Organizational charts showing roles and responsibilities.
  - Records of oversight activities performed by designated security personnel.

# Core+ Validation

Friday, December 6, 2024 11:14 AM

## Responsibility and Accountability

- **Core+ Assessment:**
  - Reviewed the delineation of roles and responsibilities for information security across the organization.
  - Assessed the organizational structure to ensure accountability for tasks and governance.
- **Positive Finding:** "The information security program delineates roles and responsibilities across the organization with clarity, ensuring accountability for security-related tasks. This structure supports compliance with Appendix A, Section III(C)(1)(a)."
- **Negative Finding:** "Roles and responsibilities for information security tasks are ambiguously defined, resulting in gaps in accountability and weak governance structures."
- **Questions:**
  - Are the roles and responsibilities for information security clearly delineated across the organization?
    - **Evidence:** Review the organizational structure and role documentation. Reference: Appendix A, Section III(C)(1)(a).
  - Does the organizational structure ensure accountability for information security tasks and governance?
- **Document Request:**
  - Organizational charts and role documentation.
  - Records demonstrating accountability for information security governance.

## Training on Information Security Program

- **Core+ Assessment:**
  - Evaluated training schedules, materials, and attendance records for staff education on safeguarding member information and organizational security policies.
  - Assessed employee understanding security policies and compliance.
- **Positive Finding:** "Staff receive regular training on the ISP, with comprehensive materials and attendance records ensuring compliance with Appendix A, Section III(C)(1)(f)."
- **Negative Finding:** "Training on information security policies is infrequent or poorly documented, leading to employee knowledge gaps and non-compliance with safeguarding requirements."
- **Questions:**
  - Is staff regularly trained on safeguarding member information and the organization's security policies?
    - **Evidence:** Review training schedules, materials, and attendance records. Reference: Appendix A, Section III(C)(1)(f).
  - Do employees understand and comply with the credit union's information security policies?
- **Document Request:**
  - Training schedules, materials, and attendance records.
  - Surveys or assessments demonstrate employee understanding of security policies.

## Monitoring Information Systems for Intrusions

- **Core+ Assessment:**
  - Reviewed the implementation and effectiveness of intrusion detection systems (IDS) or other monitoring solutions to detect unauthorized access or system intrusions.
  - Assessed logs, alerts, and response procedures for thoroughness in identifying and addressing intrusions or suspicious activity.
- **Positive Finding:** "Intrusion detection and monitoring systems are robust, with continuous reviews of logs and alerts ensuring protection against cyber threats, in compliance with Appendix A, Section III(C)(1)(d)."
- **Negative Finding:** "Monitoring practices are insufficient, with inconsistent log reviews and delayed responses to alerts, leaving the credit union vulnerable to undetected intrusions."
- **Questions:**
  - Is there an IDS or monitoring solution in place to detect unauthorized access or system intrusions?
    - **Evidence:** Review logs, alerts, and response procedures for system monitoring. Reference: Appendix A, Section III(C)(1)(d).
  - Are monitoring practices thorough and capable of identifying intrusions or suspicious activity?
- **Document Request:**
  - IDS configuration details and monitoring procedures.
  - Logs, alerts, and response records.

## Establishment of Policies, Standards, and Procedures

- **Core+ Assessment:**
  - Verified that information security policies, standards, and procedures are well-documented, regularly updated, and aligned with industry best practices.
  - Evaluated whether established policies address key risks and comply with safeguarding requirements.

- **Positive Finding:** "Information security policies and standards are well-documented and regularly updated, addressing key risks in compliance with Appendix A, Section III(C)(1)."
- **Negative Finding:** "Policies and procedures are outdated or missing key updates, failing to address evolving risks and regulatory requirements."
- **Questions:**
  - Are information security policies, standards, and procedures documented, regularly updated, and aligned with industry best practices?
    - **Evidence:** Review policy documents and revision history. Reference: Appendix A, Section III(C)(1).
  - Do the established policies and procedures address key risks and comply with the safeguarding requirements of Appendix A?
- **Document Request:**
  - Policies, standards, and revision history documentation.
  - Evidence of policy compliance and effectiveness.

## Adjustments Over Time

- **Core+ Assessment:**
  - Examined revision histories, risk assessments, and updates to ensure the ISP evolves with changes in technology, threats, and business processes.
  - Evaluated whether adjustments are documented and address evolving risks.
- **Positive Finding:** "The ISP is regularly reviewed and updated to reflect new risks and technologies, demonstrating a proactive approach consistent with Appendix A, Section III(C)(1)(e)."
- **Negative Finding:** "The ISP lacks updates to address new risks, and risk assessments are outdated, leaving the credit union vulnerable to emerging threats."
- **Questions:**
  - Is the information security program reviewed and updated regularly to address changes in technology, threats, and business processes?
    - **Evidence:** Review program revision history, risk assessments, and updates. Reference: Appendix A, Section III(C)(1)(e).
  - Are adjustments properly documented, and do they reflect evolving risks in the cybersecurity landscape?
- **Document Request:**
  - Program revision history and risk assessments.
  - Records of adjustments addressing emerging threats.

## Actions

Thursday, September 19, 2024 9:53 AM

Remediating issues related to safeguarding member information and complying with **Appendix A to Part 748, Title 12** requires a structured approach that addresses each potential issue with targeted solutions. Below are recommended **remediation strategies** for each of the identified issues:

### Governance and Oversight

**Negative Finding:** Board approval of the information security program is missing or insufficient.

- **Remediation:**

- **Action:** Schedule an annual board review and formal approval process for the information security program. Include the program on the board's meeting agenda to ensure proper oversight.
- **Documentation:** Record meeting minutes and resolutions to demonstrate formal approval by the Board of Directors, in compliance with Appendix A, Section III(C)(1).

### Access Controls and Authentication

**Negative Finding:** Access controls are incomplete or weak, and authentication mechanisms are insufficient.

- **Remediation:**

- **Action:** Conduct a comprehensive review of access controls across all systems handling member information. Implement strong authentication methods (e.g., multi-factor authentication, role-based access).
- **Documentation:** Update access control policies to reflect best practices and ensure alignment with Appendix A, Section III(C)(1)(b).
- **Testing:** Perform periodic user access reviews to ensure that only authorized individuals can access sensitive information.

### Physical Access Restrictions

**Negative Finding:** Physical access controls are inadequate or outdated.

- **Remediation:**

- **Action:** Strengthen physical security measures, including restricted access to sensitive areas, surveillance systems, secure entry points, and logging of access to critical facilities.
- **Documentation:** Create or update policies for physical access control, ensuring they meet Appendix A, Section III(C)(1)(c) standards.
- **Training:** Ensure that all staff and security personnel are trained on physical access control procedures.

### Data Encryption

**Negative Finding:** Encryption methods are weak or inconsistently applied.

- **Remediation:**

- **Action:** Implement strong encryption standards (e.g., AES-256) for data at rest and in transit. Ensure encryption is consistently applied across all systems handling member information.
- **Documentation:** Update encryption policies and procedures to align with industry standards and Appendix A, Section III(C)(1)(b).
- **Monitoring:** Regularly audit encryption implementations to ensure ongoing compliance.

### Testing Key or Critical Controls

**Negative Finding:** Security control testing is not performed regularly or is insufficiently documented.

- **Remediation:**

- **Action:** Establish a formal schedule for regular testing of critical security controls (e.g., penetration testing, vulnerability assessments, and system audits).
- **Documentation:** Ensure that testing results are documented and any vulnerabilities are addressed promptly.
- **Follow-Up:** Use test results to refine and improve security controls, ensuring they meet the requirements of Appendix A, Section III(C)(1)(d).

### Segregation of Duties

**Negative Finding:** Segregation of duties is poorly defined or inadequate.

- **Remediation:**

- **Action:** Review and restructure roles and responsibilities to ensure appropriate segregation of duties, especially for access to sensitive systems and data.
- **Documentation:** Update organizational policies to reflect the separation of roles that minimize conflicts of interest, per Appendix A, Section III(C)(1)(b).
- **Monitoring:** Implement checks and balances to ensure duties remain appropriately segregated.

### Data Destruction and Media Sanitization

**Negative Finding:** Data destruction procedures are ineffective or undocumented.

- **Remediation:**

- **Action:** Implement secure data destruction methods, such as secure shredding for paper records and disk wiping for electronic media, to ensure that data cannot be recovered.
- **Documentation:** Develop and enforce a data destruction policy that complies with Appendix A, Section III(C)(1)(c), ensuring secure disposal of member information.
- **Audit:** Periodically audit data destruction practices to confirm they are being followed correctly.

### Security Program Responsibility

**Negative Finding:** Roles and responsibilities for the security program are unclear or not assigned.

- **Remediation:**

- **Action:** Assign clear roles and responsibilities for implementing and managing the security program. Designate specific individuals or teams to oversee different aspects of the program.
- **Documentation:** Update organizational charts and role descriptions to reflect security responsibilities, ensuring compliance with Appendix A, Section III(C)(1)(a).
- **Monitoring:** Ensure regular oversight and accountability for security program tasks.

## CORE+ Validation

### Responsibility and Accountability

**Negative Finding:** Roles for security responsibilities are ambiguous or insufficiently documented.

- **Remediation:**

- **Action:** Clearly define roles and accountability for security responsibilities across the organization. Ensure that every security task has an assigned owner.
- **Documentation:** Update the organizational structure and internal policies to reflect clear lines of responsibility, in compliance with Appendix A, Section III(C)(1)(a).

### Training on Information Security Program

**Negative Finding:** Staff training on the information security program is infrequent or poorly documented.

- **Remediation:**

- **Action:** Develop and implement a regular training program for all staff, focusing on the importance of safeguarding member information.
- **Documentation:** Maintain records of training sessions, including materials, dates, and attendees, to ensure compliance with Appendix A, Section III(C)(1)(f).
- **Testing:** Regularly assess the effectiveness of the training program through knowledge assessments or simulations.

### Monitoring Information Systems for Intrusions

**Negative Finding:** Monitoring of information systems for intrusions is insufficient or non-existent.

- **Remediation:**

- **Action:** Implement or upgrade intrusion detection and monitoring systems (e.g., IDS/IPS) to continuously monitor for unauthorized access and security threats.
- **Documentation:** Ensure that logs are reviewed regularly, and alerts are investigated in a timely manner.
- **Response Plan:** Develop and document a formal incident response plan for handling detected intrusions, ensuring compliance with Appendix A, Section III(C)(1)(d).

### Establishment of Policies, Standards, and Procedures

**Negative Finding:** Information security policies are either outdated or missing.

- **Remediation:**

- **Action:** Create or update comprehensive security policies, standards, and procedures to cover all critical areas (e.g., access controls, data encryption, physical security).
- **Documentation:** Ensure policies are regularly reviewed and updated to reflect industry best practices and compliance with Appendix A, Section III(C)(1).
- **Training:** Communicate updated policies to all relevant stakeholders to ensure proper understanding and adherence.

## **Adjustments Over Time**

**Negative Finding: The security program has not evolved to address new risks or threats.**

- **Remediation:**

- **Action:** Conduct regular risk assessments to identify emerging threats and update the information security program accordingly.
- **Documentation:** Maintain a revision history of the security program that reflects adjustments over time, ensuring it evolves to meet new risks.
- **Follow-Up:** Ensure that changes to the security program are communicated across the organization and that staff are trained on any new procedures.

## **General Remediation Steps for Final Review**

### **1. Governance and Accountability:**

- Ensure formal approval by the Board of Directors.
- Assign clear roles and responsibilities for the security program.
- Implement strong oversight and review mechanisms.

### **2. Security Controls:**

- Strengthen access controls, physical safeguards, encryption, and monitoring systems.
- Implement regular testing of security controls and document the results.
- Ensure that the program evolves to address new and emerging risks.

### **3. Compliance Documentation:**

- Maintain up-to-date documentation for all policies, procedures, and security controls.
- Ensure that all documentation aligns with Appendix A to Part 748, Title 12, and is available for audits or reviews.

## Definitions

Monday, December 2, 2024 12:47 PM

### Policies

**Definition:** High-level principles and rules that govern how an organization manages information security.

#### 1. Purpose and Scope

- Purpose of the policy (e.g., safeguard member information, comply with regulatory requirements).
- Scope of application (e.g., systems, data, personnel, third parties).

#### 2. Policy Statements

- Specific requirements (e.g., "Multi-factor authentication must be used for accessing sensitive systems").
- Prohibition of certain actions (e.g., "Unauthorized devices are not permitted on the corporate network").

#### 3. Roles and Responsibilities

- Responsibilities of various roles (e.g., CISO, IT team, employees, vendors).
- Delegation of authority for implementation and enforcement.

#### 4. Compliance and Enforcement

- Consequences of policy violations.
- References to applicable laws and regulations (e.g., 12 CFR Part 748, GDPR).

#### 5. Review and Approval

- Frequency of policy review.
- Approval process by senior management or the Board of Directors.

## Procedures

**Definition:** Step-by-step instructions to implement policies.

#### 1. Purpose

- Link to the corresponding policy.
- Objective of the procedure (e.g., "Ensure secure access to member data").

#### 2. Detailed Steps

- Step-by-step guidance for tasks (e.g., onboarding new users, applying patches).
- Include flowcharts or diagrams for complex procedures.

#### 3. Roles and Responsibilities

- Identify individuals or teams responsible for executing each step.

#### 4. Tools and Resources

- Reference required tools, systems, or documents (e.g., ServiceNow, configuration management databases).

#### 5. Review and Maintenance

- Periodic review to ensure relevance and accuracy.

## Standards

**Definition:** Mandatory rules and technical specifications to ensure consistency.

#### 1. Purpose

- Define what the standard is designed to achieve.

#### 2. Technical Requirements

- Security configurations (e.g., "All systems must use AES-256 encryption for data at rest").
- Specifications for hardware, software, or network settings.

#### 3. Industry Best Practices

- Align with standards like NIST, ISO 27001, or PCI-DSS.

#### 4. Compliance Metrics

- Define measurable benchmarks for compliance (e.g., "95% of systems must meet patching requirements within 30 days of release").

## Guidelines

**Definition:** Recommendations or best practices to support the implementation of policies, standards, and procedures.

#### 1. Purpose

- Explain how the guideline supports broader policies or standards.

#### 2. Best Practices

- Security recommendations (e.g., “Users should create passwords of at least 12 characters with a mix of letters, numbers, and symbols”).
- 3. **Examples**
  - Provide illustrative examples to clarify complex recommendations.
- 4. **Flexibility**
  - Clarify that guidelines are advisory and not mandatory unless otherwise specified.

## Common Elements Across All Categories

- **Alignment with Regulations:** Include references to specific laws (e.g., 12 CFR Part 748, GDPR, HIPAA).
- **References:** Link to related policies, standards, and procedures.
- **Version Control:** Maintain records of revisions, approvals, and effective dates.
- **Training and Awareness:** Outline how employees will be informed about these documents.
- **Accessibility:** Ensure these documents are easily accessible to all relevant stakeholders.

## Specific Topics to Include

1. **Access Control:**
  - Roles, permissions, and authentication mechanisms.
2. **Data Protection:**
  - Encryption standards, data retention, and data destruction.
3. **Incident Response:**
  - Processes for detecting, responding to, and reporting security incidents.
4. **Risk Management:**
  - Regular assessments, mitigation strategies, and risk acceptance criteria.
5. **Vendor Management:**
  - Security requirements for third-party vendors and service providers.
6. **Physical Security:**
  - Measures to restrict physical access to sensitive areas.
7. **Change Management:**
  - Approval and testing processes for system or software changes.
8. **Monitoring and Auditing:**
  - Procedures for logging, monitoring, and reviewing security events.
9. **Training and Awareness:**
  - Requirements for employee education on security policies and best practices.
10. **Program Review and Updates:**
  - Frequency and triggers for reviewing and updating documents.

# Core Review Summary

Monday, December 2, 2024 12:48 PM

- **Governance and Oversight**
  - Assessed whether the **Board of Directors** had formally approved the ISP.
  - Verified alignment with strategic objectives through a review of **board meeting minutes and resolutions**.
- **Access Controls and Authentication**
  - Evaluated documentation for **access controls** and **authentication mechanisms**, including the implementation of **multi-factor authentication (MFA)**.
  - Confirmed the existence of robust measures to safeguard member information and minimize risks of unauthorized access.
- **Physical Access Restrictions**
  - Reviewed physical security measures, such as **secure premises** and **surveillance systems**, to determine their effectiveness in preventing unauthorized access to sensitive areas.
- **Data Encryption**
  - Examined encryption protocols, including **AES-256**, to ensure adequate protection of member information during storage and transmission.
- **Testing of Key Security Controls**
  - Analyzed testing schedules, **penetration testing reports**, and **system audits** to confirm the regularity and effectiveness of security control testing.
  - Verified that follow-up actions were documented and addressed vulnerabilities promptly to mitigate risks.
- **Segregation of Duties**
  - Assessed role definitions to ensure clear segregation of duties, supported by documentation of **roles** and **access permissions**, to prevent unauthorized access or conflicts of interest.
- **Data Destruction and Media Sanitization**
  - Reviewed procedures for **secure data destruction** and **media sanitization** to verify compliance with standards and the adequacy of implemented methods.
  - Evaluated evidence, such as **destruction logs**, to confirm effectiveness.
- **Responsibility for Security Program**
  - Confirmed the assignment of responsibility for the ISP through **organizational charts** and **role definitions**.
  - Ensured accountability with a designated team or individual overseeing the program's implementation and maintenance.

## Findings Summary

- **Strengths Identified:**
  - The ISP demonstrates a structured approach to data protection, leveraging MFA, AES-256 encryption, and periodic penetration testing.
  - Physical safeguards and data destruction policies are effectively documented and implemented.
  - Roles and responsibilities are clearly defined to ensure accountability.
- **Gaps Noted:**
  - Lack of consistent board approval for the ISP in meeting minutes or resolutions.
  - Testing of key controls is irregular, with some vulnerabilities left unaddressed.
  - Segregation of duties documentation requires updates to prevent potential conflicts.

# Core+ Review Summary

Friday, December 6, 2024 11:17 AM

## 1. Training on Safeguarding Member Information

- Assessed training programs for staff on the importance of **safeguarding member information** and adhering to security policies.
- Reviewed **training schedules, materials, and attendance records** to confirm regular employee education.
- Verified compliance with **Appendix A, Section III(C)(1)(f)** by ensuring employees were adequately informed of their roles in maintaining information security.

## 2. Monitoring Information Systems for Intrusions

- Evaluated the implementation and effectiveness of **intrusion detection systems (IDS)** and monitoring solutions.
- Reviewed **logs, alerts, and incident response procedures** to confirm the thoroughness of practices in detecting and addressing unauthorized access or suspicious activities.
- Ensured alignment with **Appendix A, Section III(C)(1)(d)** for proactive monitoring and response mechanisms.

## 3. Policies, Standards, and Procedures

- Analyzed the documentation of **policies, standards, and procedures** to confirm that they were:
  - Regularly updated.
  - Aligned with industry best practices.
  - Addressing key risks associated with information security.
- Verified the establishment of a **robust policy framework** to support compliance with regulatory requirements.

## 4. Adaptability and Adjustments Over Time

- Examined **program revision histories, risk assessments, and updates** to confirm that the ISP evolves in response to:
  - Emerging technologies.
  - New cybersecurity threats.
  - Changing business processes.
- Verified proper documentation of updates and alignment with **Appendix A, Section III(C)(1)(e)** to maintain relevance in a dynamic threat landscape.

## Findings Summary

### • Strengths Identified:

- The ISP incorporates a regular **training program** that equips employees with the knowledge to safeguard member information effectively.
- Robust **monitoring practices** using IDS and comprehensive logs demonstrate proactive detection of and response to potential threats.
- Policies, standards, and procedures are well-documented and regularly updated to reflect industry best practices.
- The program demonstrates adaptability through periodic updates and risk assessments, ensuring alignment with evolving cybersecurity demands.

### • Gaps Noted:

- **Training records** lack consistency, with some employees not completing mandatory training sessions, increasing the risk of non-compliance with policies.
- Inconsistent **log review and incident response procedures** result in delayed responses to potential security breaches.
- Documentation of updates and adjustments to the ISP is incomplete, making it difficult to verify responsiveness to emerging risks and threats.

## Recommendations

To enhance the effectiveness of the ISP and address identified gaps:

### 1. Training Improvements:

- Develop a mechanism to track and enforce completion of mandatory training sessions.
- Regularly assess training materials for relevance and ensure they address emerging cybersecurity risks.

### 2. Enhance Monitoring Practices:

- Implement automated systems for consistent log review and ensure timely investigation of alerts.
- Strengthen incident response procedures to minimize delays in addressing threats.

### 3. Documentation of Adjustments:

- Establish a systematic process to document program revisions, risk assessments, and updates.
- Ensure updates reflect changes in the technology landscape and regulatory requirements.

# Decision Matrix for Evaluating Information Security Program (ISP) Performance

Friday, December 6, 2024 11:33 AM

Rating	Criteria	Indicators
<b>Strong</b>	Fully compliant with regulatory requirements and exceeds expectations.	<ul style="list-style-type: none"><li>- Board-approved ISP with comprehensive documentation.</li><li>- Robust access controls, including MFA for all sensitive systems.</li><li>- Well-documented and updated policies aligned with industry best practices.</li><li>- Effective physical and data security measures.</li><li>- Proactive adjustments to address emerging risks.</li><li>- No material findings.</li></ul>
<b>Satisfactory</b>	Compliant with regulatory requirements and meets expectations, with minor areas for improvement.	<ul style="list-style-type: none"><li>- ISP is Board-approved, with minor gaps in documentation.</li><li>- Access controls and encryption meet requirements but lack periodic testing.</li><li>- Training is provided but could be more frequent.</li><li>- Security monitoring and incident response are functional but could improve in timeliness or consistency.</li><li>- Few minor findings.</li></ul>
<b>Less than Satisfactory</b>	Partially compliant with regulatory requirements; requires improvements to meet expectations.	<ul style="list-style-type: none"><li>- ISP lacks recent Board approval or documentation.</li><li>- Inconsistent implementation of access controls or encryption.</li><li>- Training records are incomplete, with gaps in employee participation.</li><li>- Incident response is reactive rather than proactive.</li><li>- Several moderate findings requiring corrective actions.</li></ul>
<b>Deficient</b>	Non-compliant with several regulatory requirements; significant improvements needed.	<ul style="list-style-type: none"><li>- ISP is outdated or lacks Board approval.</li><li>- Significant gaps in access controls or encryption protocols.</li><li>- Security monitoring is irregular, with delayed responses to incidents.</li><li>- Policies are outdated and do not address current risks.</li><li>- Numerous findings with moderate to severe impact.</li></ul>
<b>Critically Deficient</b>	Systemically non-compliant with regulatory requirements; poses critical risks to the organization.	<ul style="list-style-type: none"><li>- No evidence of Board-approved ISP.</li><li>- Critical gaps in access controls and encryption expose sensitive data.</li><li>- Training, monitoring, and testing are either absent or ineffective.</li><li>- Policies and procedures are nonexistent or severely outdated.</li><li>- Severe findings with material impact on member data security.</li></ul>

## Application of the Matrix

### 1. Key Evaluation Areas:

- **Governance and Oversight:** Board approval and program alignment with strategic goals.
- **Access Controls and Authentication:** Effectiveness of controls and implementation of MFA.
- **Physical Access Restrictions:** Robustness of physical security measures.
- **Data Encryption:** Alignment of encryption protocols with industry standards.
- **Testing and Monitoring:** Frequency and thoroughness of security control tests and incident monitoring.
- **Training and Awareness:** Consistency and effectiveness of employee training.
- **Policy and Program Updates:** Relevance and adaptability of policies to emerging risks.

### 2. Decision Framework:

- Assign a rating for each key evaluation area using the decision matrix.
- Determine the overall ISP rating based on the aggregate performance across areas.

### 3. Example Evaluation Using the Decision Matrix

Key Area	Rating	Rationale
----------	--------	-----------

Governance and Oversight	Satisfactory	The ISP is Board-approved, but documentation requires minor updates to meet best practices.
Access Controls	Less than Satisfactory	MFA is implemented for some systems, but critical systems lack robust authentication measures.
Physical Access	Satisfactory	Physical security measures are adequate but require improved logging practices.
Data Encryption	Strong	Encryption protocols meet and exceed industry standards, with consistent application of AES-256.
Testing and Monitoring	Less than Satisfactory	Irregular testing schedules and delayed follow-up on vulnerabilities reduce effectiveness.
Training and Awareness	Deficient	Training sessions are infrequent, with incomplete participation records and outdated materials.
Policy and Updates	Less than Satisfactory	Policies are outdated and lack recent updates to address new risks and threats.

**Overall Rating: Less than Satisfactory**

**Conclusion:** The ISP demonstrates compliance in some areas but requires targeted improvements to meet regulatory requirements and organizational goals. Prioritize addressing deficiencies in training, testing, and policy updates to elevate the overall rating.

# Examiner Findings

Wednesday, December 11, 2024 9:41 AM

## **Examiner Finding: Information Security Officer Reporting to the CIO**

### **Situation (S)**

During an examination of the credit union's governance structure for information security, it was observed that the Information Security Officer (ISO) reports directly to the Chief Information Officer (CIO). The review was conducted as part of assessing compliance with 12 CFR Part 748 regarding the safeguarding of member information and the segregation of duties within the information security program.

### **Behavior (B)**

The reporting structure places the ISO under the CIO's direct authority, potentially compromising the independence required to objectively assess and mitigate information security risks. This reporting relationship may inhibit the ISO from adequately challenging IT operations or escalating unresolved security concerns directly to executive management or the board.

### **Impact (I)**

This lack of independence increases the risk of conflicts of interest, as the CIO is responsible for IT operations that the ISO is tasked with monitoring and securing. Such a structure could hinder effective oversight, compromise the integrity of the information security program, and potentially result in non-compliance with regulatory requirements under 12 CFR Part 748.

### **Resolution (R)**

To enhance compliance and address independence concerns:

1. **Revised Reporting Structure:** Adjust the governance framework so the ISO reports directly to the CEO, Chief Risk Officer (CRO), or Board of Directors. This aligns with best practices and ensures independent oversight of IT security operations.
2. **Enhanced Board Engagement:** Establish periodic reporting by the ISO to the board or a designated committee, such as the Audit or Risk Committee, to maintain direct oversight.
3. **Policy Update:** Update the information security governance policy to formally document the revised reporting lines and ensure the ISO's autonomy in security matters.
4. **Regular Audits:** Conduct independent audits to evaluate the effectiveness of the revised structure and ensure ongoing compliance with regulatory expectations.

These actions will strengthen the independence of the information security function, improve risk management, and align the organization with 12 CFR Part 748 requirements.

# Notes

Tuesday, September 3, 2024 6:15 AM