The incident response program includes the following:

Friday, August 16, 2024 12:18 PM

Incident Response Validation Process

1. Preparation and Initial Data Gathering

Document Review

- Collect and review incident response policies, procedures, and plans to ensure alignment with:
  - **12 CFR 748.0(b)(1):** Written security program to protect against unauthorized access or use of member information.
  - **Appendix A to Part 748, III(A):** Risk assessment and appropriate safeguards for incidents.
  - **Appendix B to Part 749:** Record retention and preservation guidelines for business continuity incidents.

Interviews

- Conduct interviews with the Incident Response Team (IRT) and relevant personnel to validate their understanding of the response plan as required under **12 CFR 748.1(b)** (detection and response capabilities).

2. Validation of CORE Statements

Stmt 8.1: Assessment of the Nature and Scope of an Incident

- **CORE**
  - Ensure compliance with:
    - **Appendix A to Part 748, III(C)(2)(a):** Identification of systems and data involved.
    - **12 CFR 748.1(c):** Accurate incident classification per security procedures.

Stmt 8.2: Measures to Contain and Control an Incident

- **CORE**
  - Confirm alignment with:
    - **Appendix A to Part 748, III(C)(2)(b):** Incident containment and control.
    - **12 CFR 748.0(b):** Response limits unauthorized access.

Stmt 8.3: Plans for Identifying Member Information Access or Misuse

- **CORE**
  - Validate:
    - Detection tools as per **Appendix A to Part 748, III(C)(2)(a)**.
    - Protection of sensitive information during incidents under **Appendix B to Part 748**.

Stmt 8.4: Filing a Timely Suspicious Activity Report (SAR)

- **CORE**
  - Review the SAR filing process to ensure:
    - Compliance with **12 CFR 748.1(d)**.
    - Proper documentation as per **FIN-2016-A005** guidelines for financial crimes or fraud.

Stmt 8.5: Notification to Regulatory Authorities

- **CORE**
  - Confirm:
    - Timely notification under **12 CFR 748.1(e)** and **Appendix A to Part 748, III(C)(2)(b)**.

Stmt 8.6: Notification to Law Enforcement

- **CORE**
  - Validate compliance with:
    - **12 CFR 748.1(e):** Timely notification for incidents involving criminal activity.

Stmt 8.7: Member Notification Procedures

- **CORE**
  - Confirm alignment with **Appendix B to Part 748, II.ii.1.e** for timely member breach notification.

Stmt 8.8: Incident Response Plans Updated for Regulatory Reporting

- **CORE**
  - Ensure the incident response plan incorporates:
    - **12 CFR 748.1(c):** Reporting requirement timeframes and procedures for notifying the NCUA.
    - Clear guidelines for identifying reportable incidents and escalation procedures for management and NCUA notifications.

Stmt 8.9: Periodic Testing of the Incident Response Plan

- **CORE**
  - Validate:
    - Testing includes roles, responsibilities, procedures, countermeasures, and reporting mechanisms.

3. Validation of CORE+ Statements

Stmt 8.10: A Response Team with Assigned Roles and Responsibilities

- **CORE+**
  - Review IRT composition for compliance with **Appendix A to Part 748, III(A)(1)**.

Stmt 8.11: Incident Response Plans and Capabilities

- **CORE+**
  - Assess whether plans address all incident phases per **Appendix A to Part 748, III(A)** and **Appendix B to Part 749**.

Stmt 8.12: Mechanisms for Communicating During Incident Response

- **CORE+**
  - Ensure secure communication channels align with **Appendix A to Part 748, III(C)(2)(b)** and **12 CFR 748.1(b)**.

Stmt 8.13: Procedures for Vendor Incidents

- **CORE+**
  - Verify third-party compliance with **Appendix A to Part 748, III(C)(2)(d)**.

Stmt 8.14: Incident Thresholds

- **CORE+**
  - Ensure thresholds for escalation align with **Appendix A to Part 748, III(C)(2)(c)**.

Stmt 8.15: Data Recovery Practices

- **CORE+**
  - Validate recovery processes against:
    - **Appendix A to Part 748, III(C)(2)(b)**.
    - **Appendix B to Part 749:** Record retention and recovery guidelines.

Stmt 8.16: Conducting Routine Incident Response Exercises

- **CORE+**
  - Confirm simulation exercises and documentation as per **Appendix A to Part 748, III(C)(2)(c)**.

Stmt 8.17: Conducting Post-Incident Reviews

- **CORE+**
  - Ensure post-incident reviews comply with **Appendix A to Part 748, III(C)(2)(d)**.

Stmt 8.18: Tracking Action Items

- **CORE+**

- Validate action tracking and resolution following **Appendix B to Part 749** and lessons learned from real incidents or exercises.

4. Reporting and Documentation

Summary Report

- Compile findings and recommendations per **Appendix A to Part 748, III(C)(3)**.

Follow-Up Plan

- Address deficiencies referencing **12 CFR 748.1** for ongoing compliance monitoring.

5. Continuous Improvement

Ongoing Monitoring

- Establish procedures for regular updates and monitoring per **Appendix A to Part 748, III(B)**.

Feedback Loop

- Incorporate lessons learned into response strategies to ensure compliance with **Appendix B to Part 749**.

Issues

Thursday, September 19, 2024 9:36 AM

1. Incomplete Documentation or Policies
- **Gap**: Incident response documentation may not be fully aligned with **12 CFR 748.0** or **Appendix A to Part 748** in terms of covering every phase of the incident response process.
  - **Mitigation**: Review the written incident response plans and ensure they explicitly address all phases (e.g., detection, containment, eradication, and recovery) and are regularly updated.

2. Inadequate Member Notification Procedures
- **Gap**: The breach notification process might not adhere to the timing and communication requirements outlined in **Appendix A to Part 748, III(C)(2)(b)**.
  - **Mitigation**: Confirm that the member notification procedures are detailed, including who is responsible for notifications, timelines, and the method of communication with affected members.

3. Insufficient Third-Party Incident Response Review
- **Gap**: Third-party vendor incident response procedures might not be adequately reviewed or incorporated, leaving the credit union vulnerable to supply chain risks, as outlined in **Appendix A to Part 748, III(C)(2)(d)**.
  - **Mitigation**: Establish a regular review process for vendor incident response capabilities, ensuring that contracts and agreements include incident response expectations and notification timelines.

4. Lack of SAR Filing for Security Incidents
- **Gap**: Suspicious Activity Reports (SARs) may not be filed for incidents involving potential fraud or financial crime as required by **12 CFR 748.1(d)**.
  - **Mitigation**: Implement a clear protocol for assessing when a SAR is required in the context of security incidents and ensure timely filing.

5. Incomplete Incident Response Testing
- **Gap**: Incident response simulations and exercises may not be conducted regularly, as required by **Appendix A to Part 748, III(C)(2)(c)**.
  - **Mitigation**: Schedule regular tabletop exercises or full simulations to test the incident response plan, ensuring they cover different types of incidents (cyberattacks, fraud, etc.) and that lessons learned are applied.

6. Insufficient Tracking of Post-Incident Action Items
- **Gap**: The credit union may not have a robust process for tracking and resolving action items identified during post-incident reviews or simulations, per **Appendix A to Part 748, III(C)(2)(d)**.
  - **Mitigation**: Implement an action-tracking system to ensure that all items identified during incident reviews are resolved and that the response plan is updated based on these insights.

7. Incomplete Regulatory and Law Enforcement Notifications
- **Gap**: Notifications to regulatory bodies (e.g., NCUA Regional Director) and law enforcement may be delayed or incomplete, failing to meet **12 CFR 748.1(e)** and **Appendix A to Part 748, III(C)(2)(b)** standards.
  - **Mitigation**: Define clear thresholds for when and how to notify regulators and law enforcement. Ensure the notification process includes detailed documentation of incidents, response actions, and timelines.

8. Incident Response Team Roles and Responsibilities Not Clearly Defined
- **Gap**: Roles within the incident response team may not be clearly defined or aligned with the guidelines outlined in **Appendix A to Part 748, III(A)(1)**, leading to confusion during a response.
  - **Mitigation**: Review and document specific roles and responsibilities within the incident response team, including backups for key positions to ensure continuity during incidents.

9. Lack of Comprehensive Data Recovery and Business Continuity Practices
- **Gap**: Data recovery procedures may not be aligned with **Appendix B to Part 749** or **Appendix A to Part 748, III(C)(2)(b)**, potentially leading to data loss or incomplete recovery during incidents.
  - **Mitigation**: Review and enhance data recovery plans to ensure that member information is securely restored, and incorporate business continuity planning into the incident response process.

10. Insufficient Risk Assessment of Incident Response Plan
- **Gap**: The risk assessment process may not include a thorough evaluation of potential incident scenarios as described in **Appendix A to Part 748, III(A)(1)**.
  - **Mitigation**: Incorporate a risk-based approach in the incident response plan that evaluates different types of risks (e.g., ransomware, insider threats, third-party breaches) and outlines specific response strategies.

11. Missing or Incomplete Post-Incident Reviews
- **Gap**: Post-incident reviews may be missing or lack sufficient detail, leading to repeated mistakes and unaddressed vulnerabilities, contrary to **Appendix A to Part 748, III(C)(2)(d)**.
  - **Mitigation**: Conduct comprehensive post-incident reviews for all security incidents and exercises. Document lessons learned and adjust the incident response plan accordingly.

12. Incomplete Reporting to the Board of Directors
- **Gap**: The Annual Report to the Board on the Information Security Program may not include detailed updates on the incident response program, as required under **Appendix A to Part 748, III(C)(3)**.
  - **Mitigation**: Ensure that incident response activities and lessons learned are part of the annual board report and that the board is aware of any significant security incidents and response improvements.

General Recommendations to Address Gaps
1. **Regular Plan Updates**: Ensure all incident response plans, policies, and procedures are reviewed and updated at least annually or after any major incident.
2. **Ongoing Training**: Provide regular training to the incident response team and other stakeholders to ensure they are familiar with their roles and the procedures they need to follow.
3. **Automation Tools**: Implement automated tracking and monitoring systems to detect incidents more quickly and track the resolution of post-incident actions.
4. **Vendor Audits**: Conduct regular audits of third-party vendors to verify that their incident response capabilities are aligned with the credit union's policies and standards.

Remediation

Thursday, September 19, 2024 9:38 AM

1. Incomplete Documentation or Policies
- **Action**: Conduct a **policy review** to ensure that all phases of the incident response process (detection, containment, recovery, etc.) are documented.
- **Next Step**: Assign a compliance or risk management team to review and align the policies with **12 CFR 748.0** and **Appendix A to Part 748**.
- **Timeline**:
- **Deliverable**: Updated Incident Response Policy with a focus on completeness.

2. Inadequate Member Notification Procedures
- **Action**: Review and enhance the **member notification procedures** for data breaches.
- **Next Step**: Ensure templates, communication channels, and personnel responsible for member notifications are identified and documented.
- **Timeline**:
- **Deliverable**: Documented and tested member notification plan, compliant with **Appendix A to Part 748, III(C)(2)(b)**.

3. Insufficient Third-Party Incident Response Review
- **Action**: Review **vendor contracts** and ensure that they include clear incident response obligations.
- **Next Step**: Conduct an assessment of third-party incident response capabilities and create a process for ongoing vendor monitoring.
- **Timeline**:
- **Deliverable**: Updated vendor contracts and an established vendor incident response review process.

4. Lack of SAR Filing for Security Incidents
- **Action**: Ensure that the **SAR filing** process includes clear triggers for filing in case of security incidents.
- **Next Step**: Provide training to the compliance team on identifying incidents that require SAR filings as per **12 CFR 748.1(d)**.
- **Timeline**:
- **Deliverable**: SAR filing procedures and evidence of training sessions.

5. Incomplete Incident Response Testing
- **Action**: Schedule and conduct **incident response exercises** that simulate real-world scenarios.
- **Next Step**: Plan and perform tabletop exercises or full-scale simulations to test the effectiveness of the incident response plan.
- **Timeline**:
- **Deliverable**: Documentation of exercises, including scenarios, participants, results, and lessons learned.

6. Insufficient Tracking of Post-Incident Action Items
- **Action**: Implement a **tracking system** for all action items identified during post-incident reviews and exercises.
- **Next Step**: Assign responsible parties and set deadlines for resolving action items.
- **Timeline**:
- **Deliverable**: Action tracking logs and evidence of completed action items.

7. Incomplete Regulatory and Law Enforcement Notifications
- **Action**: Develop clear thresholds and timelines for **regulatory and law enforcement notifications**.
- **Next Step**: Ensure that compliance teams are familiar with notification requirements per **12 CFR 748.1(e)** and **Appendix A to Part 748, III(C)(2)(b)**.
- **Timeline**:
- **Deliverable**: Regulatory and law enforcement notification procedure, including specific timeframes and responsible parties.

8. Incident Response Team Roles and Responsibilities Not Clearly Defined
- **Action**: Clarify and document the **roles and responsibilities** of the Incident Response Team (IRT).
- **Next Step**: Update the incident response plan to reflect each team member's role and ensure cross-training for key positions.
- **Timeline**:
- **Deliverable**: Revised incident response plan with clearly defined roles.

9. Lack of Comprehensive Data Recovery and Business Continuity Practices
- **Action**: Review and update the **data recovery and business continuity plans** to ensure alignment with **Appendix B to Part 749**.
- **Next Step**: Perform testing of backup and recovery procedures, and evaluate business continuity practices.
- **Timeline**:
- **Deliverable**: Tested data recovery and business continuity procedures with documented results.

10. Insufficient Risk Assessment of Incident Response Plan
- **Action**: Conduct a **risk assessment** that includes potential incident scenarios and their impact on the credit union.
- **Next Step**: Work with IT, compliance, and risk management teams to update the risk assessment process to include specific incident response risks.
- **Timeline**:
- **Deliverable**: Updated risk assessment and corresponding incident response measures.

11. Missing or Incomplete Post-Incident Reviews
- **Action**: Ensure **post-incident reviews** are thorough and well-documented, identifying root causes and corrective actions.
- **Next Step**: Establish a formal review process for all incidents, regardless of size, and ensure lessons learned are incorporated into the incident response plan.
- **Timeline**:
- **Deliverable**: Post-incident review template and a documented history of reviews.

12. Incomplete Reporting to the Board of Directors
- **Action**: Update the **Annual Report** to the board to include detailed summaries of the incident response program and significant incidents.
- **Next Step**: Schedule a presentation or discussion with the board to review the incident response updates and any major findings from the previous year.
- **Timeline**:
- **Deliverable**: Comprehensive annual report, including incident response findings, updates, and action plans.

General Next Steps for All Gaps:
1. **Assign Accountability**: Designate key stakeholders and teams to be responsible for addressing each gap. Ensure they have the authority and resources to carry out corrective actions.
2. **Set Timelines**: Establish **specific deadlines** for each corrective action and schedule periodic reviews to monitor progress.
3. **Documentation and Reporting**: Ensure every step of the process is well-documented and create a **reporting mechanism** that allows senior management and the board to monitor the effectiveness of the program.
4. **Regular Training**: Conduct regular training sessions for the Incident Response Team, third-party vendors, and relevant stakeholders to ensure familiarity with updated policies and procedures.
5. **Monitoring and Continuous Improvement**: Establish a **continuous monitoring system** that regularly evaluates the incident response plan, assesses new risks, and incorporates improvements from lessons learned during incidents and exercises.

Compliance

Thursday, September 19, 2024 1:11 PM

To ensure compliance with **Appendix A to Part 748, Title 12** and **Appendix B to Part 749**, credit unions must develop a robust **Incident Response Program** (IRP) that protects member information and responds effectively to security breaches. The following are the **compliance steps** for developing, maintaining, and monitoring an Incident Response Program that meets the regulatory requirements outlined in t hese Appendices.

1. Develop an Incident Response Program Framework

1.1 Establish a Written Incident Response Plan (IRP)

- **Action:** Create a formal, written Incident Response Plan that outlines the policies and procedures for responding to security incidents, particularly those involving unauthorized access to member information.
- **Reference: Appendix A to Part 748, Section III(A)(2)** – Requires the establishment of a written information security program, which includes an incident response plan.
- **Compliance Steps:**
  1. Define roles and responsibilities for incident response team members.
  2. Develop step-by-step procedures for handling security incidents, including detection, investigation, containment, mitigation, and recovery.
  3. Ensure the plan is aligned with regulatory requirements, business continuity, and disaster recovery efforts.

1.2 Incident Classification and Prioritization

- **Action:** Establish a classification system for incidents based on severity and potential impact, prioritizing incidents that involve member information.
- **Reference: Appendix A to Part 748, Section III(A)(3)** – The security program should define how incidents are classified and escalated based on severity.
- **Compliance Steps:**
  1. Classify incidents as high, medium, or low risk based on the extent of the breach and the sensitivity of the data involved.
  2. Create criteria for escalating incidents to senior management or the board, as required by regulatory standards.

2. Detection and Monitoring of Incidents

2.1 Continuous Monitoring and Detection

- **Action:** Implement monitoring systems to detect unauthorized access to member information and suspicious activity.
- **Reference: Appendix A to Part 748, Section III(A)(4)** – Requires ongoing monitoring of systems to detect unauthorized access or misuse of member information.
- **Compliance Steps:**
  1. Install intrusion detection/prevention systems (IDS/IPS), network monitoring tools, and logging mechanisms to track activity.
  2. Regularly review system logs for unusual patterns or behavior that may indicate a breach.

2.2 Threat Intelligence and Vulnerability Management

- **Action:** Use external threat intelligence and vulnerability assessments to proactively identify risks and enhance the detection of emerging threats.
- **Reference: Appendix A to Part 748, Section III(A)(5)** – Institutions must stay updated on new and evolving threats.
- **Compliance Steps:**
  1. Subscribe to threat intelligence feeds to stay informed of emerging risks.
  2. Conduct regular vulnerability assessments and penetration tests to identify potential weaknesses in systems.

3. Response and Containment of Security Incidents

3.1 Immediate Incident Containment

- **Action:** Define clear procedures for containing incidents quickly to prevent further damage or unauthorized access.
- **Reference: Appendix A to Part 748, Section III(A)(2)** – The incident response plan must include containment strategies to limit the scope of a breach.
- **Compliance Steps:**
  1. Document containment actions, such as disconnecting affected systems from the network or disabling compromised accounts.
  2. Assign responsibilities for containment to specific team members to ensure swift action.

3.2 Notification and Escalation Procedures

- **Action:** Establish notification protocols for alerting internal and external parties, including affected members, senior management, law enforcement, and regulators.
- **Reference: Appendix A to Part 748, Section III(A)(3)** – Requires timely notification of key stakeholders and affected parties in the event of a breach.
- **Compliance Steps:**
  1. Develop a process for notifying members whose data has been compromised, following regulatory guidelines for breach notificat ion.
  2. Include escalation procedures for reporting incidents to the Board, regulators (e.g., NCUA), and other relevant authorities.

4. Recovery and Remediation

4.1 Incident Remediation

- **Action:** Define remediation actions to correct the underlying causes of security incidents and prevent future occurrences.
- **Reference: Appendix A to Part 748, Section III(A)(4)** – Incident response must include measures to mitigate damage and prevent recurrence.
- **Compliance Steps:**
  1. Identify and correct vulnerabilities that led to the breach (e.g., software patches, access control improvements).
  2. Update security policies and procedures based on lessons learned from the incident.

4.2 System Recovery and Business Continuity

- **Action:** Ensure the IRP includes procedures for restoring normal operations, including recovery of systems and data after an incident.
- **Reference: Appendix A to Part 748, Section III(A)(5)** – Requires business continuity and disaster recovery measures to restore services after an incident.
- **Compliance Steps:**
  1. Develop system recovery protocols to ensure timely restoration of affected systems.
  2. Conduct regular testing of recovery procedures to ensure they are effective.

5. Post-Incident Review and Documentation

5.1 Post-Incident Analysis

- **Action:** Conduct a post-incident review after each security breach to evaluate the effectiveness of the response and identify areas for improvement.
- **Reference: Appendix A to Part 748, Section III(B)(3)** – Requires the review of incidents to improve the institution's security posture.
- **Compliance Steps:**
  1. Document the timeline of the incident, actions taken, and lessons learned.
  2. Use this analysis to update the IRP and improve response capabilities for future incidents.

5.2 Reporting and Record-Keeping

- **Action:** Maintain detailed records of all security incidents and responses, including communications with affected parties and regulators.
- **Reference: Appendix A to Part 748, Section III(C)(1)** and **Appendix B to Part 749** – Requires institutions to maintain accurate records of incidents and communications with external stakeholders.
- **Compliance Steps:**
  1. Document all aspects of the incident, including detection, containment, remediation, and notification actions.
  2. Store incident reports securely and make them available for regulatory audits.

6. Compliance with Regulatory and Legal Requirements

6.1 Breach Notification Requirements

- **Action:** Comply with legal and regulatory requirements for notifying members, regulators, and other authorities when a breach occurs.
- **Reference: Appendix A to Part 748, Section III(C)(1)(d)** – Requires timely notification of member information breaches.
- **Compliance Steps:**
  1. Ensure the IRP includes procedures for notifying affected members as soon as feasible, following applicable state and federal data breach notification laws.
  2. Maintain records of all communications with members, regulators, and law enforcement.

6.2 Reporting to Regulators

- **Action:** Follow guidelines for reporting significant security incidents to the appropriate regulatory agencies, such as the NCUA.
- **Reference: Appendix B to Part 749** – Outlines requirements for reporting incidents that could affect the institution's operations or financial condition.
- **Compliance Steps:**
  1. Notify the NCUA or other regulators if a breach could have a significant impact on the institution's operations.
  2. Provide detailed incident reports and updates as requested by regulators.

7. Training and Awareness

7.1 Employee Training on Incident Response

- **Action:** Train all employees on the institution's incident response procedures, including how to detect and report security incidents.
- **Reference: Appendix A to Part 748, Section III(C)(1)(c)** – Employees must be trained to recognize and respond to security incidents.
- **Compliance Steps:**
  1. Develop mandatory training programs for employees on incident reporting protocols and their role in the IRP.
  2. Conduct regular tabletop exercises to simulate incidents and test the effectiveness of the IRP.

7.2 Incident Response Team Training

- **Action:** Provide advanced training for members of the incident response team, including specific technical skills and response strategies.
- **Reference: Appendix A to Part 748, Section III(C)(1)(b)** – Requires specialized training for employees responsible for managing incidents.
- **Compliance Steps:**
  1. Ensure incident response team members receive regular training on the latest cybersecurity threats, response tactics, and leg al requirements.
  2. Evaluate the team's readiness through simulated incident response drills.

8. Regular Testing and Updating of the IRP

8.1 Regular Testing of the Incident Response Plan

- **Action:** Conduct regular tests of the Incident Response Plan, including mock incident simulations and tabletop exercises.
- **Reference: Appendix A to Part 748, Section III(B)(3)** – The IRP must be tested regularly to ensure its effectiveness.

- **Compliance Steps:**
    1. Schedule annual or biannual testing of the IRP to evaluate its effectiveness and make adjustments as necessary.
    2. Document the results of these tests and use the findings to update the plan.

8.2 Update the IRP Based on Lessons Learned

- **Action:** Update the Incident Response Plan based on lessons learned from actual incidents and test results.
- **Reference: Appendix A to Part 748, Section III(A)(5)** – Requires continuous improvement of the IRP based on experience and emerging threats.
- **Compliance Steps:**
    1. Review and revise the IRP regularly to incorporate new technologies, regulatory changes, and lessons learned from previous in cidents.
    2. Ensure that all updates are communicated to the incident response team and other relevant personnel.

By following these **compliance steps**, credit unions can ensure that their **Incident Response Program** meets the regulatory requirements outlined in **Appendix A to Part 748, Title 12** and **Appendix B to Part 749**. These steps help protect member information, mitigate the impact of security incidents, and ensure the institution's preparedness to handle data breaches and other securi ty events.

Compliance Tools

Friday, August 16, 2024 1:54 PM

****1. Microsoft 365 Compliance Center**

- **Features**: Data loss prevention, information protection, insider risk management, compliance score, and audit log search.
- **Best For**: Organizations using Microsoft 365, providing seamless integration with other Microsoft tools and services.

****2. Vanta**

- **Features**: Automated compliance monitoring, continuous security monitoring, customizable policies, and controls for SOC 2, ISO 27001, GDPR, and HIPAA.
- **Best For**: Startups and SMBs looking to achieve and maintain various certifications with minimal manual effort.

****3. OneTrust**

- **Features**: Data privacy management, GDPR compliance, vendor risk management, incident management, and data discovery.
- **Best For**: Large enterprises needing robust data privacy and compliance management solutions.

****4. Compliance.ai**

- **Features**: Regulatory change management, policy management, compliance automation, and risk assessment.
- **Best For**: Financial institutions and highly regulated industries needing to stay updated with regulatory changes.

****5. LogicGate Risk Cloud**

- **Features**: GRC (Governance, Risk, and Compliance) management, incident management, policy management, and audit management.
- **Best For**: Organizations of all sizes looking for a flexible and customizable GRC platform.

****6. Hyperproof**

- **Features**: Compliance automation, evidence collection, risk management, control management, and continuous monitoring.
- **Best For**: Companies seeking to streamline compliance workflows and automate evidence collection for audits.

****7. RSA Archer**

- **Features**: Integrated risk management, compliance management, audit management, and incident management.
- **Best For**: Large organizations needing a comprehensive and scalable GRC platform.

****8. AuditBoard**

- **Features**: Audit management, risk management, compliance management, and SOX compliance.
- **Best For**: Companies needing robust audit and compliance management, particularly for SOX compliance.

****9. TrustArc**

- **Features**: Privacy management, data inventory, consent management, risk management, and GDPR compliance.
- **Best For**: Organizations focused on data privacy and GDPR compliance.

****10. Drata**

- **Features**: Automated compliance, continuous monitoring, policy management, and support for SOC 2, ISO 27001, GDPR, and HIPAA.
- **Best For**: Fast-growing companies aiming to achieve and maintain compliance certifications efficiently.

****11. NAVEX Global**

- **Features**: Risk management, compliance management, policy management, incident reporting, and whistleblower hotlines.
- **Best For**: Organizations of all sizes needing a comprehensive suite of compliance and risk management solutions.

****12. ZenGRC by Reciprocity**

- **Features**: GRC management, audit management, risk assessment, and compliance automation.
- **Best For**: Businesses looking for an easy-to-use GRC platform with strong integration capabilities.

****13. Qualys**

- **Features**: Vulnerability management, policy compliance, asset management, and continuous monitoring.
- **Best For**: Organizations focused on IT security and compliance, particularly those needing robust vulnerability management.

****14. Tugboat Logic**

- **Features**: Compliance automation, policy management, audit readiness, and continuous monitoring.
- **Best For**: Small to mid-sized businesses seeking to simplify and automate compliance processes.

****15. ComplySci**

- **Features**: Regulatory compliance, conflict management, personal trading compliance, and risk assessments.
- **Best For**: Financial services firms needing to manage regulatory compliance and employee conflicts of interest.

Criteria for Selection

When choosing the right compliance tool, consider the following criteria:

- **Regulatory Coverage**: Ensure the tool supports the specific regulations and standards your organization needs to comply with.
- **Ease of Use**: The tool should be user-friendly and require minimal training for your team.
- **Integration Capabilities**: Look for tools that integrate seamlessly with your existing systems and workflows.
- **Automation Features**: Automation can significantly reduce the manual effort required for compliance management and reporting.
- **Scalability**: Choose a tool that can grow with your organization and handle increased compliance demands.
- **Vendor Support**: Ensure the vendor provides robust support and regular updates to the tool.

Resources

Friday, August 16, 2024 12:19 PM

Incident Response (IR) Plans	Organizations maintain, practice, and update cybersecurity incident response plans for relevant threat scenarios.	Inability to quickly and effectively contain, mitigate, and communicate about cybersecurity incidents.	Organization-wide	Organizations have, maintain, update, and regularly drill IT and OT cybersecurity incident response plans for both common and organizationally-specific (e.g., by sector, locality) threat scenarios and TTPs. When conducted, tests or drills are as realistic as feasible. IR plans are drilled at least annually, and are updated within a risk-informed time frame following the lessons learned portion of any exercise or drill.
Detecting Relevant Threats and TTPs	Organizations are aware of and able to detect relevant threats and TTPs.	Without the knowledge of relevant threats and ability to detect them, organizations risk that threat actors may exist undetected in their networks for long periods.	N/A	Organizations document a list of threats and cyber actor TTPs relevant to their organization (e.g., based on industry, sectors), and maintain the ability (such as via rules, alerting, or commercial prevention and detection systems) to detect instances of those key threats.
Incident Reporting	LETTER NO: 23-CU-07. Federally Insured Credit Unions. Cyber Incident Notification Requirements.	Beginning on September 1, 2023, all federally insured credit unions must notify the NCUA as soon as possible, and no later than 72 hours, after the credit union reasonably believes it has experienced a reportable cyber incident or received a notification from a third party regarding a reportable cyber incident.	Organization-wide	The rule requires a federally insured credit union that experiences a reportable cyber incident to report the incident to the NCUA as soon as possible and no later than 72 hours after the credit union reasonably believes that it experienced a reportable cyber incident. The 72 hours begins when the credit union forms a reasonable belief a reportable cyber incident has taken place. When a federally insured credit union receives a notification from a third party that sensitive data has been compromised or business operations have been disrupted due to a cyber incident, the credit union has 72 hours to report to the NCUA. This timeframe starts from the moment the credit union receives the notification from the third party or when the credit union forms a reasonable belief that such an incident has occurred, whichever is sooner.
Incident Planning and Preparedness	Organizations are capable of safely and effectively recovering from a cybersecurity incident.	Disruption to availability of an asset, service, or system.	IT and OT assets	Develop, maintain, and execute plans to recover and restore to service business- or mission-critical assets or systems that might be impacted by a cybersecurity incident

Strong	Satisfactory	Less Than Satisfactory	Deficient	Critically Deficient
☐ A written incident response plan that defines roles of personnel and incident management; ☐ Specific personnel designated to support the incident handling process; ☐ Notification of law enforcement, regulators, and members; ☐ Identification of third parties who provide mitigation strategies; ☐ Periodic testing; ☐ Information is published to all employees, the incident handling team, and include employee awareness activities.	☐ A written incident response plan that defines roles of personnel and incident management; ☐ Specific personnel designated to support the incident handling process; ☐ Notification of law enforcement, regulators, and members; ☐ Identification of third parties who provide mitigation strategies; ☐ Periodic testing; ☐ Information is not consistently published to all employees, the incident handling team, and include employee awareness activities.	☐ A written incident response plan that defines roles of personnel and incident management; ☐ No specific personnel designated to support the incident handling process; ☐ No notification of law enforcement, regulators, and members; ☐ No identification of third parties who provide mitigation strategies; ☐ No periodic testing; ☐ Information is not published to all employees, the incident handling team, and include employee awareness activities.	☐ An informal incident response plan; ☐ No specific personnel designated to support the incident handling process; ☐ No notification of law enforcement, regulators, and members; ☐ No identification of third parties who provide mitigation strategies; ☐ No Periodic testing; ☐ Information is not published to all employees, the incident handling team, and include employee awareness activities.	☐ No incident response plan.

A response team with assigned roles and responsibilities

1. Team Structure and Composition
Defined Team Roles: Clearly identify the roles within the response team, such as Incident Response Manager, Communication Lead, Technical Lead, Legal Advisor, and Public Relations Officer.
Role Assignment: Assign specific individuals to each role, ensuring that their responsibilities are well-understood and documented.
Diversity of Skills: Ensure the team includes members with diverse skill sets, including technical expertise, communication skills, legal knowledge, and strategic decision-making abilities.
2. Roles and Responsibilities
Incident Response Manager: Oversees the entire incident response process, coordinates team activities, and ensures that the response follows the incident response plan.
Technical Lead: Manages the technical investigation, including identifying the root cause, containing the breach, eradicating threats, and restoring affected systems.
Communication Lead: Handles internal and external communications, ensuring that accurate and timely information is shared with stakeholders, including employees, customers, and regulatory bodies.
Legal Advisor: Provides legal guidance on regulatory requirements, compliance issues, and potential legal implications of the incident.
Public Relations Officer: Manages the organization's public image, prepares press releases, and handles media inquiries to maintain public trust and confidence.
3. Training and Preparedness
Regular Training: Conduct regular training sessions for all team members to keep their skills and knowledge up-to-date with the latest threat landscapes and response techniques.
Simulated Drills: Perform regular incident response drills to test the team's readiness and effectiveness in handling real-life scenarios.
Documentation and Resources: Ensure all team members have access to detailed documentation, incident response plans, and necessary tools and resources to perform their duties effectively.
4. Incident Response Process
Preparation: Establish and maintain an incident response plan, including predefined procedures for different types of incidents.
Detection and Analysis: Set up mechanisms for detecting security incidents and performing a thorough analysis to understand the scope and impact.
Containment, Eradication, and Recovery: Develop strategies for containing the incident, eradicating the threat, and recovering affected systems to normal operation.
Post-Incident Activities: Conduct a post-incident review to identify lessons learned, update response plans, and improve overall security posture.
5. Communication and Coordination
Communication Plan: Develop a communication plan outlining how information will be shared among team members, with management, and with external parties.
Coordination with External Entities: Establish relationships and protocols for coordinating with external entities, such as law enforcement, regulatory bodies, and third-party vendors.
Reporting and Documentation: Maintain detailed records of the incident, actions taken, and communications made during the response process.
6. Metrics and Evaluation
Performance Metrics: Define metrics to evaluate the performance of the incident response team, such as response time, containment time, and recovery time.
Continuous Improvement: Regularly review and update the incident response plan and team structure based on feedback, post-incident reviews, and changing threat landscapes.

Incident response plans and capabilities

1. Preparation
Policy and Framework: Establish a comprehensive incident response policy that aligns with organizational goals, compliance requirements, and industry standards.
Incident Response Team: Form a dedicated incident response team with clearly defined roles and responsibilities, as detailed in the previous criterion.
Training and Awareness: Conduct regular training sessions and awareness programs to ensure all employees understand their role in incident response.
Resources and Tools: Equip the incident response team with necessary tools, technologies, and resources to detect, analyze, and respond to incidents.
2. Identification and Detection
Monitoring and Detection Systems: Implement advanced monitoring and detection systems, including intrusion detection systems (IDS), security information and event management (SIEM) systems, and

endpoint detection and response (EDR) tools.
Threat Intelligence: Utilize threat intelligence feeds to stay informed about emerging threats and vulnerabilities.
Baseline and Anomaly Detection: Establish a baseline of normal network behavior to identify anomalies that could indicate a security incident.
3. Incident Classification and Prioritization
Incident Classification: Develop a classification schema for incidents based on severity, impact, and type (e.g., malware, phishing, insider threats).
Prioritization Criteria: Establish criteria for prioritizing incidents to ensure the most critical issues are addressed first.
4. Containment, Eradication, and Recovery
Containment Strategies: Develop strategies for immediate containment of incidents to prevent further damage, including short-term and long-term containment procedures.
Eradication Procedures: Outline steps for removing the root cause of the incident, such as malware removal, system patching, and vulnerability mitigation.
Recovery Plans: Define recovery procedures to restore affected systems and services to normal operations, including data restoration and system verification.
5. Communication
Internal Communication: Establish clear communication channels and protocols for informing relevant stakeholders within the organization during an incident.
External Communication: Develop protocols for communicating with external parties, including customers, regulatory bodies, and law enforcement, ensuring compliance with legal and regulatory requirements.
Crisis Communication: Prepare a crisis communication plan to manage public relations and media inquiries effectively during high-profile incidents.
6. Documentation and Reporting
Incident Documentation: Maintain detailed records of all incidents, including the nature of the incident, actions taken, and lessons learned.
Reporting Procedures: Define procedures for reporting incidents to internal and external stakeholders, ensuring timely and accurate communication.
7. Post-Incident Review and Continuous Improvement
Post-Incident Analysis: Conduct thorough post-incident reviews to identify strengths, weaknesses, and areas for improvement in the incident response process.
Lessons Learned: Document lessons learned from each incident and incorporate them into future incident response planning and training.
Continuous Improvement: Regularly update the incident response plan based on feedback, changes in the threat landscape, and advancements in technology.
8. Compliance and Legal Considerations
Regulatory Compliance: Ensure the incident response plan meets all relevant regulatory and compliance requirements, including data protection laws and industry-specific regulations.
Legal Counsel: Involve legal advisors in the incident response process to provide guidance on legal obligations and implications.
9. Metrics and Evaluation
Performance Metrics: Define key performance indicators (KPIs) to measure the effectiveness of the incident response process, such as response time, containment time, and recovery time.
Regular Testing and Drills: Conduct regular tests and simulated drills to evaluate the readiness and effectiveness of the incident response plan.
Third-Party Assessments: Periodically engage third-party experts to assess and validate the incident response plan and capabilities.
10. Integration with Broader Security Program
Alignment with Security Policies: Ensure the incident response plan is aligned with the organization's broader security policies and strategies.
Coordination with Other Teams: Foster collaboration between the incident response team and other departments, such as IT, legal, and human resources, to ensure a coordinated and comprehensive response.


Federal_Government...


federal-government...

Third-Party

Friday, August 16, 2024 1:52 PM

1. Extend Data Collection to Third-Party Incidents
- **Third-Party Integration**: Integrate PowerApps with third-party vendor management systems or portals to collect incident data from external vendors automatically. If your vendors provide APIs, you can connect PowerApps directly to these sources.
- **Custom Forms for Third-Party Incidents**: Create specific forms within PowerApps for logging incidents that originate from third-party vendors. These forms should capture details such as the nature of the breach, impacted systems or data, vendor response, and communication timelines.

2. Automate Third-Party Incident Assessment
- **Risk Scoring**: Develop automated scoring mechanisms within PowerApps to assess the risk level of third-party breaches based on factors such as data sensitivity, the extent of the breach, and vendor response time.
- **Vendor Incident Classification**: Use Power Automate to classify incidents reported by third parties automatically. This can be based on predefined criteria such as the type of data involved, the number of records affected, and the compliance requirements triggered by the breach.

3. Automate Notifications and Escalations for Third-Party Incidents
- **Vendor Notifications**: Configure automated workflows in PowerApps to notify relevant internal stakeholders when a third-party breach is reported. These notifications can include the details of the breach, the vendor's response, and any immediate actions required.
- **Escalation Workflows**: If the third-party breach meets certain risk thresholds, automate the escalation process within PowerApps, alerting senior management, legal, and compliance teams. This ensures prompt attention to high-risk incidents.
- **Automated Communication with Vendors**: Set up workflows that automatically trigger communication with the vendor, requesting additional information or updates on the breach. Predefined email templates or direct API integrations can be used for this purpose.

4. Monitor Vendor Compliance and Response Times
- **Incident Response SLA Tracking**: Use PowerApps to track whether third-party vendors are meeting their Service Level Agreements (SLAs) for incident response. This could involve monitoring the time taken by the vendor to detect, report, and mitigate the breach.
- **Compliance Checks**: Automate compliance checks within PowerApps to ensure that third-party vendors follow the agreed-upon security and incident response protocols. Non-compliance can trigger alerts and corrective actions.

5. Implement Automated Post-Breach Review for Third-Party Incidents
- **Post-Incident Review Forms**: After resolving a third-party breach, use PowerApps to generate a post-incident review form that includes sections specific to third-party involvement. This form should capture lessons learned, the effectiveness of the vendor's response, and any required changes to vendor management practices.
- **Action Item Tracking**: If the post-incident review identifies areas for improvement, use PowerApps to create and assign action items to relevant teams, including follow-ups with the third-party vendor. Power Automate can manage reminders and status tracking for these action items.

6. Integrate Third-Party Incident Response Plans
- **Third-Party Incident Response Playbooks**: Develop and integrate third-party-specific incident response playbooks into PowerApps. These playbooks can be triggered automatically when a third-party breach is reported, guiding the response team through the required steps.
- **Automated Documentation**: Ensure that all third-party incidents are automatically documented within PowerApps, including the incident timeline, actions taken, communication with the vendor, and final outcomes. This documentation is crucial for audits and compliance checks.

7. Continuous Monitoring and Reporting
- **Third-Party Risk Dashboards**: Extend your Power BI dashboards within PowerApps to include third-party breach metrics, such as the number of breaches reported by vendors, the average time to respond, and the compliance status of each vendor.
- **Automated Reporting to Management**: Configure PowerApps to generate regular reports on third-party breaches, summarizing key incidents, vendor performance, and any ongoing risks. These reports can be automatically distributed to senior management and compliance teams.

8. Enhance Security and Access Control
- **Vendor-Specific Access**: If vendors need to interact with PowerApps (e.g., for reporting incidents), ensure that role-based access controls are in place to limit what they can see and do within the application. Only relevant information should be accessible to third-party users.
- **Audit Logs**: Implement detailed audit logging within PowerApps to track all interactions related to third-party incidents. This includes logging who accessed or modified incident data and what actions were taken.

9. Conduct Routine Third-Party Incident Response Exercises
- **Simulated Vendor Breaches**: Use PowerApps to manage and simulate third-party breach scenarios as part of your routine incident response exercises. This helps assess the readiness of both your internal teams and your vendors to handle real-world incidents.
- **Review and Feedback Loop**: After each exercise, use PowerApps to collect feedback from all participants, including third-party vendors, and integrate any lessons learned into your incident response strategy.

10. Establish Automated Follow-Up Procedures
- **Vendor Follow-Up Workflow**: Implement automated workflows in PowerApps to follow up with vendors after a breach has been resolved. This can include requesting post-breach reports, updated risk assessments, or confirmation of remediation actions.
- **Ongoing Monitoring**: Use PowerApps to set up automated checks on third-party vendors, ensuring that any identified vulnerabilities from the breach have been addressed and that the vendor remains in compliance with your security standards.

Tools

Friday, August 16, 2024 1:53 PM

**1. PowerApps
- **Custom Forms and Apps**: Use PowerApps to build custom forms and applications for incident data entry, vendor breach reporting, and task management. PowerApps enables non-developers to create user-friendly interfaces that integrate with other systems.
- **Dashboards**: Integrate Power BI dashboards within PowerApps for real-time monitoring of third-party incidents and risk metrics.

**2. Power Automate (formerly Microsoft Flow)
- **Automated Workflows**: Use Power Automate to create workflows that handle notifications, escalations, and task assignments automatically. Workflows can also trigger follow-ups with vendors and internal stakeholders.
- **Approval Processes**: Automate approval processes related to third-party incident management, ensuring that all necessary parties review and sign off on actions taken.

**3. Microsoft SharePoint or Dataverse
- **Data Storage**: Store incident reports, vendor details, compliance documentation, and post-incident reviews in SharePoint or Dataverse, which integrates seamlessly with PowerApps.
- **Document Management**: Use SharePoint's document management features to maintain version-controlled records of incident response plans, vendor contracts, and compliance audits.

**4. Microsoft Teams
- **Collaboration**: Integrate Microsoft Teams with PowerApps and Power Automate to facilitate real-time communication between teams during an incident response. Teams can also be used to notify stakeholders about incidents or escalate critical issues.
- **Incident Response Channels**: Create dedicated Teams channels for each incident, where all communications, files, and updates can be centralized.

**5. Azure Logic Apps
- **Advanced Integration**: For more complex integrations, such as connecting with third-party vendor systems or external APIs, Azure Logic Apps can be used. It provides robust connectors and workflows for integrating various services and automating responses.
- **API Management**: Manage and monitor API integrations with third-party systems, ensuring secure and reliable data exchange.

**6. Azure Sentinel (SIEM)
- **Security Monitoring**: Use Azure Sentinel to monitor third-party activities and detect suspicious behavior or breaches. Sentinel can trigger alerts and automatically feed incident data into PowerApps for response management.
- **Threat Intelligence Integration**: Integrate threat intelligence feeds with Sentinel to enhance the detection of third-party risks and automate the correlation of incidents with known threats.

**7. Microsoft 365 Compliance Center
- **Compliance Management**: Use the Compliance Center to monitor and enforce compliance with regulatory requirements and internal policies, especially related to third-party breaches.
- **Audit and Reporting**: Generate automated reports and audit logs for third-party incidents, ensuring that all activities are documented and compliant with regulations.

**8. Power BI
- **Visualization and Reporting**: Create detailed reports and dashboards to visualize incident response performance, vendor risk assessments, and compliance metrics. Power BI can pull data from PowerApps, SharePoint, and other sources to provide a comprehensive view.
- **Data Analysis**: Use Power BI's analytics capabilities to analyze trends in third-party incidents, identify recurring issues, and provide insights for improving incident response.

**9. Microsoft Defender for Cloud
- **Threat Detection and Response**: Use Microsoft Defender for Cloud to enhance security monitoring of third-party vendors' cloud environments. Integrate alerts and threat intelligence with PowerApps for a unified incident response.
- **Security Posture Management**: Continuously monitor and assess the security posture of third-party environments and automatically trigger responses if issues are detected.

**10. API Management Tools
- **Vendor API Integration**: Use tools like Postman or Azure API Management to interact with third-party vendor APIs. Automate data exchange, incident reporting, and updates from vendors into your incident response workflows.
- **Custom Connectors in PowerApps**: If third-party systems do not have pre-built connectors, you can create custom connectors in PowerApps to interface with vendor APIs.

**11. Incident Response Platforms
- **Third-Party Breach Management**: Use platforms like ServiceNow, Resilient, or PagerDuty for more specialized incident response management, especially if you need to handle complex third-party incidents. Integrate these platforms with PowerApps for seamless data flow.
- **Automated Playbooks**: Implement automated incident response playbooks within these platforms to handle third-party breaches, triggering actions within PowerApps and Power Automate.

**12. Vendor Risk Management Tools
- **Vendor Assessment**: Use tools like BitSight, SecurityScorecard, or UpGuard to continuously assess the security posture of third-party vendors. These assessments can be integrated into PowerApps to inform risk-based decisions.
- **Automated Risk Alerts**: Set up automated alerts from these tools to notify your PowerApps workflows when a vendor's risk score changes or a new vulnerability is detected.

**13. Data Encryption and Security Tools
- **Encryption**: Ensure that all data stored or transmitted through PowerApps, SharePoint, or any other integrated system is encrypted using tools like Azure Key Vault or Microsoft Information Protection.
- **Access Control**: Implement Azure Active Directory (AAD) for role-based access control (RBAC) and single sign-on (SSO) to manage user access to PowerApps and related systems securely.

**14. Azure Monitor
- **Incident Tracking**: Use Azure Monitor to track and log incidents, including those involving third-party vendors, providing a centralized location for monitoring and analysis.
- **Automated Alerts**: Set up automated alerts in Azure Monitor to trigger actions in PowerApps when certain thresholds or conditions are met.

Notes

Tuesday, September 3, 2024 7:08 AM

The review process for validating the incident response program encompassed a thorough examination of documented policies, procedures, and plans, aligned with regulatory requirements under 12 CFR 748.0 and Appendix A and B to Part 748. This included assessing the credit union's capability to identify, contain, and mitigate incidents, notify members and regulatory authorities, file timely Suspicious Activity Reports (SARs), and conduct post-incident reviews. Validation involved interviews with the Incident Response Team to ensure understanding of roles, responsibilities, and reporting obligations. Testing and review of periodic exercises, vendor incident response protocols, data recovery practices, communication mechanisms, and thresholds for incident escalation were also conducted. Furthermore, the process evaluated whether updates to the incident response plan incorporated required reporting timeframes, and if action items from lessons learned were tracked and implemented effectively. The results confirm adherence to regulatory standards and identify opportunities for continuous improvement.

1