2.The annual report to the Board on the overall status of the information security program includes the following:

Tuesday, August 13, 2024 3:46 PM

Reference: Appendix A to Part 748, Title 12

1. Review of the Annual Report

- **Objective:** Ensure the report to the Board of Directors contains the required elements outlined in the statement, including risk assessments, testing results, information security controls, and security incidents.
- **Area of Focus:** Comprehensive content of the annual report to the Board.
    - **Reference:** Appendix A to Part 748, I.C.2.
- **What Needs to Be in the Report to the Board of Directors:**
    - Summaries of all major elements of the information security program, including:
        - Risk assessments, testing results, and security incidents.
        - Updates on previous findings and their resolution.
        - Changes to security policies or processes during the reporting period.
        - Date provided to the Board
        - Reporting structure
- **Document Review List:**
    - Most recent annual report to the Board of Directors.
    - Documentation of prior Board reports for comparison.
    - Supporting documents for risk assessments, testing results, and incidents.
- **Positive Findings:**
    - The report covers all required elements, including risk assessments, control testing results, security incidents, and management's responses.
    - The report includes updates on progress toward addressing previously identified gaps.
- **Negative Findings:**
    - Key elements such as security incidents or control testing results are missing or incomplete.
    - Findings from prior assessments were not addressed or updated in the current report.

2. CORE Statements Validation

Stmt 2.1: Results from the Information Security Risk Assessment

- **Objective:** Ensure the report to the Board of Directors includes results from the information security risk assessment, covering internal and external risks, their impacts, and mitigation strategies.
- **Area of Focus:** Risk identification, evaluation, and mitigation.
    - **Reference:** Appendix A to Part 748, III.B.
- **What Needs to Be in the Report to the Board of Directors:**
    - A detailed summary of internal and external risks identified during the risk assessment.
    - Analysis of the impact and likelihood of these risks.
    - Documentation of mitigation strategies implemented.
    - Updates on previously identified risks and their resolution status.
    - Date reported to the Board
- **Document Review List:**
    - Most recent risk assessment report.
    - Prior risk assessments for comparison.
    - Documentation of mitigation strategies and tracking logs.
- **Positive Findings:**
    - The assessment identifies both internal and external risks with detailed impact analysis and mitigation strategies.
    - Risks associated with third-party relationships are clearly outlined and addressed.
- **Negative Findings:**
    - The risk assessment lacks documentation of certain risks or mitigation strategies.
    - Findings from prior risk assessments remain unresolved or untracked.

Stmt 2.2: Control Arrangements with Service Providers

- **Objective:** Ensure the report to the Board of Directors includes details on control arrangements with service providers, including reviews of their security practices and compliance with contractual security requirements.

- **Area of Focus:** Security of third-party relationships.
    - **Reference:** Appendix A to Part 748, III (D)
- **What Needs to Be in the Report to the Board of Directors:**
    - A list of service providers with access to sensitive member information.
    - Results of periodic reviews of service providers' security practices.
    - Documentation of compliance with contractual security requirements.
    - Updates on any deficiencies identified and the actions taken to resolve them.
- **Document Review List:**
    - Contracts with service providers.
    - Reports from periodic reviews of service providers.
    - Documentation of deficiencies and remediation actions.
- **Positive Findings:**
    - All service provider contracts include robust information security requirements.
    - Periodic reviews demonstrate strong security practices by third-party providers.
- **Negative Findings:**
    - Contracts with some service providers lack specific information security requirements.
    - Service provider reviews are outdated or inconsistently performed.

Stmt 2.3: Results of Testing Key or Critical Controls

- **Objective:** Ensure the report to the Board of Directors includes results of testing for key or critical controls, documenting effectiveness and remediation actions.
- **Area of Focus:** Effectiveness of key or critical controls.
    - **Reference:** Appendix A to Part 748, III.C.3.
- **What Needs to Be in the Report to the Board of Directors:**
    - A summary of key or critical controls tested during the reporting period.
    - Results of these tests, including identified weaknesses and remediation actions.
    - Updates on previously identified issues and their resolution.
- **Document Review List:**
    - Reports of control testing activities.
    - Documentation of remediation plans and progress reports.
    - Logs of control-related incidents and resolutions.
- **Positive Findings:**
    - Testing is conducted on schedule, with detailed and actionable results documented.
    - Identified issues are promptly resolved, and control effectiveness is verified.
- **Negative Findings:**
    - Testing schedules are delayed, or results are not documented.
    - Critical control failures remain unaddressed or lack follow-up action plans.

Stmt 2.4: Security Incidents and Management's Response

- **Objective:** Ensure the report to the Board of Directors includes a summary of security incidents and management's responses, along with lessons learned.
- **Area of Focus:** Incident reporting and response actions.
    - **Reference:** Appendix A to Part 748, III.C.1.f
- **What Needs to Be in the Report to the Board of Directors:**
    - A summary of all security incidents during the reporting period.
    - Classification of incidents by type, scope, and impact.
    - Details on management's response to each incident.
    - Lessons learned and updates to the security program based on incident reviews.
- **Document Review List:**
    - Security incident reports for the reporting period.
    - Logs of incident classification and response activities.
    - Documentation of lessons learned and updates to policies or procedures.
- **Positive Findings:**
    - All incidents are documented with clear analysis of scope, impact, and resolution.
    - Lessons learned are incorporated into updated security measures.
- **Negative Findings:**
    - Incident documentation is incomplete, or responses are delayed.
    - Lessons learned are not reflected in subsequent security enhancements.

Stmt 2.5: Oversee Risk Mitigation Activities

- **Objective:** Ensure the report to the Board of Directors includes an overview of risk mitigation activities, progress, and alignment with the credit union's information security strategy.
- **Area of Focus:** Ongoing risk mitigation and alignment with strategy.
    - **Reference:** Appendix A to Part 748, III.C.1.
- **What Needs to Be in the Report to the Board of Directors:**
    - A summary of ongoing risk mitigation activities.
    - Progress reports on previously identified mitigation efforts.
    - Documentation of challenges or delays encountered during mitigation.
- **Document Review List:**
    - Logs tracking risk mitigation efforts.
    - Documentation of challenges or delays encountered.
    - Records of updates provided to the Board.
- **Positive Findings:**
    - Mitigation activities are well-documented, aligned with strategic goals, and show measurable risk reduction.
    - Regular updates are provided to the Board.
- **Negative Findings:**
    - Mitigation activities are poorly documented or show limited progress.
    - The Board is not regularly updated on risk mitigation efforts.

Stmt 2.6: Implement a Risk Acceptance Process

- **Objective:** Ensure the report to the Board of Directors includes details on accepted risks, their justification, monitoring activities, and instances of re-evaluated risks.
- **Area of Focus:** Process for accepting and documenting risks.
    - **Reference:** Appendix A to Part 748, III.C.2.
- **What Needs to Be in the Report to the Board of Directors:**
    - Documentation of risks accepted during the reporting period, including justification and approval.
    - Confirmation of management and stakeholder involvement in risk acceptance decisions.
    - Details on monitoring activities for accepted risks and any re-evaluated risks.
- **Document Review List:**
    - Risk acceptance documentation, including approvals and justifications.
    - Logs of accepted risks and associated monitoring activities.
    - Records of re-evaluated risks and changes made.
- **Positive Findings:**
    - Accepted risks are documented with clear justification and approved by stakeholders.
    - Monitoring activities are ongoing and include updates to the Board.

- **Negative Findings:**
    - Risk acceptance decisions lack documentation or justification.
    - The Board is not informed of significant risk acceptance decisions.

Stmt 2.7: Approve Risk Thresholds Relating to Information Security Threats or Incidents

- **Objective:** Ensure the report to the Board of Directors includes approved risk thresholds, details of incidents exceeding these thresholds, and rationale for changes to thresholds.
- **Area of Focus:** Governance and escalation of risk thresholds.
    - **Reference:** Appendix A to Part 748, III.C.2.
- **What Needs to Be in the Report to the Board of Directors:**
    - Defined and approved risk thresholds with clear alignment to the credit union's risk appetite.
    - A summary of incidents exceeding thresholds, including escalation details.
    - Documentation of periodic reviews and any changes made to thresholds.
- **Document Review List:**
    - Records of approved risk thresholds.
    - Incident reports for threshold-exceeding events.
    - Logs of reviews and changes to risk thresholds, including rationale.
- **Positive Findings:**
    - Risk thresholds are clearly defined, periodically reviewed, and communicated effectively.
    - Incidents exceeding thresholds are promptly escalated and documented.
- **Negative Findings:**
    - Risk thresholds are outdated or unclear.
    - Threshold-exceeding incidents are not escalated appropriately or lack supporting documentation.

Stmt 2.8: Monitoring Reports Related to Patching, Vulnerability Management, or Other Areas

- **Objective:** Ensure the report to the Board of Directors includes summaries of monitoring reports related to patching, vulnerability management, and other critical areas.
- **Area of Focus:** Reporting and monitoring security-related activities.
    - **Reference:** Appendix A to Part 748, III.C.3.
- **What Needs to Be in the Report to the Board of Directors:**
    - Summaries of monitoring activities, including patch deployment status and vulnerability management.
    - Documentation of recurring issues or trends identified during monitoring.
    - Updates on delays or issues and actions taken to address them.
- **Document Review List:**
    - Monitoring reports for patching, vulnerability management, and other areas.
    - Records of delays, issues, and resolutions.
    - Logs of recurring trends or systemic issues.

- **Positive Findings:**
    - Monitoring reports are accurate, reliable, and include actionable insights.
    - Regular updates are provided to the Board, including progress and resolutions.
- **Negative Findings:**
    - Reports are incomplete, outdated, or lack detail.
    - Recurring issues are not adequately documented or addressed.

Resources

Thursday, August 15, 2024 9:48 AM

Metrics aid management in its ability to assess the overall IT environment. The specific metrics reported, and the frequency with which they are reported, depend on the institution's IT environment. The following are common examples:

- Number of risk issues identified for IT activities (updated regularly to reflect new or mitigated issues). This may include information gathered through the threat intelligence and collaboration process.
- Number of risk acceptance issues approved by senior management. This information may be maintained in a database or other repository of the descriptions, mitigation options, and documentation of management acceptance.
- Number of current and historical events or issues (external and internal events that deviate from the control standards).
- Number of current or outstanding (i.e., unresolved) issues identified by the business unit, internal audit, external audit, or regulator.

From <https://ithandbook.ffiec.gov/it-booklets/management/iii-it-risk-management/iiid-monitoring-and-reporting/iiid1-metrics.aspx>

Core Review Summary

Monday, December 9, 2024 1:35 PM

1. **Stmt 2.1: Results from the Information Security Risk Assessment**
    - Reviewed the most recent **information security risk assessment**, ensuring it comprehensively identified internal and external risks, analyzed their impact and likelihood, and outlined corresponding mitigation strategies.
    - Verified the inclusion of risks associated with third-party relationships.
    - Assessed the documentation of actions taken to address findings from prior risk assessments.
2. **Stmt 2.2: Control Arrangements with Service Providers**
    - Examined control arrangements with **third-party service providers** that have access to sensitive member information.
    - Validated the presence of security provisions in contracts, results of periodic security practice reviews, and documentation of any identified deficiencies and their resolution.
3. **Stmt 2.3: Results of Testing Key or Critical Controls**
    - Reviewed documentation of testing performed on key or critical information security controls during the reporting period.
    - Verified that results of the testing were documented, issues were addressed, and follow-up actions were implemented.
4. **Stmt 2.4: Security Incidents and Management's Response**
    - Analyzed reports summarizing security incidents, focusing on type, scope, and impact.
    - Reviewed management's response to incidents and incorporation of lessons learned into the information security program.

- **Stmt 2.5: Oversee Risk Mitigation Activities**
  - Reviewed ongoing **risk mitigation efforts** to confirm alignment with the information security strategy.
  - Evaluated documentation of progress, updates provided to the Board, and challenges or delays in mitigation activities.
- **Stmt 2.6: Implement a Risk Acceptance Process**
  - Assessed the **risk acceptance process** to ensure that accepted risks were justified, documented, and approved by management and stakeholders.
  - Verified that significant risk acceptance decisions were communicated to the Board and that monitoring activities were in place for accepted risks.
  - Reviewed documentation of any re-evaluated risks and updates made.
- **Stmt 2.7: Approve Risk Thresholds Relating to Information Security Threats or Incidents**
  - Examined the establishment and **approval of risk thresholds** to ensure they were well-defined, aligned with the credit union's risk appetite, and periodically reviewed.
  - Reviewed documentation of incidents exceeding these thresholds, escalation processes, and updates made to the thresholds, including the rationale for changes.
- **Stmt 2.8: Monitoring Reports Related to Patching, Vulnerability Management, or Other Areas**
  - Reviewed **monitoring reports** on patching, vulnerability management, and other critical security areas to ensure accuracy, reliability, and timeliness.
  - Evaluated documentation of recurring issues, delays, and actions taken to resolve them.
  - Assessed whether updates from monitoring activities were regularly communicated to the Board.

Decision Matrix for CORE and CORE+ Statements

Monday, December 9, 2024 1:45 PM

Rating	Criteria for CORE and CORE+ Statements	Description of Performance
Strong	- Fully satisfies all CORE and CORE+ statement requirements. - Risk assessments, controls, and incident responses are well-documented and proactively managed. - Service provider controls are exemplary. - Board reporting is comprehensive and fully aligned with Appendix A to Part 748.	- All aspects of the program, including risk assessments, control testing, third-party management, and Board reporting, exceed expectations. - Issues are negligible or resolved immediately. - Documentation is thorough, accurate, and up-to-date. - Board engagement is proactive and well-informed.
Satisfactory	- Meets most CORE and CORE+ requirements with only minor deviations. - Risk assessments, controls, and incident responses are functional and effective. - Service provider reviews are adequate. - Board reporting is generally compliant but may lack some minor details.	- The program is generally effective, though minor areas for improvement exist. - Risk mitigation and control testing processes are adequate but may not demonstrate innovation. - Board reporting covers required areas but may miss advanced insights or proactive measures.
Less Than Satisfactory	- Meets some but not all CORE and CORE+ requirements. - Risk assessments or control testing exhibit notable gaps. - Service provider management lacks consistency. - Board reporting is incomplete or delayed, with missing elements from Appendix A to Part 748.	- Certain components of the program are underperforming, with deficiencies in risk assessment, third-party controls, or incident reporting. - Documentation lacks detail, and follow-up actions for identified issues may be inconsistent. - Board awareness and engagement are limited.
Deficient	- Fails to meet several CORE and CORE+ requirements. - Risk assessments, controls, or incident responses are poorly executed or inconsistently applied. - Service provider controls are inadequate. - Board reporting is significantly lacking or non-compliant with Appendix A to Part 748.	- Deficiencies in the program present notable risks to information security. - Service provider and risk acceptance processes lack thorough reviews or documentation. - Risk thresholds or monitoring reports are unreliable or absent. - Board is not sufficiently informed of program issues.
Critically Deficient	- Fails to meet most or all CORE and CORE+ requirements. - Risk assessments, controls, and incident responses are non-existent or ineffective. - Service provider controls are absent or severely lacking. - Board reporting is absent or grossly non-compliant with Appendix A to Part 748.	- The program is in critical failure, with severe deficiencies in risk management, control effectiveness, and incident response. - Service providers are unmanaged or pose unmitigated risks. - Board is unaware of systemic issues or program failures. - Immediate corrective actions are required.

Step 1: Identify Key Evaluation Areas

Evaluate the following critical areas for each CORE and CORE+ statement:

1. **Risk Management:**
   - Completeness and accuracy of risk assessments.
   - Identification, evaluation, and mitigation of risks.
   - Documentation of risk thresholds and accepted risks.
2. **Control Effectiveness:**
   - Testing and validation of key or critical controls.
   - Results of periodic reviews and follow-up actions.
3. **Incident Response:**
   - Reporting, classification, and resolution of security incidents.
   - Lessons learned and their integration into the program.
4. **Third-Party Management:**
   - Security arrangements and oversight for service providers.
   - Compliance with contractual obligations and remediation of deficiencies.
5. **Board Engagement:**
   - Quality and timeliness of reporting to the Board.
   - Inclusion of all required elements as outlined in Appendix A to Part 748.
6. **Monitoring and Reporting:**
   - Reliability and timeliness of monitoring reports.
   - Resolution of recurring trends, delays, or issues.

Step 2: Apply the Decision Tree

Use the following decision tree to categorize performance based on the evaluation results:

Decision Tree for Performance Ratings

1. **Does the program fully meet the statement requirements?**
   - **Yes:** Move to Step 2.
   - **No:** Assign a preliminary rating of **Less Than Satisfactory** or lower and proceed to Step 4.
2. **Are the processes and documentation proactive, complete, and up-to-date?**
   - **Yes:** Assign a preliminary rating of **Strong**.
   - **No:** Assign a preliminary rating of **Satisfactory**.
3. **Are there opportunities for minor improvements?**
   - **Yes:** Adjust the rating to **Satisfactory** with recommendations for optimization.
   - **No:** Confirm the rating as **Strong**.
4. **Are the deficiencies causing tangible risks to the credit union?**
   - **Yes:** Assign a preliminary rating of **Deficient** or **Critically Deficient** based on severity.
   - **No:** Assign a preliminary rating of **Less Than Satisfactory**.
5. **Are there systemic or repeated failures?**
   - **Yes:** Confirm the rating as **Critically Deficient**.
   - **No:** Confirm the rating as **Deficient** or adjust based on severity.

Step 3: Make a Decision and Document Findings

After following the decision tree:

1. **Finalize the Rating:** Based on the decision tree outcome, assign one of the following ratings:
    - **Strong**
    - **Satisfactory**
    - **Less Than Satisfactory**
    - **Deficient**
    - **Critically Deficient**
2. **Document Findings:** Include evidence, such as:
    - Documentation reviewed (e.g., risk assessments, incident reports, monitoring logs).
    - Observed gaps or deficiencies.
    - Actions taken or recommended to address issues.

24-CU-02 / October 2024

Tuesday, February 25, 2025 12:10 PM

Board of Director Engagement in Cybersecurity Oversight
To Federally Insured Credit Unions
Subject Cybersecurity
Status Active
Dear Boards of Directors and Chief Executive Officers:

The frequency, speed, and sophistication of cyberattacks have increased at an exponential rate. Foreign adversaries and cyber-fraudsters continue to target all sectors of our nation's critical infrastructure — including credit unions and other financial institutions. From September 1, 2023, the effective date of the NCUA's cyber incident notification rule, through August 31, 2024, federally insured credit unions reported 1,072 cyber incidents. Seven out of ten of these cyber incident reports were related to the use or involvement of a third-party vendor.

A recent ransomware attack on a credit union has been attributed to " This is an external link to a website belonging to another federal agency, private organization, or commercial entity. malvertising (Opens new window) ," a relatively new cyberattack technique that injects malicious code within digital ads. For this type of attack to work, the user doesn't even have to physically click on a link for the system to become infected. Instead, a simple internet search can result in malvertising that exploits the vulnerabilities in an internet browser. Credit union cybersecurity teams should focus on standardizing and securing web browsers and deploying ad blocking software to protect against this threat.
Given the proliferation of sophisticated information security threats and the importance of safeguarding the assets and information of your members, the NCUA urges credit union boards of directors to prioritize cybersecurity as a top oversight and governance responsibility. Credit union board directors like you must ensure that a credit union's senior leadership is highly focused on managing cyber risks and that your credit union has the necessary resources to maintain an effective cybersecurity program that aligns with the products, services, and risk profile of your institution.
The following are four key areas your board of directors should focus on:

Provide for Recurring Training

Your board should engage in ongoing education about current cybersecurity threats, trends, and best practices. The NCUA provides various resources to assist, including training webinars, web-based learning resources (Opens new window) , and written guidance. Your credit union board needs to stay aware of the specific cyber risks that pertain to your credit union's operations and the implications of these risks. Board members don't need to be technical experts, but they must know enough about cybersecurity to provide effective oversight and direction for the executive team and subject matter experts.
Furthermore, your board should ensure the credit union's employees receive regular cybersecurity education to maintain high awareness and preparedness across the organization. This education should emphasize the importance of a security-minded culture and adherence to important information security practices to mitigate the risk of cyber incidents.

Approve Information Security Program

Your board must approve a comprehensive information security program that meets the requirements of This is an external link to a website belonging to another federal agency, private organization, or commercial entity. Part 748 (Opens new window) of the NCUA's regulations, which includes risk

assessments, security controls, and incident response plans. Your credit union board should review the program at least annually to ensure it adapts to the evolving threat landscape and incorporates lessons learned from past incidents.

Oversee Operational Management

Your board is responsible for overseeing management of the credit union, focusing on the following cybersecurity areas:

- ***Third-Party Due Diligence***. Your board should set clear expectations for management about the due diligence of third-party vendors with respect to information security. The credit union must ensure that contracts with third-party vendors include specific cybersecurity requirements, like timely notification to the credit union of any incidents, and clauses that protect credit union and member data.
- ***Embed Cybersecurity and Operational Resilience into the Organizational Culture***. Your board and management should ensure that cybersecurity is a core value within the credit union, influencing decision-making at all levels.
- ***Resources***. Your board must provide management access to cybersecurity expertise and an adequate budget to implement and maintain a cybersecurity posture commensurate with the credit union's risk profile. Your board should also encourage needed investment in cybersecurity technologies and tools to enhance the credit union's defenses.
- ***Vulnerability/Patch Management and Threat Intelligence***. Your board must ensure that operational management places high emphasis on diligent vulnerability management, including timely software updates, patch management, and whitelisting and blacklisting URLs, websites, and software to mitigate risks. The credit union should use threat intelligence to stay informed about emerging threats and vulnerabilities that could impact the credit union. Government resources such as the Cybersecurity and Infrastructure Security Agency's cyber hygiene service for vulnerability management and the U.S. Treasury's automated threat information feed are free to credit unions.[1]
- ***Audit Function***. Consistent with the size and risk profile of the credit union, your board should ensure management engages external parties with the requisite expertise to conduct audits of the cybersecurity program, to receive an objective assessment of program effectiveness.
- ***Reporting***. Your board should establish a framework for periodic reporting by management to the board on cybersecurity audits, incidents, and the effectiveness of the cybersecurity program. This reporting should include cybersecurity risk assessments, including the identification of threats, vulnerabilities, and the effectiveness of controls. These reports should describe the overall status of the program. Reports should also outline material matters related to the program, including risk assessments, risk-management and control decisions, service provider arrangements, results of testing, and any recommendations for changes in the cybersecurity program.
- ***Protecting and Managing Backups***. In the face of increasing ransomware threats, credit unions must implement robust backup strategies to safeguard credit union and member data. Your board should ensure management regularly backs up all critical data and that these backups are securely stored. Implementation of access controls will also prevent unauthorized access to backup data. In addition, the credit union needs clear, documented procedures for restoring data from backups in the event of a ransomware attack or data loss incident. This process should include identifying which data is critical for operations and prioritizing its restoration. Backup systems should be tested regularly to ensure that data can be restored quickly and effectively. Conducting routine drills will help identify any gaps in the backup process and ensure that staff are familiar with restoration procedures.
- ***Membership Education***. Your board should work with management to provide periodic information security education for members to promote sound cybersecurity practices, such as the use of multi-factor authentication and the importance of strong, frequently changed passwords.

Incident Response Planning and Resilience

Your board must, moreover, ensure that resilience plans allow the credit union to operate effectively

during and after a cyber-attack. This planning may involve identifying alternative processes or systems that can be utilized during an outage. Consistent with statutory requirements, the NCUA's regulations require that a federally insured credit union that experiences a reportable cyber incident must report the incident to the NCUA as soon as possible and no later than 72 hours after the credit union reasonably believes that it has experienced such an incident. This statutory requirement underscores the importance of having a well-defined incident response plan that enables prompt reporting and effective communication with regulatory bodies.[2]

Effective resilience planning includes the following:

- ***Internal and External Communication***. Establish a communication strategy for informing your board immediately following a security incident, ensuring transparency and timely decision-making. The communication strategy should also inform both internal stakeholders and external parties, including your members and regulators, in the event of a cyber incident. Clear communication can help manage expectations and maintain trust.
- ***Insurance Considerations***. Evaluate cybersecurity insurance policies to ensure adequate coverage for potential incidents. This assessment includes understanding the scope of coverage and any exclusions that may apply.
- ***Incident Response Team***. Identify and designate an incident response team that includes key personnel from various departments. This team should be prepared to take immediate action in the event of a cyber incident.
- ***Tabletop Exercises***. Conduct regular tabletop exercises to simulate cyber incident scenarios. These exercises will help your credit union board and management practice response plans, identify areas for improvement, and ensure that all team members understand their roles during an incident.

Conclusion

By focusing on the key areas outlined above, your credit union's board of directors can significantly improve the credit union's cybersecurity posture and protect the interests of its members. Cybersecurity is not just an "IT" issue. It must be a critical component of any credit union's overall governance and risk-management strategy. A cyber incident can have far-reaching consequences, not only affecting your institution's financial stability but also potentially impacting the entire financial services system while eroding member trust and damaging your credit union's reputation.

By taking the proactive steps outlined above and prioritizing cybersecurity as a fundamental aspect of governance, your credit union's board of directors can effectively safeguard the credit union and its members' assets, maintain member trust, and ensure compliance with regulatory requirements. To that end, we encourage you to consult the many available cybersecurity resources available on the NCUA's public website not just during cybersecurity month in October but also year round.

Sincerely,

/s/

Todd M. Harper

Chairman

From <https://ncua.gov/regulation-supervision/letters-credit-unions-other-guidance/board-director-engagement-cybersecurity-oversight>

ISO Independence

Tuesday, February 25, 2025 1:15 PM

NCUA Examiner's Recommendation: Ensuring the Independence of the Information Security Officer (ISO) for Effective Cybersecurity Governance

To: Credit Union Management and Board of Directors
From: [NCUA Examiner Name]
Subject: The Necessity of an Independent Information Security Officer (ISO)

As part of my examination of your credit union's **cybersecurity governance framework**, I want to emphasize the critical need for the **Information Security Officer (ISO) to operate independently from IT operations**. The increasing **frequency, sophistication, and impact of cyber threats** require a governance structure that **ensures cybersecurity risks are identified, assessed, and reported without conflicts of interest**.

The **NCUA's Letter to Credit Unions (24-CU-02, October 2024), federal regulations, and the Business Judgment Rule** all support this requirement. Failing to establish an independent ISO structure could create **compliance risks, regulatory scrutiny, and governance weaknesses** that may expose the credit union to **operational and financial harm**.

1. NCUA's Letter to Credit Unions (24-CU-02, October 2024): Cybersecurity is a Governance Issue, Not Just an IT Function

The **NCUA's Letter to Credit Unions (24-CU-02, October 2024) on Board of Director Engagement in Cybersecurity Oversight** underscores the **Board's responsibility for cybersecurity governance**, explicitly stating that **cybersecurity must be a top oversight priority** and that **senior leadership must remain focused on managing cyber risks effectively**.

◇ **NCUA Key Points Supporting ISO Independence:**

- **Cybersecurity is not just an IT issue—it is a core governance responsibility.**
- **The Board must approve and oversee the credit union's cybersecurity program, including risk assessments and security controls.**
- **The Board should establish a framework for periodic reporting on cybersecurity risks, audits, and incidents.**

🚨 **Key Concern:** If the **ISO reports to the CIO**, security risks may be **underreported or filtered** due to operational priorities, **reducing transparency and hindering the Board's ability to oversee cybersecurity effectively**.

💡 **NCUA's Expectation:** The **ISO must report directly to the Board or a designated risk committee** to provide **unbiased and transparent cybersecurity risk assessments**.

2. Regulatory Requirements: NCUA, FFIEC, and GLBA Mandate Board-Level Cybersecurity Oversight

Federal regulations **reinforce the NCUA's position** by requiring credit unions to implement **a cybersecurity governance structure that ensures independent**

oversight of security risks.

A. 12 CFR Part 748 (NCUA Regulations)

- **Appendix A to Part 748** mandates that the Board **approve and oversee an information security program**, ensuring it includes **risk assessments, security controls, and incident response plans**.
- The Board must receive **unfiltered cybersecurity reports**, which is **not possible if the ISO reports to the CIO**—a role that is responsible for IT performance rather than security risk assessment.
- The **NCUA's Cyber Incident Notification Rule** requires credit unions to report **cyber incidents within 72 hours**, highlighting the need for an **independent ISO with authority to escalate security issues immediately**.

B. FFIEC IT Examination Handbook – Information Security

- Clearly states that the **ISO should be independent of IT operations** to ensure **objective risk assessments and unbiased reporting**.
- Recommends **separating cybersecurity responsibilities from IT management to avoid conflicts of interest**.

C. Gramm-Leach-Bliley Act (GLBA) – Safeguards Rule

- Requires **financial institutions to implement an independent cybersecurity governance structure** with **Board-level accountability for cybersecurity risks**.
- Mandates **continuous monitoring and timely risk reporting**, which is best achieved through **an independent ISO**.

💡 **NCUA's Expectation: To comply with these regulations, the ISO must report directly to the Board or an independent committee—not the CIO.**

3. Avoiding Conflicts of Interest: Security Oversight vs. IT Operations

The **CIO is responsible for IT infrastructure performance, cost efficiency, and service availability**. However, **cybersecurity often requires implementing strict controls that may slow operations or increase costs**. If the **ISO reports to the CIO**, this creates an **inherent conflict of interest** that could **undermine cybersecurity risk management**.

🚨 **Key Risks of ISO Reporting to CIO:**

- **Security risks may be deprioritized** due to IT operational concerns.
- **Delayed or underreported security incidents** due to potential reputational concerns within IT management.
- **Budget decisions favoring IT efficiency over critical security investments.**

💡 **NCUA's Expectation:** The **ISO must be independent to ensure cybersecurity risks are objectively assessed and escalated** to the Board **without interference from IT operational priorities**.

4. Business Judgment Rule: Protecting the Board from Legal and Regulatory Risks

The **Business Judgment Rule (BJR)** protects the Board from liability **only if it exercises due care, acts in good faith, and makes informed decisions in the best interest of the credit union**. The Board is **legally obligated to ensure effective cybersecurity oversight**, which includes:

☑ **Maintaining an independent security function to provide unfiltered**

assessments of cyber risks.

☑ **Receiving direct reports from the ISO without CIO influence.**

☑ **Demonstrating due diligence in cybersecurity decision-making to prevent claims of negligence.**

🚨 **Legal & Reputational Risks if ISO Reports to CIO:**

- **Regulatory findings and enforcement actions** for failure to ensure independent cybersecurity oversight.
- **Board accountability for security failures due to lack of independent reporting.**
- **Potential member lawsuits and reputational damage** following a cybersecurity breach that could have been prevented with better governance.

💡 **NCUA's Expectation:** The Board **must demonstrate due diligence by ensuring the ISO operates independently and reports directly to them or an appropriate risk committee**.

NCUA Examiner's Recommendation: Establishing an Independent ISO Structure

📌 **To align with NCUA guidance, regulatory requirements, and governance expectations, the credit union should take the following steps:**

☑ **Reorganize the ISO's reporting structure to be independent of IT operations.**

☑ **Establish direct reporting to the Board or an independent risk committee.**

☑ **Ensure the ISO has the authority to assess and escalate security concerns without CIO influence.**

☑ **Implement a structured process for independent security reporting and risk assessments.**

🚀 **Benefits of ISO Independence:**

✓ **Compliance with NCUA regulations and expectations outlined in Letter 24-CU-02 (October 2024).**

✓ **Objective cybersecurity risk assessments and reporting.**

✓ **Enhanced Board protection under the Business Judgment Rule.**

✓ **Stronger defenses against cyber threats, protecting member assets and trust.**

◇ **Cybersecurity is not just an IT function—it is a critical governance responsibility. The independence of the ISO is essential for meeting regulatory requirements, ensuring effective oversight, and reducing liability for the Board.**

I urge credit union management to take immediate action to implement this structure and ensure compliance with cybersecurity governance expectations.

NCUA Examiner Name
[NCUA Regional Office]

Finding: Inadequate Board Oversight and Lack of Information Security Officer (ISO) Independence

Tuesday, February 25, 2025 1:15 PM

Situation:
During the examination, it was observed that the **Information Security Officer (ISO) reports directly to the Chief Information Officer (CIO)** rather than the Board of Directors or an independent risk committee. This reporting structure creates an inherent **conflict of interest** where cybersecurity risks may be **underreported, deprioritized, or influenced by operational IT concerns** rather than being objectively assessed and escalated to the Board for proper oversight.
Additionally, the Board has not established **a clear framework for periodic cybersecurity reporting** as required by **NCUA Letter 24-CU-02 (October 2024), 12 CFR Part 748, and the FFIEC IT Examination Handbook**, limiting its ability to exercise informed cybersecurity governance.

Behavior:
The Board has **delegated cybersecurity oversight responsibilities primarily to IT operations**, allowing the CIO to control security risk assessments and incident reporting. As a result, the **ISO does not have the independence necessary** to:

- Conduct objective risk assessments.
- Report security concerns **directly to the Board**.
- Escalate incidents without operational interference.

Furthermore, there is **no evidence** that the Board has taken steps to establish **independent cybersecurity reporting channels**, despite NCUA guidance emphasizing that **cybersecurity is a governance issue, not just an IT function** (NCUA Letter 24-CU-02, October 2024).

Impact:

🚨 **Regulatory Non-Compliance:**

- **12 CFR Part 748** requires the Board to **oversee and approve the information security program** and ensure **objective cybersecurity reporting**. A lack of ISO independence **jeopardizes compliance** with these requirements.
- The **FFIEC IT Examination Handbook** explicitly states that the **ISO must be independent of IT operations** to prevent conflicts of interest. The current reporting structure fails to meet this standard.

⚠ **Weak Board Oversight and Increased Cybersecurity Risk:**

- Without **direct and independent security reporting**, the Board **lacks visibility into key cybersecurity risks**.
- **Security incidents may be underreported or delayed**, increasing the risk of regulatory fines, data breaches, and operational disruptions.

⚖ **Legal and Fiduciary Risk to the Board:**

- Under the **Business Judgment Rule**, the Board is required to make **informed, good-faith decisions** to protect the credit union from cybersecurity threats.

- Failure to ensure **effective cybersecurity oversight** and **independent security reporting** could expose the Board to **legal liability in the event of a security breach or regulatory enforcement action**.

Resolution:
To **comply with regulatory requirements** and strengthen **cybersecurity governance**, the credit union must:
☑ **Reorganize the ISO's reporting structure** so that the **ISO reports directly to the Board or an independent risk committee**, rather than the CIO.
☑ **Establish a structured process for periodic cybersecurity reporting** that includes:

- Regular **security briefings** to the Board.
- Transparent reporting on **risk assessments, threat intelligence, and incident response activities**.
- Clear escalation procedures for critical security issues.
  ☑ **Ensure the Board receives independent security assessments** from external auditors or third-party experts to validate cybersecurity effectiveness.
  ☑ **Demonstrate compliance with NCUA Letter 24-CU-02 (October 2024), 12 CFR Part 748, and FFIEC guidance** by implementing governance practices that enhance cybersecurity oversight.

🚀 **By taking these steps, the credit union will:**
✓ **Align with NCUA cybersecurity expectations and regulatory requirements.**
✓ **Reduce legal and compliance risks for the Board.**
✓ **Strengthen its defenses against cyber threats, protecting member assets and trust.**
Failure to take corrective action may result in **further supervisory actions or heightened regulatory scrutiny**.

Notes

Tuesday, September 3, 2024 6:47 AM