BCP/DR

Friday, August 16, 2024 2:21 PM

Stmt 10: Disaster Recovery / Business Continuity Program

Stmt 10.1 CORE: Backup and Recovery Plans for Critical Systems and Services

- **Verify documentation**: Confirm that detailed backup and recovery plans are documented for all critical systems and services.
- **Identify critical systems**: Ensure that a list of critical systems and services is maintained and regularly updated.
- **Backup frequency**: Verify that the backup frequency meets the organization's recovery time objectives (RTOs) and recovery point objectives (RPOs).
- **Offsite storage**: Confirm that backups are stored offsite and that the location is secure and geographically separated from the primary site.
- **Data integrity**: Check that backup data integrity is verified through regular testing.
- **Recovery procedures**: Review the documented recovery procedures to ensure they are clear, concise, and have been tested for effectiveness.

Stmt 10.2 CORE: Business Impact Analysis (BIA)

- **Impact analysis documentation**: Confirm that a BIA is documented, identifying the potential impact of disruptive events on the entity's functions and processes.
- **Identification of critical functions**: Ensure that the BIA identifies critical functions, processes, and services, along with their interdependencies.
- **Assessment of financial impacts**: Check that the BIA includes an assessment of financial impacts for different scenarios.
- **Update frequency**: Verify that the BIA is reviewed and updated regularly or after significant changes to the business or IT infrastructure.
- **Management review**: Ensure that the BIA is reviewed and approved by senior management.

Stmt 10.3 CORE: Training and Testing of Contingency Plans

- **Training programs**: Verify that there are training programs in place for all employees, particularly those with roles in disaster recovery or business continuity.
- **Documentation of training**: Confirm that training sessions are documented, including attendance records, materials used, and assessment results.
- **Testing schedule**: Check that a testing schedule for contingency plans is documented and adhered to.
- **Types of tests**: Ensure that different types of tests (e.g., tabletop exercises, full-scale simulations) are conducted and documented.
- **Test results and improvements**: Verify that test results are reviewed, documented, and used to make improvements to contingency plans.

Stmt 10.4 CORE: Reporting to the Board

- **Board reporting process**: Ensure that there is a formal process for reporting the status of the business continuity program to the Board.
- **Report content**: Verify that reports include key metrics, test results, updates to plans, and any identified gaps or areas for improvement.
- **Frequency of reporting**: Confirm that reports are provided to the Board at least annually or after significant events/tests.
- **Board meeting minutes**: Review Board meeting minutes to ensure that the business continuity reports are discussed and that the Board provides oversight.

Stmt 10.5 CORE+: Redundant and Separated Data Centers

- **Redundancy documentation**: Verify that data centers are redundant and that this redundancy is documented in the disaster recovery plan.
- **Geographical separation**: Ensure that redundant data centers are appropriately separated geographically to mitigate risks from regional disasters.
- **Data synchronization**: Check that data is synchronized between data centers to ensure continuity of operations in case of a failure at one site.
- **Failover procedures**: Review failover procedures to ensure they are documented, tested, and effective.

Stmt 10.6 CORE+: Network Equipment and Communication Needs

- **Inventory of network equipment**: Verify that an up-to-date inventory of network equipment is maintained, including both entity-owned and personal devices used for work.
- **Connectivity plan**: Ensure that there is a documented plan for maintaining connectivity during a disaster, including alternative communication methods.
- **Mobile device management**: Confirm that policies and controls are in place for managing mobile devices, including security controls for personal devices used for work.
- **Vendor communication**: Check that communication methods with key vendors are documented and tested.

Stmt 10.7 CORE+: Prioritization and Procedures for Recovery

- **Recovery prioritization**: Ensure that there is a documented prioritization of functions, services, and processes for recovery in the event of a disaster.
- **Recovery procedures**: Verify that procedures for recovering prioritized functions, services, and processes are documented and tested.
- **Resource allocation**: Check that resources (personnel, technology, etc.) are allocated according to recovery priorities.

Stmt 10.8 CORE+: Exercises and Tests with Vendors

- **Vendor participation in tests**: Confirm that exercises and tests involving interaction with core and significant vendors are documented and regularly conducted.
- **Documentation of exercises**: Verify that results from these exercises are documented, including any issues identified and corrective actions taken.
- **Contractual agreements**: Ensure that contractual agreements with vendors include provisions for their participation in business continuity exercises.

Stmt 10.9 CORE+: Reciprocal Agreements

- **Documentation of agreements**: Verify that reciprocal agreements with other businesses or institutions for recovery are documented and

current.

- **Effectiveness of agreements**: Check that the effectiveness of these agreements has been tested and documented.
- **Legal review**: Ensure that reciprocal agreements have been reviewed by legal counsel to address potential risks and liabilities.

Stmt 10.10 CORE+: Risk Assessment for Critical Systems

- **Risk assessment documentation**: Verify that a risk assessment is conducted to determine critical systems, considering various threats and vulnerabilities.
- **Inclusion in continuity plan**: Ensure that the results of the risk assessment are integrated into the overall business continuity plan.
- **Update frequency**: Confirm that the risk assessment is reviewed and updated regularly or after significant changes.

Stmt 10.11 CORE+: Comprehensive Written Plan

- **Authority structure**: Verify that the written plan clearly identifies the persons with authority to enact the plan.
- **Vital records preservation**: Ensure that the plan includes methods for preserving and restoring vital records.
- **Restoration of critical services**: Check that there are documented methods for restoring critical member services.
- **Communication methods**: Confirm that the plan includes communication methods for employees, members, and regulators.
- **Notification of regulators**: Ensure that the plan includes procedures for notifying regulators in the event of a significant disruption.
- **Training and testing**: Verify that the plan includes provisions for regular training and testing of all components.

Stmt 10.12 CORE+: Internal Controls for Annual Review

- **Annual review process**: Ensure that there is a documented process for reviewing the disaster recovery/business continuity plan at least annually.
- **Documentation of reviews**: Verify that review findings are documented, including any identified gaps and actions taken to address them.
- **Board involvement**: Confirm that the results of the annual review are reported to the Board and that the Board provides oversight.
- **Continuous improvement**: Check that the review process includes mechanisms for continuous improvement of the plan.

Checklist for Integrating BIA with BCP

Friday, August 16, 2024 2:28 PM

Checklist for Integrating Business Impact Analysis (BIA) with Business Continuity Plan (BCP)
Aligned with Appendix A to Part 748, Title 12, and Appendix B to Part 749
This checklist ensures that a credit union's **Business Continuity Plan (BCP)** is properly aligned with the **Business Impact Analysis (BIA)** and complies with regulatory requirements as outlined in **Appendix A to Part 748, Title 12** and **Appendix B to Part 749**. Each step refers to specific regulatory sections to ensure compliance.

1. Alignment of BIA Findings with BCP Objectives

1.1 Critical Function Prioritization
- **Action:** Ensure that the BCP prioritizes recovery efforts based on the critical functions identified in the BIA, considering their Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs).
- **Reference: Appendix A, Section III(A)(1)** – Requires the identification and prioritization of critical functions in safeguarding member information.

1.2 Risk Mitigation Strategies
- **Action:** Verify that the BCP incorporates risk mitigation strategies that address the specific vulnerabilities and dependencies identified in the BIA.
- **Reference: Appendix A, Section III(B)(1)** – Ensures that the BCP includes mitigation strategies for potential risks and threats.

1.3 Resource Allocation
- **Action:** Confirm that the BCP allocates resources (e.g., personnel, technology, financial) according to the criticality of business functions as determined by the BIA.
- **Reference: Appendix A, Section III(A)(2)** – Requires resource allocation based on the criticality of functions necessary to protect member information.

2. Continuity and Recovery Strategies

2.1 Continuity Strategies
- **Action:** Ensure that the BCP includes continuity strategies (e.g., alternate work locations, redundant systems) that directly align with the BIA's assessment of critical functions.
- **Reference: Appendix A, Section III(B)(2)** – The BCP must include strategies for maintaining continuity of critical operations.

2.2 Recovery Procedures
- **Action:** Verify that the BCP details specific recovery procedures for each critical function identified in the BIA, including timelines and responsible parties.
- **Reference: Appendix A, Section III(B)(1)** – Recovery procedures should be clear, tested, and aligned with critical functions.

2.3 Alternate Suppliers and Partners
- **Action:** Confirm that the BCP includes arrangements with alternate suppliers or partners for critical services identified as high-risk in the BIA.
- **Reference: Appendix B to Part 749** – Ensures that recovery plans include provisions for alternate vendors to maintain critical operations.

3. Communication and Coordination

3.1 Communication Plans
- **Action:** Ensure that the BCP includes communication plans that address the needs of the critical functions identified in the BIA, including internal and external stakeholders.
- **Reference: Appendix A, Section III(C)(1)(e)** – Communication strategies must be in place to inform stakeholders during disruptions.

3.2 Incident Response Teams
- **Action:** Verify that the BCP outlines the roles and responsibilities of incident response teams in relation to the critical functions identified in the BIA.
- **Reference: Appendix A, Section III(A)(2)** – The plan must define the roles of key personnel in incident response and recovery efforts.

3.3 Coordination with External Entities
- **Action:** Confirm that the BCP includes plans for coordinating with external entities (e.g., suppliers, regulators) as identified in the BIA's dependencies analysis.
- **Reference: Appendix B to Part 749** – External entities must be included in the recovery process to ensure business continuity.

4. Testing and Exercising

4.1 Scenario Development
- **Action:** Ensure that the BCP's testing and exercise scenarios are informed by the critical functions and potential impacts identified in the BIA.
- **Reference: Appendix A, Section III(B)(3)** – The BCP must include regular testing to validate continuity plans based on realistic scenarios.

4.2 Validation of Recovery Strategies
- **Action:** Verify that BCP tests and exercises validate the effectiveness of the recovery strategies for the critical functions identified in the BIA.
- **Reference: Appendix A, Section III(B)(1)** – Testing must verify the effectiveness of recovery procedures for critical systems.

4.3 Inclusion of BIA Findings
- **Action:** Confirm that the results of the BIA are used to develop realistic test scenarios that address the most significant risks and impacts.
- **Reference: Appendix A, Section III(B)(2)** – Test scenarios must reflect the risk assessments and BIA findings.

5. Review and Update Processes

5.1 BCP Update Schedule
- **Action:** Ensure that the BCP is updated regularly or after significant changes in business operations, in alignment with the findings of periodic BIA reviews.
- **Reference: Appendix A, Section III(B)(2)** – The BCP must be regularly reviewed and updated based on changes in the organization.

5.2 Feedback Incorporation
- **Action:** Verify that feedback from BIA results is incorporated into the BCP during regular reviews or after major incidents.
- **Reference: Appendix A, Section III(B)(3)** – Review findings and feedback from BIA and testing exercises must be incorporated into the BCP.

5.3 Continuous Improvement
- **Action:** Confirm that there is a process in place to continuously improve the BCP based on new insights gained from updated BIA findings.
- **Reference: Appendix A, Section III(B)(3)** – Continuous improvement mechanisms must be part of the BCP's review process.

6. Documentation and Reporting

6.1 Consistency in Documentation
- **Action:** Ensure that the critical functions, RTOs, RPOs, and other key data identified in the BIA are consistently reflected in the BCP documentation.
- **Reference: Appendix A, Section III(A)(1)** – The BCP must consistently reflect the critical functions identified in the BIA.

6.2 BCP Reporting
- **Action:** Verify that the BCP includes mechanisms for reporting the status of continuity efforts for critical functions as identified in the BIA to senior management.
- **Reference: Appendix A, Section III(C)(2)(b)** – Regular reports on the status of the BCP must be presented to senior management.

6.3 Compliance with Standards
- **Action:** Confirm that the integration of the BIA with the BCP is documented and meets relevant regulatory and industry standards (e.g., ISO 22301).
- **Reference: Appendix A, Section III(B)(1)** – Compliance with regulatory and industry standards must be documented and ensured.

7. Stakeholder Engagement

7.1 Stakeholder Alignment
- **Action:** Ensure that the BCP has been reviewed and approved by all relevant stakeholders, including those responsible for the critical functions identified in the BIA.
- **Reference: Appendix A, Section III(C)(2)(b)** – The BCP must be reviewed and approved by stakeholders, including senior management and board members.

7.2 Awareness and Training
- **Action:** Verify that training programs incorporate BIA findings to ensure that stakeholders understand their roles in the continuity of critical functions.
- **Reference: Appendix A, Section III(C)(1)(b)** – Regular training on the BCP and its integration with the BIA must be conducted.

7.3 Feedback Mechanisms
- **Action:** Confirm that there are mechanisms in place for stakeholders to provide feedback on the integration of BIA findings into the BCP.
- **Reference: Appendix A, Section III(B)(3)** – Feedback mechanisms must be included to continuously improve the BCP based on stakeholder input.

8. Compliance and Auditability

8.1 Regulatory Alignment
- **Action:** Ensure that the BCP's alignment with the BIA meets any applicable regulatory requirements or industry guidelines.
- **Reference: Appendix A, Section III(A)(1)** – The BCP must comply with regulatory requirements, including integration with the BIA.

8.2 Audit Readiness
- **Action:** Verify that the integration of BIA findings into the BCP is well-documented and that the organization is prepared for potential audits or reviews.
- **Reference: Appendix B to Part 749** – All continuity and recovery processes must be documented and audit-ready.

By following this **checklist** and adhering to the specific regulatory references from **Appendix A to Part 748, Title 12** and **Appendix B to Part 749**, credit unions can ensure that their **Business Continuity Plan (BCP)** is effectively aligned with the findings of the **Business Impact Analysis (BIA)** and meets regulatory and operational standards.

Issues

Thursday, September 19, 2024 2:31 PM

Stmt 10.1 CORE: Backup and Recovery Plans for Critical Systems and Services

Potential Findings:

1. **Missing or Incomplete Backup and Recovery Plans:**
   - **Impact:** Without documented plans, critical systems may not be recoverable in a timely manner following an incident.
   - **Reference: Appendix A to Part 748, Section III(B)(1)**
2. **Outdated List of Critical Systems:**
   - **Impact:** Critical systems may be overlooked during backup and recovery efforts if the list is not regularly updated.
   - **Reference: Appendix A, Section III(C)(1)(a)**
3. **Backup Frequency Does Not Meet RTOs/RPOs:**
   - **Impact:** If backups are not frequent enough, the organization may suffer data loss or extended downtime.
   - **Reference: Appendix B to Part 749**
4. **Backups Not Stored Offsite:**
   - **Impact:** Storing backups onsite increases the risk of data loss in case of physical disasters (e.g., fires, floods).
   - **Reference: Appendix A, Section III(A)(3)**
5. **Lack of Regular Data Integrity Testing:**
   - **Impact:** Without regular testing, there is no assurance that backups can be restored successfully when needed.
   - **Reference: Appendix B to Part 749**
6. **Unclear or Untested Recovery Procedures:**
   - **Impact:** Recovery efforts may be delayed or ineffective if procedures are not clear or tested.
   - **Reference: Appendix A, Section III(B)(1)**

Stmt 10.2 CORE: Business Impact Analysis (BIA)

Potential Findings:

1. **BIA Not Documented:**
   - **Impact:** The organization may not understand the potential impact of disruptive events, resulting in uncoordinated recovery efforts.
   - **Reference: Appendix A, Section III(A)(1)**
2. **Critical Functions Not Properly Identified:**
   - **Impact:** If critical functions and interdependencies are not identified, resources may be misallocated during a disaster recovery.
   - **Reference: Appendix A, Section III(A)(1)**
3. **Lack of Financial Impact Assessment:**
   - **Impact:** The organization may not properly account for financial losses in its recovery efforts, impacting overall business recovery.
   - **Reference: Appendix A, Section III(B)(2)**
4. **BIA Not Regularly Updated:**
   - **Impact:** Failure to review and update the BIA regularly means it may not reflect current business processes or IT infrastructure.
   - **Reference: Appendix A, Section III(B)(2)**
5. **BIA Not Approved by Senior Management:**
   - **Impact:** Without management approval, the BIA may not receive sufficient organizational support or funding.
   - **Reference: Appendix A, Section III(A)(1)**

Stmt 10.3 CORE: Training and Testing of Contingency Plans

Potential Findings:

1. **Lack of Employee Training Programs:**
   - **Impact:** Employees may not understand their roles in disaster recovery, resulting in confusion during an actual event.
   - **Reference: Appendix A, Section III(C)(1)(b)**
2. **Training Not Documented:**
   - **Impact:** Without documentation, it is difficult to verify whether staff have been adequately trained.
   - **Reference: Appendix A, Section III(C)(1)(c)**
3. **No Documented Testing Schedule for Contingency Plans:**
   - **Impact:** Contingency plans may not be tested frequently enough to identify potential issues or gaps.
   - **Reference: Appendix A, Section III(B)(3)**
4. **Lack of Test Variety (e.g., Tabletop Exercises, Simulations):**
   - **Impact:** Without testing different scenarios, the organization may not be fully prepared for various disaster types.
   - **Reference: Appendix A, Section III(B)(3)**
5. **Test Results Not Documented or Used for Improvements:**
   - **Impact:** Without reviewing and documenting test results, there is no way to improve the contingency plans based on lessons learned.
   - **Reference: Appendix A, Section III(B)(3)**

Stmt 10.4 CORE: Reporting to the Board

Potential Findings:

1. **No Formal Process for Reporting to the Board:**
   - **Impact:** The Board may not be aware of the current status of the business continuity program, reducing their oversight capabilities.

    - **Reference: Appendix A, Section III(C)(2)(b)**
2. **Reports Do Not Include Key Metrics or Test Results:**
    - **Impact:** Without key data, the Board cannot fully understand the effectiveness of the disaster recovery program.
    - **Reference: Appendix A, Section III(C)(2)(b)**
3. **Reports Not Provided to the Board Regularly:**
    - **Impact:** Infrequent updates may leave the Board unaware of significant developments or gaps in the business continuity program.
    - **Reference: Appendix A, Section III(C)(2)(b)**
4. **Board Meeting Minutes Do Not Reflect Oversight of the Business Continuity Program:**
    - **Impact:** If discussions and decisions related to business continuity are not reflected in meeting minutes, there is a lack of accountability.
    - **Reference: Appendix A, Section III(C)(2)(b)**

Stmt 10.5 CORE+: Redundant and Separated Data Centers

Potential Findings:

1. **Lack of Documented Redundancy for Data Centers:**
    - **Impact:** Without redundancy, the organization risks losing critical data and services if one data center fails.
    - **Reference: Appendix A, Section III(A)(3)**
2. **Geographical Separation Not Ensured:**
    - **Impact:** Data centers located too close together may both be affected by the same regional disaster (e.g., earthquakes, hurricanes).
    - **Reference: Appendix A, Section III(B)(2)**
3. **Data Not Synchronized Between Centers:**
    - **Impact:** If data is not synchronized, there may be data loss or inconsistencies during failover.
    - **Reference: Appendix B to Part 749**
4. **Failover Procedures Not Documented or Tested:**
    - **Impact:** Without clear and tested failover procedures, recovery efforts may be delayed during a disaster.
    - **Reference: Appendix A, Section III(B)(1)**

Stmt 10.6 CORE+: Network Equipment and Communication Needs

Potential Findings:

1. **Incomplete Inventory of Network Equipment:**
    - **Impact:** Missing or outdated inventory may hinder recovery efforts if critical devices are overlooked.
    - **Reference: Appendix A, Section III(A)(1)**
2. **No Connectivity Plan for Disasters:**
    - **Impact:** Without a documented plan, the organization may lose network connectivity during a disaster, slowing recovery efforts.
    - **Reference: Appendix A, Section III(B)(1)**
3. **Inadequate Mobile Device Management (MDM):**
    - **Impact:** Personal devices used for work may introduce security risks if not properly managed.
    - **Reference: Appendix A, Section III(C)(1)(c)**
4. **Vendor Communication Not Documented or Tested:**
    - **Impact:** Lack of communication with key vendors during a disaster may delay critical services or supplies needed for recovery.
    - **Reference: Appendix B to Part 749**

Stmt 10.7 CORE+: Prioritization and Procedures for Recovery

Potential Findings:

1. **Lack of Documented Recovery Prioritization:**
    - **Impact:** Without prioritization, critical functions may not be recovered in a timely manner, leading to extended downtime.
    - **Reference: Appendix A, Section III(A)(1)**
2. **Recovery Procedures Not Tested:**
    - **Impact:** If recovery procedures are not tested, they may fail during an actual disaster.
    - **Reference: Appendix A, Section III(B)(1)**
3. **Resources Not Allocated According to Priorities:**
    - **Impact:** Misallocation of resources may lead to inefficient recovery efforts, further extending the impact of a disaster.
    - **Reference: Appendix A, Section III(B)(2)**

Remediation

Thursday, September 19, 2024 2:39 PM

Remediation Steps for Findings in Stmt 10: Disaster Recovery / Business Continuity Program

Stmt 10.1 CORE: Backup and Recovery Plans for Critical Systems and Services

1. Missing or Incomplete Backup and Recovery Plans

- **Remediation Steps:**
  1. **Develop and Document Backup and Recovery Plans:** Create detailed plans for each critical system, including specific backup processes, locations, and recovery procedures.
  2. **Ensure Regular Updates:** Establish a process for reviewing and updating these plans annually or after significant changes.
  3. **Assign Responsibilities:** Designate personnel responsible for maintaining and updating the backup and recovery documentation.
  - **Reference: Appendix A to Part 748, Section III(B)(1)**

2. Outdated List of Critical Systems

- **Remediation Steps:**
  1. **Review and Update Critical Systems List:** Conduct a thorough review of all critical systems and ensure the list is accurate and current.
  2. **Establish Regular Review Cadence:** Schedule regular updates (e.g., quarterly) to the critical systems list to reflect changes in IT infrastructure.
  3. **Centralize Documentation:** Maintain the critical systems list in a centralized, accessible location.
  - **Reference: Appendix A, Section III(C)(1)(a)**

3. Backup Frequency Does Not Meet RTOs/RPOs

- **Remediation Steps:**
  1. **Adjust Backup Schedules:** Modify backup schedules to meet the Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs) for each critical system.
  2. **Test Backup Restoration:** Regularly test the backup process to ensure it meets the defined RTO/RPO criteria.
  3. **Monitor Compliance:** Use automated tools to monitor backup frequency and flag any discrepancies.
  - **Reference: Appendix B to Part 749**

4. Backups Not Stored Offsite

- **Remediation Steps:**
  1. **Implement Offsite Backup Strategy:** Use secure offsite locations or cloud services for storing backups to mitigate risks from physical disasters.
  2. **Ensure Geographic Separation:** Verify that offsite locations are geographically separated from the primary site to reduce the risk of regional disasters.
  3. **Test Offsite Backup Retrieval:** Conduct regular tests of offsite backups to ensure they can be retrieved and restored efficiently.
  - **Reference: Appendix A, Section III(A)(3)**

5. Lack of Regular Data Integrity Testing

- **Remediation Steps:**
  1. **Implement Regular Integrity Checks:** Schedule regular tests to verify the integrity and recoverability of backup data.
  2. **Document Testing Results:** Maintain records of all integrity tests and their outcomes to demonstrate compliance.
  3. **Use Automated Tools:** Utilize automated tools to regularly test and verify the integrity of backups.
  - **Reference: Appendix B to Part 749**

6. Unclear or Untested Recovery Procedures

- **Remediation Steps:**
  1. **Clarify and Document Procedures:** Develop detailed recovery procedures for each critical system and ensure they are documented clearly.
  2. **Conduct Regular Testing:** Schedule regular tests of recovery procedures to ensure they work effectively in real-world scenarios.
  3. **Train Staff:** Provide staff training on recovery procedures to ensure they are well-prepared during an actual incident.
  - **Reference: Appendix A, Section III(B)(1)**

Stmt 10.2 CORE: Business Impact Analysis (BIA)

1. BIA Not Documented

- **Remediation Steps:**
  1. **Develop and Document the BIA:** Work with all relevant departments to conduct and document a thorough Business Impact Analysis (BIA).
  2. **Formalize BIA Review:** Ensure that the BIA is reviewed and approved by senior management.
  3. **Centralize BIA Documentation:** Store the documented BIA in a central location for easy access and updates.
  - **Reference: Appendix A, Section III(A)(1)**

2. Critical Functions Not Properly Identified

- **Remediation Steps:**
  1. **Identify and Document Critical Functions:** Conduct a thorough assessment to identify all critical business functions, including dependencies and interdependencies.
  2. **Engage Department Heads:** Involve key department heads in identifying critical functions and validating their importance.
  3. **Update Regularly:** Implement a process to regularly review and update the list of critical functions.
  - **Reference: Appendix A, Section III(A)(1)**

3. Lack of Financial Impact Assessment

- **Remediation Steps:**
  1. **Conduct Financial Impact Analysis:** Work with finance and other relevant departments to assess and quantify the financial impact of potential disruptions.
  2. **Document Financial Impacts:** Ensure that financial impact assessments are included in the BIA report.
  3. **Review Regularly:** Update the financial impact analysis as business processes or financial conditions change.
  - **Reference: Appendix A, Section III(B)(2)**

4. BIA Not Regularly Updated

- **Remediation Steps:**
  1. **Establish an Update Schedule:** Ensure the BIA is reviewed and updated at least annually or after major changes to business processes or IT infrastructure.
  2. **Assign Ownership:** Designate a team responsible for updating the BIA and communicating any changes to stakeholders.
  3. **Monitor Changes in Critical Systems:** Implement a change management process to trigger BIA reviews when critical systems are updated.
  - **Reference: Appendix A, Section III(B)(2)**

5. BIA Not Approved by Senior Management

- **Remediation Steps:**
  1. **Present BIA to Senior Management:** Ensure that the BIA is submitted for review and approval by senior management.
  2. **Provide Regular Updates to Management:** Regularly update senior management on BIA findings, changes, and the overall business continuity program.
  3. **Track Approval:** Document and track the approval process to demonstrate oversight and management support.
  - **Reference: Appendix A, Section III(A)(1)**

Stmt 10.3 CORE: Training and Testing of Contingency Plans

1. Lack of Employee Training Programs

- **Remediation Steps:**
  1. **Develop Training Programs:** Implement training programs for all employees, focusing on their roles in disaster recovery and business continuity.
  2. **Track Training Completion:** Use a learning management system (LMS) to track training completion and ensure all relevant staff have received training.
  3. **Conduct Refresher Courses:** Schedule regular refresher courses for employees to maintain their preparedness.
  - **Reference: Appendix A, Section III(C)(1)(b)**

2. Training Not Documented

- **Remediation Steps:**
  1. **Document All Training Activities:** Maintain detailed records of all training activities, including dates, participants, and outcomes.
  2. **Centralize Training Records:** Store training records in a centralized system accessible for compliance reviews and audits.
  3. **Use Automation:** Automate the documentation of training activities through training management software.
  - **Reference: Appendix A, Section III(C)(1)(c)**

3. No Documented Testing Schedule for Contingency Plans

- **Remediation Steps:**
  1. **Establish a Formal Testing Schedule:** Develop and document a schedule for regularly testing contingency plans.
  2. **Adhere to Testing Cadence:** Ensure testing occurs at defined intervals (e.g., annually or biannually) and after major system changes.
  3. **Communicate the Schedule:** Share the testing schedule with all relevant stakeholders to ensure participation.
  - **Reference: Appendix A, Section III(B)(3)**

4. Lack of Test Variety (e.g., Tabletop Exercises, Simulations)

- **Remediation Steps:**
  1. **Implement Diverse Testing Methods:** Introduce various testing methods, including tabletop exercises, full-scale simulations, and scenario-based drills.
  2. **Test Real-World Scenarios:** Ensure that different types of potential disasters are tested to assess readiness for multiple scenarios.
  3. **Document Test Results:** Record the outcomes of each test and evaluate the effectiveness of the contingency plans.
  - **Reference: Appendix A, Section III(B)(3)**

5. Test Results Not Documented or Used for Improvements

- **Remediation Steps:**
  1. **Document All Test Results:** Ensure detailed documentation of all test results, including identified gaps and areas for improvement.
  2. **Conduct Post-Test Reviews:** Hold post-test review sessions to discuss the results and identify actionable improvements.
  3. **Update Contingency Plans:** Modify and improve contingency plans based on the results and lessons learned from tests.
  - **Reference: Appendix A, Section III(B)(3)**

Stmt 10.4 CORE: Reporting to the Board

1. No Formal Process for Reporting to the Board

- **Remediation Steps:**
    1. **Establish a Reporting Process:** Develop a formalized process for reporting the status of the business continuity program to the Board.
    2. **Create a Regular Reporting Cadence:** Schedule regular reporting sessions (e.g., quarterly or annually) to provide the Board with updates.
    3. **Involve Senior Management:** Ensure that senior management is involved in preparing the reports for Board review.
    - **Reference: Appendix A, Section III(C)(2)(b)**

2. Reports Do Not Include Key Metrics or Test Results

- **Remediation Steps:**
    1. **Include Comprehensive Metrics in Reports:** Ensure that key metrics (e.g., RTOs, test results, incident response times) are included in Board reports.
    2. **Report on Testing and Incident Results:** Include results from contingency plan tests, incidents, and recovery efforts.
    3. **Provide Actionable Insights:** Ensure that reports offer insights into program performance and any areas that require improvement.
    - **Reference: Appendix A, Section III(C)(2)(b)**

3. Reports Not Provided to the Board Regularly

- **Remediation Steps:**
    1. **Schedule Regular Reports:** Set a regular reporting schedule to provide the Board with timely updates on the business continuity program.
    2. **Track Reporting Compliance:** Use a tracking system to ensure that reports are delivered on schedule and reviewed by the Board.
    3. **Automate Reminders:** Automate reminders to ensure that reports are prepared and submitted on time.
    - **Reference: Appendix A, Section III(C)(2)(b)**

4. Board Meeting Minutes Do Not Reflect Oversight of the Business Continuity Program

- **Remediation Steps:**
    1. **Document Business Continuity Discussions:** Ensure that discussions about the business continuity program are reflected in the Board meeting minutes.
    2. **Track Board Actions:** Document decisions made by the Board regarding the business continuity program and follow up on those actions.
    3. **Ensure Accountability:** Assign responsibility for ensuring that all Board decisions related to business continuity are implemented.
    - **Reference: Appendix A, Section III(C)(2)(b)**

By implementing these remediation steps, credit unions can address gaps in their **Disaster Recovery and Business Continuity Program**, ensuring compliance with **Appendix A to Part 748, Title 12** and **Appendix B to Part 749**. These steps will help ensure that critical systems, functions, and processes are safeguarded against disruption, improving the organization's overall resilience.

Compliance

Thursday, September 19, 2024 2:16 PM

Compliance Steps for Stmt 10: Disaster Recovery / Business Continuity Program
Aligned with Appendix A to Part 748, Title 12, and Appendix B to Part 749
To comply with **Appendix A to Part 748** and **Appendix B to Part 749**, credit unions must establish a comprehensive and effective **Disaster Recovery and Business Continuity Program**. The steps below ensure compliance with regulatory requirements for each sub-statement in **Stmt 10**.

Stmt 10.1 CORE: Backup and Recovery Plans for Critical Systems and Services
Compliance Steps:
1. **Document Backup and Recovery Plans:**
   - **Action:** Ensure that backup and recovery plans for all critical systems and services are fully documented and up to date.
   - **Reference: Appendix A to Part 748, Section III(B)(1)** – Requires safeguarding member information by ensuring recoverability in the event of a system failure.
2. **Maintain a List of Critical Systems:**
   - **Action:** Maintain and regularly update a list of critical systems and services.
   - **Reference: Appendix A, Section III(C)(1)(a)** – Ensure the identification of critical systems involved in safeguarding member data.
3. **Verify Backup Frequency:**
   - **Action:** Ensure that backup frequency meets recovery time objectives (RTOs) and recovery point objectives (RPOs).
   - **Reference: Appendix B to Part 749** – Requires credit unions to have an effective records preservation program, including backup procedures.
4. **Store Backups Offsite:**
   - **Action:** Store backups in a secure offsite location that is geographically separated from the primary site.
   - **Reference: Appendix A, Section III(A)(3)** – Requires data to be safeguarded, including through offsite backup storage.
5. **Test Data Integrity:**
   - **Action:** Perform regular integrity checks on backup data to ensure recoverability.
   - **Reference: Appendix B to Part 749** – Ensures that records can be recovered accurately in the event of a disaster.
6. **Review Recovery Procedures:**
   - **Action:** Ensure recovery procedures are documented, concise, and tested for effectiveness.
   - **Reference: Appendix A, Section III(B)(1)** – Requires the testing of controls to ensure recoverability.

Stmt 10.2 CORE: Business Impact Analysis (BIA)
Compliance Steps:
1. **Document the BIA:**
   - **Action:** Ensure a Business Impact Analysis (BIA) is documented, identifying the potential impact of disruptive events.
   - **Reference: Appendix A, Section III(A)(1)** – The BIA should assess risks to member information and critical functions.
2. **Identify Critical Functions:**
   - **Action:** Identify critical business functions, processes, and services, including their interdependencies.
   - **Reference: Appendix A, Section III(A)(1)** – Requires identification of systems and processes essential for safeguarding member information.
3. **Assess Financial Impact:**
   - **Action:** Include an assessment of financial impacts for various disaster scenarios.
   - **Reference: Appendix A, Section III(B)(2)** – The BIA should evaluate the financial risks posed by business interruptions.
4. **Update BIA Regularly:**
   - **Action:** Ensure the BIA is reviewed and updated after significant changes to the business or IT infrastructure.
   - **Reference: Appendix A, Section III(B)(2)** – Requires regular updates to the risk assessment.
5. **Obtain Management Approval:**
   - **Action:** Ensure that the BIA is reviewed and approved by senior management.
   - **Reference: Appendix A, Section III(A)(1)** – Senior management must approve and oversee the business continuity program.

Stmt 10.3 CORE: Training and Testing of Contingency Plans
Compliance Steps:
1. **Establish Training Programs:**
   - **Action:** Ensure training programs are in place for all employees, particularly those with disaster recovery or business continuity roles.
   - **Reference: Appendix A, Section III(C)(1)(b)** – Requires that employees are trained on contingency plans.
2. **Document Training:**
   - **Action:** Document training sessions, including attendance, materials, and assessment results.
   - **Reference: Appendix A, Section III(C)(1)(c)** – Ensures documentation of training as part of the information security program.
3. **Create a Testing Schedule:**
   - **Action:** Develop and adhere to a documented schedule for testing contingency plans.
   - **Reference: Appendix A, Section III(B)(3)** – Requires regular testing of the information security program's components.
4. **Conduct Various Tests:**
   - **Action:** Conduct a variety of tests, including tabletop exercises and full-scale simulations, to evaluate the effectiveness of contingency plans.
   - **Reference: Appendix A, Section III(B)(3)** – Testing of plans should include different scenarios to validate readiness.
5. **Review and Document Test Results:**
   - **Action:** Document test results, review the outcomes, and use them to improve contingency plans.
   - **Reference: Appendix A, Section III(B)(3)** – Test results must be used to identify gaps and improve recovery strategies.

Stmt 10.4 CORE: Reporting to the Board
Compliance Steps:
1. **Establish a Reporting Process:**
   - **Action:** Ensure that a formal process for reporting the status of the business continuity program to the Board is in place.
   - **Reference: Appendix A, Section III(C)(2)(b)** – Requires regular reporting to the Board on the status of the information security program.
2. **Include Key Metrics and Updates:**
   - **Action:** Ensure Board reports include key metrics, test results, updates to plans, and any identified gaps or improvements.
   - **Reference: Appendix A, Section III(C)(2)(b)** – Reports should include critical updates and assessments.
3. **Maintain Reporting Frequency:**
   - **Action:** Confirm that reports are provided to the Board at least annually or after significant events/tests.
   - **Reference: Appendix A, Section III(C)(2)(b)** – Requires that regular updates be provided to the Board.
4. **Review Board Meeting Minutes:**
   - **Action:** Ensure Board meeting minutes reflect discussions of business continuity reports and show the Board's oversight.
   - **Reference: Appendix A, Section III(C)(2)(b)** – Ensures the Board is actively involved in overseeing the program.

Stmt 10.5 CORE+: Redundant and Separated Data Centers
Compliance Steps:
1. **Document Data Center Redundancy:**
   - **Action:** Ensure redundancy is documented for all critical data centers in the disaster recovery plan.
   - **Reference: Appendix A, Section III(A)(3)** – Redundancy helps safeguard member information.
2. **Ensure Geographic Separation:**
   - **Action:** Verify that redundant data centers are geographically separated to mitigate the risk of regional disasters.
   - **Reference: Appendix A, Section III(B)(2)** – Requires geographical separation for effective disaster recovery.
3. **Synchronize Data Between Centers:**
   - **Action:** Ensure data synchronization between data centers to maintain continuity of operations.
   - **Reference: Appendix B to Part 749** – Requires the preservation of records across geographically separated locations.
4. **Test Failover Procedures:**
   - **Action:** Document and test failover procedures to ensure they are effective in the event of a failure.
   - **Reference: Appendix A, Section III(B)(1)** – Testing of controls includes the failover process.

Stmt 10.6 CORE+: Network Equipment and Communication Needs
Compliance Steps:
1. **Maintain an Inventory of Network Equipment:**
   - **Action:** Verify that an updated inventory of all network equipment is maintained.
   - **Reference: Appendix A, Section III(A)(1)** – Requires identification and safeguarding of critical assets.
2. **Develop a Connectivity Plan:**
   - **Action:** Ensure a documented plan for maintaining network connectivity during a disaster, including alternative communication methods.
   - **Reference: Appendix A, Section III(B)(1)** – Requires contingency planning for maintaining essential services.
3. **Manage Mobile Devices:**
   - **Action:** Confirm that policies and controls are in place for managing mobile devices, including personal devices.
   - **Reference: Appendix A, Section III(C)(1)(c)** – Requires policies for device management to ensure secure access.
4. **Test Vendor Communication:**
   - **Action:** Document and test communication methods with key vendors as part of the business continuity plan.
   - **Reference: Appendix B to Part 749** – Requires plans to ensure continued communication with vendors during recovery.

Stmt 10.7 CORE+: Prioritization and Procedures for Recovery

Compliance Steps:

1. **Document Recovery Prioritization:**
   - **Action:** Ensure recovery prioritization for critical functions and services is documented.
   - **Reference: Appendix A, Section III(A)(1)** – The continuity plan must prioritize critical systems and services.
2. **Test Recovery Procedures:**
   - **Action:** Verify that procedures for recovering prioritized functions are documented and tested.
   - **Reference: Appendix A, Section III(B)(1)** – Regular testing of recovery procedures is required.
3. **Allocate Resources:**
   - **Action:** Ensure resources (personnel, technology) are allocated according to recovery priorities.
   - **Reference: Appendix A, Section III(B)(2)** – Resource allocation must align with the business continuity plan.

By following these **compliance steps**, credit unions can ensure that their **Disaster Recovery and Business Continuity Program** aligns with the regulatory requirements of **Appendix A to Part 748, Title 12** and **Appendix B to Part 749**, enabling them to effectively protect member data, maintain critical operations, and mitigate the impact of disruptions.

RTO/RPO

Thursday, September 19, 2024 2:18 PM

RTO (Recovery Time Objective) and **RPO (Recovery Point Objective)** are two critical metrics in disaster recovery and business continuity planning. They define the maximum acceptable downtime a nd data loss during a disruption. Ensuring compliance with **RTO/RPO** helps an organization meet regulatory requirements and maintain operational resilience.
Here's an overview of **RTO/RPO compliance**:

1. Understanding RTO (Recovery Time Objective)

RTO Definition:

- **RTO** is the maximum acceptable time a system, application, or function can be offline after a disruption before it causes signific ant business harm.

Compliance Requirements for RTO:

- **Appendix A to Part 748, Title 12** requires financial institutions to protect member information and maintain operational continuity. Ensuring systems are resto red within defined RTOs aligns with these requirements.
- **Appendix B to Part 749** mandates that critical operations must be restored within a timeframe that prevents significant disruption to members and sta keholders.

Steps for RTO Compliance:

1. **Identify Critical Systems:** Develop a list of critical systems and functions that need to be restored quickly after an outage.
2. **Define Acceptable Downtime:** Set specific RTOs for each system, ensuring they align with the organization's business impact analysis (BIA).
3. **Test Recovery Procedures:** Regularly test recovery procedures to confirm that systems can be restored within the RTO.
4. **Monitor and Adjust:** Review RTOs after significant changes in business processes, infrastructure, or regulations.

2. Understanding RPO (Recovery Point Objective)

RPO Definition:

- **RPO** is the maximum amount of data loss measured in time that is acceptable during a disruption. It defines how far back in time d ata must be recovered following a failure.

Compliance Requirements for RPO:

- **Appendix A to Part 748, Section III(B)(1)** mandates the protection of member information, which includes ensuring that data loss is minimized through appropriate backup procedures.
- **Appendix B to Part 749** requires that records be preserved in a manner that allows for their recovery within a specific time window, ensuring minimal data loss.

Steps for RPO Compliance:

1. **Assess Data Criticality:** Identify the critical data that must be backed up frequently to minimize data loss.
2. **Set Backup Intervals:** Define RPOs for each system and ensure backup processes (e.g., real -time, hourly, daily) align with the organization's data loss tolerance.
3. **Test Data Recovery:** Regularly test data recovery from backups to verify that data can be restored within the RPO.
4. **Review and Update:** Update RPOs in response to system upgrades, changes in data storage solutions, or regulatory requirements.

3. RTO/RPO Compliance Best Practices

Documentation and Plan Alignment:

- **Action:** Document all RTOs and RPOs in the disaster recovery and business continuity plans.
- **Reference: Appendix A to Part 748, Section III(A)** requires the documentation of procedures to recover critical systems and protect member information.

Backup and Recovery Infrastructure:

- **Action:** Implement robust backup and recovery systems that support the defined RPOs and RTOs.
- **Reference: Appendix B to Part 749** mandates the safeguarding and recoverability of records in a timely manner, ensuring minimal impact to member services.

Testing and Review:

- **Action:** Perform regular testing of backup and recovery processes to ensure they meet the defined RTO and RPO.
- **Reference: Appendix A, Section III(B)(3)** requires regular testing of the information security program, including recovery strategies.

Senior Management Oversight:

- **Action:** Ensure that RTO and RPO metrics are reviewed and approved by senior management and the Board of Directors.
- **Reference: Appendix A to Part 748, Section III(C)(2)(b)** requires the Board to oversee the institution's disaster recovery and business continuity efforts.

4. Challenges to RTO/RPO Compliance:

Challenges:

- **Complex IT Environments:** Organizations with complex IT systems may struggle to restore systems quickly or lose data beyond acceptable levels.
- **Inadequate Testing:** Without regular testing, recovery procedures may fail to meet the RTO/RPO requirements during an actual event.
- **Outdated Plans:** Failure to update business continuity plans can result in RTO/RPO metrics that no longer reflect the current IT and business environment.

Solutions:

- **Automated Backup Solutions:** Implementing real-time or near-real-time data replication can ensure compliance with stringent RPOs.
- **Cloud-Based Disaster Recovery:** Using cloud platforms for redundancy can help organizations meet RTOs by quickly restoring services from remote locations.
- **Continuous Testing and Updates:** Regularly test backup and recovery plans and update them to reflect changes in the organization or its risk environment.

5. Regulatory Reporting and Accountability

Reporting Requirements:

- **Action:** Report RTO/RPO compliance status to regulators, such as the NCUA (National Credit Union Administration), as required.
- **Reference: Appendix A to Part 748, Section III(C)(2)(b)** requires institutions to report on the effectiveness of their business continuity and disaster recovery efforts to senior man agement and regulatory bodies.

Documentation of Non-Compliance:

- **Action:** If RTO/RPO compliance is not achieved, document the reasons and corrective actions taken to resolve the gaps.
- **Reference: Appendix B to Part 749** requires institutions to maintain accurate records and ensure they are available for audit.

By ensuring **RTO/RPO compliance**, financial institutions protect critical operations, minimize data loss, and meet the regulatory requirements outlined in **Appendix A to Part 748** and **Appendix B to Part 749**. This compliance ensures that the institution can recover from disruptions while safeguarding member information.

BIA

Friday, August 16, 2024 2:27 PM

Business Impact Analysis (BIA) Validation Checklist with Specific References to Appendix A to Part 748, Title 12, and Appendix B to Part 749
This checklist ensures compliance with **Appendix A to Part 748, Title 12** and **Appendix B to Part 749**. It provides a structured approach to conducting a Business Impact Analysis (BIA) for ensuring the continuity of critical business functions and services.

1. Pre-Analysis Preparation

Project Scope Definition
- **Action:** Ensure that the scope of the BIA is clearly defined, including which departments, functions, and processes are included.
- **Reference: Appendix A to Part 748, Section III(A)(1)** – The BIA should identify critical systems and processes that safeguard member information.

Stakeholder Identification
- **Action:** Confirm that all relevant stakeholders (e.g., department heads, IT, legal, finance) have been identified and involved in the BIA process.
- **Reference: Appendix A, Section III(A)(1)** – Involve key personnel to ensure effective risk identification and management of critical systems.

Objectives and Goals
- **Action:** Verify that the objectives and goals of the BIA are documented and aligned with the organization's overall risk management and business continuity objectives.
- **Reference: Appendix A, Section III(B)(1)** – Ensure alignment between business continuity objectives and safeguarding member data.

BIA Methodology
- **Action:** Ensure that the methodology to be used for the BIA is documented, understood by all stakeholders, and follows industry best practices.
- **Reference: Appendix A, Section III(A)(2)** – Requires documented policies and procedures to mitigate risks to critical functions.

Data Collection Tools
- **Action:** Check that appropriate tools (e.g., surveys, questionnaires, interviews) are identified for collecting data from different departments and functions.
- **Reference: Appendix A, Section III(A)(3)** – The data collection process must identify risks and assess the impact on critical functions.

2. Data Collection

Identification of Critical Business Functions
- **Action:** Verify that all critical business functions and processes have been identified and documented.
- **Reference: Appendix A, Section III(A)(1)** – Identify and document critical systems that handle member information.

Dependencies and Interdependencies
- **Action:** Ensure that both internal and external dependencies (e.g., IT systems, suppliers, third-party services) are identified for each critical function.
- **Reference: Appendix A, Section III(A)(1)** – Identify interdependencies that could affect the availability of critical systems.

Resource Requirements
- **Action:** Confirm that the necessary resources (e.g., personnel, technology, facilities) required for each critical function are documented.
- **Reference: Appendix B to Part 749** – Ensure that resources required to restore critical systems and services are identified.

Maximum Tolerable Downtime (MTD)
- **Action:** Check that the MTD for each critical function is documented, indicating the maximum time the function can be unavailable before severe consequences occur.
- **Reference: Appendix A, Section III(A)(1)** – Set specific recovery objectives to protect critical systems.

Recovery Time Objective (RTO)
- **Action:** Verify that the RTO for each critical function is documented, indicating the target time to restore operations after a disruption.
- **Reference: Appendix B to Part 749** – Ensure recovery objectives are defined to restore services within acceptable timeframes.

Recovery Point Objective (RPO)
- **Action:** Ensure that the RPO for each critical function is documented, indicating the maximum acceptable amount of data loss measured in time.
- **Reference: Appendix B to Part 749** – Requires the identification of acceptable data loss during recovery operations.

Impact Categories
- **Action:** Confirm that impact categories (e.g., financial, reputational, operational, legal) are identified and that the impact of a disruption is assessed for each category.
- **Reference: Appendix A, Section III(B)(2)** – The BIA must assess the financial, operational, and reputational impacts of disruptions.

Financial Impact Analysis
- **Action:** Ensure that potential financial impacts (e.g., revenue loss, increased costs) are quantified and documented.
- **Reference: Appendix A, Section III(B)(2)** – Quantify financial impacts to ensure the proper allocation of resources for business continuity.

Non-Financial Impacts
- **Action:** Verify that non-financial impacts (e.g., reputational damage, legal implications) are also assessed and documented.
- **Reference: Appendix A, Section III(B)(2)** – Non-financial impacts must be considered as part of the risk assessment.

Interviews and Surveys
- **Action:** Check that data collection through interviews and surveys is thorough, and that the responses are documented and validated.
- **Reference: Appendix A, Section III(A)(3)** – Data collection must involve all relevant personnel and departments for accuracy.

3. Analysis and Documentation

Criticality Ranking
- **Action:** Verify that all critical business functions are ranked based on their criticality and potential impact on the organization.
- **Reference: Appendix A, Section III(A)(1)** – Rank critical systems based on their importance to safeguarding member data and continuing operations.

Impact Analysis
- **Action:** Ensure that the analysis of potential impacts on each critical function is comprehensive, including both short-term and long-term impacts.
- **Reference: Appendix A, Section III(B)(2)** – The BIA must cover short-term and long-term risks and their impacts on business operations.

Documented Assumptions
- **Action:** Confirm that all assumptions made during the analysis are documented and justified.
- **Reference: Appendix A, Section III(B)(2)** – All assumptions should be transparent and justified to ensure accuracy in the BIA.

Scenario Analysis
- **Action:** Check that different disruption scenarios (e.g., natural disasters, cyber-attacks, supply chain disruptions) are considered and their impacts analyzed.
- **Reference: Appendix A, Section III(A)(1)** – Requires consideration of various threat scenarios to test recovery plans.

Risk Assessment Integration
- **Action:** Ensure that the BIA findings are integrated with the organization's risk assessment to identify high-risk areas.
- **Reference: Appendix A, Section III(B)(2)** – Requires the integration of BIA findings into the overall risk management process.

Validation of Findings
- **Action:** Verify that BIA findings are validated by key stakeholders, including the accuracy of data and assumptions.
- **Reference: Appendix A, Section III(B)(2)** – Validation of findings ensures that the BIA is accurate and reflective of real business risks.

Documentation of Results
- **Action:** Confirm that the results of the BIA are documented in a formal report, including an executive summary, detailed analysis, and recommendations.
- **Reference: Appendix A, Section III(C)(1)** – Requires documentation of business continuity strategies and risk mitigation measures.

4. Reporting and Review

Management Review
- **Action:** Ensure that the BIA report is reviewed and approved by senior management or the board of directors.
- **Reference: Appendix A, Section III(C)(2)(b)** – Requires senior management and the Board to oversee and approve BIA findings.

Actionable Recommendations
- **Action:** Verify that the BIA report includes actionable recommendations for mitigating identified risks and improving business continuity.
- **Reference: Appendix A, Section III(B)(2)** – Requires that the BIA provide recommendations for risk mitigation.

Presentation of Findings
- **Action:** Check that the BIA findings are presented to all relevant stakeholders, including department heads, for awareness and feedback.
- **Reference: Appendix A, Section III(C)(1)(a)** – Stakeholders must be informed of findings and contribute to business continuity efforts.

Distribution of the BIA Report
- **Action:** Ensure that the BIA report is distributed to all relevant stakeholders, including those responsible for business continuity and disaster recovery planning.
- **Reference: Appendix A, Section III(B)(3)** – Requires communication of risk assessment results to all relevant personnel.

Feedback and Updates
- **Action:** Confirm that feedback is collected from stakeholders and that any necessary updates to the BIA are made.
- **Reference: Appendix A, Section III(B)(2)** – Requires continuous feedback and updates to maintain the accuracy of the BIA.

Periodic Review
- **Action:** Verify that a schedule for periodic review and update of the BIA is in place, typically annually or whenever there are significant changes in the business.
- **Reference: Appendix A, Section III(B)(2)** – Requires regular updates to the BIA to reflect changes in business operations or risk.

5. Integration with Business Continuity Planning

Alignment with Business Continuity Plan (BCP)
- **Action:** Ensure that the BIA findings are integrated into the organization's BCP, including prioritization of recovery efforts based on BIA results.
- **Reference: Appendix A, Section III(A)(1)** – Requires alignment between BIA findings and the continuity plan to ensure effective recovery efforts.

Continuity Strategies
- **Action:** Verify that continuity strategies (e.g., redundant systems, alternative suppliers) are aligned with the critical functions identified in the BIA.
- **Reference: Appendix A, Section III(B)(1)** – Ensure that strategies reflect the priorities and risks identified in the BIA.

Resource Allocation
- **Action:** Check that resources are allocated based on the criticality of functions identified in the BIA.
- **Reference: Appendix A, Section III(B)(2)** – Resource allocation must reflect the criticality of systems and processes.

Training and Awareness
- **Action:** Ensure that the results of the BIA are communicated to all relevant employees and that training is provided to ensure understanding of critical functions and recovery priorities.
- **Reference: Appendix A, Section III(C)(1)(b)** – Requires training and awareness programs for staff involved in business continuity.

Testing and Exercises
- **Action:** Verify that the BIA informs the development of testing and exercise scenarios for the business continuity plan.
- **Reference: Appendix A, Section III(B)(3)** – Requires regular testing of the business continuity plan, informed by the BIA.

6. Compliance and Governance

Regulatory Compliance
- **Action:** Ensure that the BIA complies with relevant regulatory requirements and industry standards (e.g., ISO 22301, NIST SP 800-34).
- **Reference: Appendix A, Section III(B)(2)** – Requires compliance with regulations and standards related to business continuity.

Audit Trail
- **Action:** Confirm that all steps in the BIA process are documented and that an audit trail is maintained for compliance purposes.
- **Reference: Appendix A, Section III(C)(2)(c)** – Requires documentation of the BIA process for audit purposes.

Continuous Improvement
- **Action:** Verify that there is a process in place for continuous improvement of the BIA, including lessons learned from incidents and changes in the business environment.
- **Reference: Appendix A, Section III(B)(2)** – Requires continuous improvement of the business continuity plan based on new risks and business changes.

This checklist, aligned with **Appendix A to Part 748, Title 12** and **Appendix B to Part 749**, helps ensure that the **Business Impact Analysis (BIA)** is comprehensive, regularly reviewed, and integrated with the organization's overall risk management and business continuity planning.

Frameworks

Friday, August 16, 2024 2:31 PM

1. ISO 22301:2019 - Business Continuity Management Systems (BCMS)

- **Overview**: ISO 22301 is an international standard that specifies the requirements for a management system to protect against, reduce the likelihood of, and ensure your business recovers from disruptive incidents.
- **Key Components**:
  - **Context of the Organization**: Understanding internal and external factors that can impact the business.
  - **Leadership**: Commitment from top management and the establishment of a business continuity policy.
  - **Planning**: Risk assessments, business impact analysis (BIA), and strategy development.
  - **Support**: Resource allocation, competence, awareness, and communication.
  - **Operation**: Implementation of business continuity procedures, emergency response, and incident management.
  - **Performance Evaluation**: Monitoring, measurement, analysis, and evaluation of business continuity performance.
  - **Improvement**: Continuous improvement through corrective actions and audits.
- **Benefits**: Provides a comprehensive and systematic approach to business continuity, is recognized globally, and is certifiable, which can be valuable for regulatory compliance and demonstrating commitment to stakeholders.

2. NIST SP 800-34 Rev. 1 - Contingency Planning Guide for Federal Information Systems

- **Overview**: This framework, developed by the National Institute of Standards and Technology (NIST), provides guidelines for information system contingency planning, particularly for federal information systems but applicable to other sectors.
- **Key Components**:
  - **Contingency Planning Process**: Involves developing a contingency planning policy, conducting a business impact analysis (BIA), identifying preventive controls, creating contingency strategies, developing an information system contingency plan, and ensuring plan testing, training, and exercises.
  - **Plan Development**: Detailed guidance on creating contingency plans for IT systems, including backup and recovery, alternate processing facilities, and continuity of operations.
  - **Testing and Maintenance**: Emphasizes the importance of regular testing, plan maintenance, and continuous improvement.
- **Benefits**: Highly detailed with a focus on IT and information systems, making it ideal for organizations heavily reliant on technology. It also aligns with broader federal standards and practices.

3. COBIT 2019 - Control Objectives for Information and Related Technologies

- **Overview**: COBIT is a framework for the governance and management of enterprise IT. While it's primarily focused on IT governance, it includes extensive guidance on IT continuity and resilience.
- **Key Components**:
  - **Governance and Management Objectives**: Specific objectives related to business continuity include ensuring that IT services can be restored in a timely manner after a disruption.
  - **Risk Management**: Emphasizes the identification and management of risks related to IT operations and continuity.
  - **Performance Measurement**: Guidance on measuring the effectiveness of business continuity strategies and processes.
- **Benefits**: COBIT is well-suited for organizations where IT is a critical component of business operations. It integrates IT governance with overall business continuity planning.

4. FFIEC Business Continuity Management (BCM) Handbook

- **Overview**: Developed by the Federal Financial Institutions Examination Council (FFIEC), this framework provides comprehensive guidance for financial institutions on maintaining resilience and continuity of operations.
- **Key Components**:
  - **Governance and Oversight**: Emphasizes the role of the board of directors and senior management in BCM.
  - **Risk Management**: Detailed processes for risk identification, assessment, and mitigation specific to the financial industry.
  - **Continuity Strategies**: Development of recovery strategies, including IT disaster recovery, data backup, and alternate facilities.
  - **Communication Plans**: Guidelines for internal and external communication during a disruption.
- **Benefits**: Tailored for financial institutions, it provides industry-specific guidance and is often referenced by regulatory bodies during audits.

5. DRII Professional Practices for Business Continuity Management

- **Overview**: The Disaster Recovery Institute International (DRII) offers a set of professional practices that are widely recognized in the business continuity field.
- **Key Components**:
  - **Program Initiation and Management**: Establishing and managing the business continuity program.
  - **Risk Evaluation and Control**: Identifying risks and implementing controls to mitigate them.
  - **Business Impact Analysis**: Conducting a BIA to identify critical processes and the impact of their disruption.
  - **Recovery Strategy**: Developing and selecting recovery strategies based on the BIA.
  - **Plan Development and Implementation**: Documenting continuity and recovery plans.
  - **Awareness and Training**: Ensuring that all stakeholders are aware of the BCP and trained in their roles.
  - **Testing and Maintenance**: Regular testing, updating, and improving the BCP.
- **Benefits**: Comprehensive and widely recognized in the industry. It serves as a benchmark for business continuity professionals and aligns with best practices across various industries.

6. ITIL 4 - Information Technology Infrastructure Library

- **Overview**: ITIL is a set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of the business. ITIL 4 includes guidance on service continuity management.
- **Key Components**:
  - **Service Continuity Management**: Ensures that IT services can be restored after a disruption within agreed timelines.
  - **Incident Management**: Processes for managing and resolving incidents quickly to minimize impact.
  - **Problem Management**: Identifying and resolving the root causes of incidents to prevent recurrence.
  - **Risk Management**: Identifying, assessing, and mitigating risks to IT services.
- **Benefits**: ITIL is particularly valuable for organizations where IT services are critical to business operations. It integrates service management with continuity planning, providing a holistic approach.

7. BS 25999-2:2007 (Replaced by ISO 22301)

- **Overview**: BS 25999 was the British standard for business continuity management, which has since been replaced by ISO 22301. However, it laid the groundwork for many of the practices now codified in ISO 22301.
- **Key Components**: Much of BS 25999's structure is reflected in ISO 22301, including risk assessment, business impact analysis, continuity strategies, and plan development.
- **Benefits**: While it has been replaced by ISO 22301, BS 25999 influenced modern BCM practices and can still provide useful insights for organizations familiar with it.

8. NFPA 1600 - Standard on Continuity, Emergency, and Crisis Management

- **Overview**: The National Fire Protection Association (NFPA) 1600 standard provides a framework for continuity, emergency, and crisis management, widely used in the U.S.
- **Key Components**:
  - **Program Management**: Establishing a comprehensive continuity and emergency management program.
  - **Risk Assessment and Business Impact Analysis**: Identifying hazards and assessing the impact of disruptions.
  - **Incident Management**: Coordinating response efforts during an incident.
  - **Recovery and Restoration**: Ensuring the timely recovery of operations and services.
  - **Training and Education**: Providing training to employees on their roles in continuity and emergency response.
  - **Public and Private Sector Coordination**: Integrating continuity efforts with local and national public sector agencies.
- **Benefits**: NFPA 1600 is recognized by U.S. federal agencies and widely adopted by organizations of all sizes for its comprehensive approach to continuity and emergency management.

Resources

Friday, August 16, 2024 2:35 PM

https://hazards.fema.gov/nri/

System Backups	Organizations reduce the likelihood and duration of data loss at loss of service delivery or operations.	Data Destruction (T1485, ICS T0809) Data Encrypted for Impact (T1486) Disk Wipe (T1561) Inhibit System Recovery (T1490) Denial of Control (ICS T0813) Denial/Loss of View (ICS T0815, T0829) Loss of Availability (T0826) Loss/Manipulation of Control (T0828, T0831)	IT and OT assets necessary for business operations	All systems that are necessary for operations are regularly backed up on a regular cadence (no less than once per year). Backups are stored separately from the source systems and tested on a recurring basis, no less than once per year. Stored information for OT assets includes at a minimum: configurations, roles, programmable controller (PLC) logic, engineering drawings, and tools.

Strong	Satisfactory	Less Than Satisfactory	Deficient	Critically Deficient
☐ Business continuity testing program is able to demonstrate ability to meet continuity objectives; ☐ Regular testing of varying scenarios; ☐ Testing of critical business lines; ☐ Testing of internal interdependencies between business units and processes; ☐ Documentation of the continuity testing program, including; ☐ analysis of test results and resolution of any identified issues; ☐ Testing with critical third-party service providers; ☐ Use of offsite resources to conduct the recovery test; ☐ Testing the adequacy of remote access infrastructure and capacity.	☐ Business continuity testing program is able to demonstrate ability to meet continuity objectives; ☐ Regular testing of varying scenarios; ☐ Testing of critical business lines; ☐ Testing of internal interdependencies between business units and processes; ☐ Documentation of the continuity testing program, including; ☐ Analysis of test results and resolution of any identified issues; ☐ Testing with critical third-party service providers; ☐ No use of offsite resources to conduct the recovery test; ☐ Not consistently testing the adequacy of remote access infrastructure and capacity.	☐ Business continuity testing program is able to demonstrate ability to meet continuity objectives; ☐ Regular testing of varying scenarios; ☐ No testing of critical business lines; ☐ No testing of internal interdependencies between business units and processes; ☐ No documentation of the continuity testing program, including; ☐ No analysis of test results and resolution of any identified issues; ☐ No testing with critical third-party service providers; ☐ No use of offsite resources to conduct the recovery test; ☐ No testing the adequacy of remote access infrastructure and capacity.	☐ Business continuity testing program is unable to demonstrate ability to meet continuity objectives; ☐ No regular testing of varying scenarios; ☐ No testing of critical business lines; ☐ No testing of internal interdependencies between business units and processes; ☐ No documentation of the continuity testing program, including; ☐ No analysis of test results and resolution of any identified issues; ☐ No testing with critical third-party service providers; ☐ No use of offsite resources to conduct the recovery test; ☐ No testing the adequacy of remote access infrastructure and capacity.	☐ No business continuity testing program in place.

Strong	Satisfactory	Less Than Satisfactory	Deficient	Critically Deficient
☐ The plans include enterprise-wide business continuity plan, business impact analysis, risk/threat assessment, including cyber risks/threats; ☐ The plan includes a testing program and results; ☐ Plans are Board and senior management approved annually. ☐ Addresses pandemic issues.	☐ The plans include enterprise-wide business continuity plan, business impact analysis, risk/threat assessment, including cyber risks/threats; ☐ The plan includes a testing program and results; ☐ Plans are Board and senior management approved annually. ☐ Does not address pandemic issues	☐ The plans include enterprise-wide business continuity plan, business impact analysis, risk/threat assessment, including cyber risks/threats ☐ The plans do not include a testing program and results; ☐ Plans are not Board and senior management approved annually; ☐ Does not address pandemic issues	☐ The plans do not include enterprise-wide business continuity plan, business impact analysis, risk/threat assessment, including cyber risks/threats ☐ The plans do not include a testing program and results; ☐ Plans are not Board and senior management approved; ☐ Does not address pandemic issues	☐ There are no corporate contingency planning and business resumption plans, programs, and assessments.

Strong	Satisfactory	Less Than Satisfactory	Deficient	Critically Deficient
☐ Business impact analyses and risk assessments have been completed; ☐ Analysis of reasonably foreseeable threats; ☐ Identifies critical business assets and prioritize recovery; ☐ Includes input from all business units; ☐ Include recovery time objectives (RTOs), recovery point objectives (RPOs); ☐ Include IT services provided by third-party vendors;	☐ Business impact analyses and risk assessments have been completed; ☐ Analysis of reasonably foreseeable threats; ☐ Identifies critical business assets and prioritize recovery; ☐ Includes input from all business units; ☐ Include recovery time objectives (RTOs), recovery point objectives (RPOs); ☐ Does not include IT services provided by third-party vendors;	☐ Business impact analyses and risk assessments have been completed; ☐ analysis of reasonably foreseeable threats; ☐ Identifies critical business assets and prioritize recovery; ☐ Does not include input from all business units; ☐ Does not include recovery time objectives (RTOs), recovery point objectives (RPOs); ☐ Does not include IT services provided by third-party vendors;	☐ Business impact analyses and risk assessments have been completed; ☐ analysis of reasonably foreseeable threats; ☐ Does not identify critical business assets or prioritize recovery; ☐ Does not include input from all business units; ☐ Does not include recovery time objectives (RTOs), recovery point objectives (RPOs); ☐ Does not include IT services provided by third-party vendors;	☐ Business impact analyses and risk assessments have not been completed.

veeam_backup_11_0...

sp800-34-rev1_bia_template

Quantivate

Thursday, September 19, 2024 2:49 PM

To ensure compliance with **Appendix A to Part 748, Title 12** and **Appendix B to Part 749**, you will need to review specific components of your **Quantivate** Business Continuity Planning (BCP) platform. Below is a guide on what to review and ensure within **Quantivate** to maintain compliance:

1. Risk Assessment and Management

What to Review:

- **Risk Assessment Documentation:** Ensure that Quantivate captures documented risk assessments, including risks related to the security and confidentiality of member information.
- **Vulnerability Identification:** Verify that vulnerabilities are regularly assessed and that results are documented in the system.
- **Integration of BIA:** Ensure the Business Impact Analysis (BIA) in Quantivate is integrated into your risk assessment process to identify critical systems and functions that involve member data.
- **Risk Mitigation Measures:** Review Quantivate to confirm that mitigation measures for identified risks are tracked and updated.
- **Compliance Reference:**
  - **Appendix A to Part 748, Section III(A)(1)** – Risk assessments must be conducted to identify internal and external threats to member information.
  - **Appendix A to Part 748, Section III(A)(5)** – Mitigation steps should be taken based on identified risks.

2. Business Impact Analysis (BIA)

What to Review:

- **Critical Functions Identification:** Review the BIA section in Quantivate to ensure all critical systems, processes, and dependencies are identified and documented.
- **Impact Assessment:** Ensure that the potential impact of disruptions is assessed for each critical function, including financial, operational, and reputational impacts.
- **Recovery Time Objectives (RTOs) and Recovery Point Objectives (RPOs):** Check if Quantivate documents RTOs and RPOs for each critical system.
- **Update Frequency:** Confirm that the BIA is regularly reviewed and updated in Quantivate, at least annually or when significant changes occur in business processes.
- **Compliance Reference:**
  - **Appendix A to Part 748, Section III(B)(2)** – BIA must include assessment of the potential impacts of disruptions and prioritize systems according to criticality.
  - **Appendix B to Part 749** – BIA should ensure the timely recovery of critical records and functions.

3. Backup and Recovery Plans

What to Review:

- **Backup Documentation:** Ensure Quantivate contains comprehensive backup and recovery plans for all critical systems, with clear documentation of offsite storage and data integrity verification.
- **Offsite Backup Procedures:** Confirm that backup locations are securely documented and geographically separated from the primary site.
- **Testing of Backup and Recovery:** Review the results of any backup and recovery tests conducted through Quantivate to ensure that these are regularly scheduled and documented.
- **Data Integrity Verification:** Ensure there is a documented process in Quantivate for verifying the integrity of backups through testing.
- **Compliance Reference:**
  - **Appendix A to Part 748, Section III(A)(3)** – Requires safeguarding member information, including through secure offsite backups.
  - **Appendix B to Part 749** – Ensures that records can be restored in the event of an incident.

4. Business Continuity and Disaster Recovery (BC/DR) Plans

What to Review:

- **BCP Documentation:** Review Quantivate's documentation for the business continuity and disaster recovery plans to ensure that all critical systems, processes, and services are covered.
- **Plan Testing and Updates:** Check the test results of the BC/DR plans and ensure they are regularly reviewed, tested, and updated as needed.
- **Contingency Planning:** Confirm that contingency plans for member data and critical functions are documented and have been tested under various scenarios (e.g., cyberattacks, natural disasters).
- **Board Reporting:** Ensure that Quantivate includes a process for reporting the status of the business continuity program to the Board, along with key metrics and test results.
- **Compliance Reference:**
  - **Appendix A to Part 748, Section III(B)(1)** – Requires the implementation of an effective business continuity program to safeguard critical functions.
  - **Appendix A to Part 748, Section III(C)(2)(b)** – Board reporting and oversight are essential components of the business continuity program.

5. Employee Training and Awareness

What to Review:

- **Training Records:** Review employee training records in Quantivate to ensure that all employees are regularly trained on business continuity, disaster recovery, and security protocols related to safeguarding member information.
- **Training Content:** Ensure that the training materials in Quantivate cover key topics such as incident response, cyber threats, and compliance with regulatory requirements.
- **Test Results and Competency:** Check the results of employee training assessments to ensure staff competency in handling incidents and understanding their roles in business continuity.
- **Board and Executive Training:** Ensure that board members and senior executives are trained on their oversight responsibilities regarding the business continuity program.
- **Compliance Reference:**
  - **Appendix A to Part 748, Section III(C)(1)(b)** – Requires regular training and awareness programs for all staff, especially those responsible for managing critical systems.
  - **Appendix A to Part 748, Section III(C)(2)(b)** – Requires regular updates to the Board on the effectiveness of the information security and business continuity programs.

6. Incident Response Plans

What to Review:

- **Incident Response Plan Documentation:** Ensure that Quantivate contains a fully documented incident response plan (IRP) that includes procedures for detecting, mitigating, and recovering from incidents involving member information.
- **Incident Tracking:** Check Quantivate's tracking of incidents to ensure that any security breaches or disruptions involving member information are logged, investigated, and addressed.
- **Response Time and Effectiveness:** Review the timeliness and effectiveness of response efforts logged in Quantivate, including the resolution of incidents and lessons learned.
- **Regulatory Notifications:** Confirm that Quantivate tracks and documents any required notifications to regulators in the event of significant security incidents.
- **Compliance Reference:**
  - **Appendix A to Part 748, Section III(A)(2)** – Requires the establishment of an incident response plan to manage incidents related to unauthorized access to member information.
  - **Appendix A to Part 748, Section III(C)(1)(d)** – Requires timely notification of security incidents involving member information.

7. Vendor Management

What to Review:

- **Vendor Risk Assessments:** Ensure that Quantivate tracks risk assessments for third-party vendors that have access to member information or critical systems.
- **Vendor Continuity Plans:** Review whether Quantivate contains vendor-provided continuity and disaster recovery plans, and confirm their integration into your organization's business continuity strategy.
- **Contractual Agreements:** Ensure that contracts with vendors include provisions for business continuity, incident reporting, and safeguarding member information.
- **Vendor Testing and Participation:** Check Quantivate for documentation of vendor participation in business continuity tests and exercises.
- **Compliance Reference:**
  - **Appendix A to Part 748, Section III(C)(1)(c)** – Requires institutions to ensure third-party vendors implement safeguards for member information.
  - **Appendix B to Part 749** – Requires that vendor contracts ensure the continued protection and recovery of critical systems and data.

8. Documentation, Testing, and Audit Trails

What to Review:

- **Documentation of All Policies and Procedures:** Ensure that Quantivate houses up-to-date documentation of all business continuity and disaster recovery policies, procedures, and plans.
- **Test Results and Audit Trails:** Verify that Quantivate maintains audit trails for all business continuity tests, updates, and improvements, and that these records are accessible for review.
- **Compliance Reporting:** Review Quantivate's reports on compliance with **Appendix A to Part 748** and **Appendix B to Part 749** to ensure the organization meets regulatory requirements.
- **Continuous Improvement:** Check whether Quantivate is being used to track and document improvements made to the business continuity program based on test results, incidents, and audits.
- **Compliance Reference:**
  - **Appendix A to Part 748, Section III(C)(2)(c)** – Requires the documentation and auditability of business continuity plans, tests, and corrective actions.
  - **Appendix A to Part 748, Section III(B)(3)** – Requires ongoing testing and improvement of the business continuity program.

By reviewing these components within **Quantivate**, your organization can ensure that its **Business Continuity Program** (BCP) is compliant with **Appendix A to Part 748, Title 12**, and **Appendix B to Part 749**, helping safeguard member information and ensure resilience in the event of a disruption.

Examiner Findings

Friday, December 13, 2024 3:57 PM

Findings:

1. **Last BCP Test More Than 12 Months Ago**
   - **Issue**: The absence of regular testing violates **Stmt 10.3** (Testing and Training of Contingency Plans). Regular testing ensures the effectiveness of contingency plans.
   - **Action**: Conduct a BCP test immediately and create a documented schedule for testing at least annually.
2. **Backup Procedures Not in the BCP**
   - **Issue**: Non-compliance with **Stmt 10.1** (Backup and Recovery Plans). Backup procedures are critical and must be documented within the BCP.
   - **Action**: Update the BCP to include detailed backup procedures for critical systems.
3. **No Backup Generator or Long-Term Alternate Power Source**
   - **Issue**: Dependency on UPS devices for short-term power exposes the organization to risks during prolonged outages, impacting **Stmt 10.6** (Network Equipment and Communication Needs).
   - **Action**: Evaluate the feasibility of installing a backup generator or ensuring access to a long-term power source.
4. **Undocumented Backup Program**
   - **Issue**: Discrepancy between actual practices and documented procedures violates **Stmt 10.1** (Document Backup and Recovery Plans).
   - **Action**: Align documentation with the implemented backup program and include periodic reviews for accuracy.
5. **Small-Scale VPN Test; Full Failover Scheduled**
   - **Issue**: While small-scale testing aligns with **Stmt 10.3**, the lack of a recent full failover test indicates incomplete compliance with **Stmt 10.5** (Redundant and Separated Data Centers).
   - **Action**: Proceed with the full failover test in October 2024 and document results.
6. **No Physical Media for Backups**
   - **Observation**: Compliance with **Stmt 10.1** is still achieved since Cohesity ensures secure and encrypted backups, reducing dependency on physical media.
7. **Cohesity Backup Encryption Verified**
   - **Observation**: Strong compliance with **Stmt 10.1** and **Stmt 10.5**, demonstrating that backups are safeguarded against unauthorized access.
8. **Quarterly Backup Testing Conducted**
   - **Observation**: Aligns well with **Stmt 10.1** (Test Data Integrity). Regular testing of backups enhances reliability.
9. **Primary and Backup Data Centers 292 Miles Apart**
   - **Observation**: Geographic separation supports compliance with **Stmt 10.5** (Ensure Geographic Separation).
10. **Simultaneous Patching of Primary and Backup Data Centers**
    - **Issue**: Concurrent patching creates a risk of simultaneous vulnerabilities, conflicting with **Stmt 10.5** (Synchronize Data Between Centers).
    - **Action**: Implement staggered patching schedules to ensure continuous availability.
11. **No Exercises Involving Core and Significant Vendors**
    - **Issue**: Non-compliance with **Stmt 10.6** (Test Vendor Communication).
    - **Action**: Plan and conduct tabletop exercises or simulations with key vendors to validate vendor communication and coordination.

Recommendations and Priorities:

1. **Immediate Actions:**
   - Update the BCP to document backup procedures.
   - Schedule and conduct a full BCP test to meet compliance with **Stmt 10.3**.
2. **Short-Term Actions (Next 3-6 Months):**
   - Address gaps in vendor interaction exercises as outlined in **Stmt 10.6**.
   - Review and align the backup program documentation with operational practices.
3. **Long-Term Improvements (Within 12 Months):**
   - Consider long-term alternate power solutions to reduce reliance on UPS-only systems.
   - Conduct failover tests and stagger patching schedules for data centers.
4. **Ongoing Compliance:**
   - Maintain quarterly backup testing and documentation.
   - Ensure the BIA and BCP are updated and approved by senior management as required by **Stmt 10.2** and **Stmt 10.4**.

1. Situation (S)

The evaluation occurred during a compliance review of the credit union's Disaster Recovery and Business Continuity Program (DR/BCP) in alignment with Appendix A to Part 748, Title 12, and Appendix B to Part 749. The review focused on backup and recovery plans, testing schedules, data center redundancy, power solutions, vendor interaction, and other aspects critical to ensuring business continuity and safeguarding member information.

2. Behavior (B)

Several specific observations were noted during the review:

1. **Testing and Backup Documentation**:
   - The last BCP test was conducted over 12 months ago.
   - Backup procedures were not included in the documented BCP.
   - A small-scale VPN test was conducted; a full failover test is pending.
2. **Power and Redundancy**:
   - No long-term alternate power source is installed; reliance on UPS devices only.
   - Primary and backup data centers are 292 miles apart, but patching is conducted simultaneously.
3. **Vendor Interaction**:
   - No exercises or tests involving coordination with core and significant vendors were conducted.
4. **Backup and Recovery Practices**:
   - Backups are performed regularly using Cohesity, which encrypts data, and backup testing occurs quarterly.
   - Backup documentation does not match the program in practice.

3. Impact (I)

The observed behaviors led to the following consequences:

1. **Testing and Documentation**:
   - Insufficient testing frequency and missing backup procedures in the BCP reduce preparedness for real-world disruptions.
   - Pending failover testing delays assurance of data center functionality in a disaster.
2. **Power and Redundancy**:
   - Reliance on short-term UPS power creates vulnerabilities during extended outages, potentially leading to service disruption.
   - Simultaneous patching increases the risk of concurrent vulnerabilities or outages in both primary and backup centers.
3. **Vendor Interaction**:
   - Lack of vendor engagement in DR/BCP exercises hinders the ability to assess and coordinate effective recovery processes with third parties during an incident.
4. **Backup and Recovery Practices**:
   - Misaligned documentation may lead to compliance gaps and confusion during audits or actual recovery events.

4. Resolution (R)

To address the identified gaps and improve compliance with Appendix A and B of 12 CFR Part 748 and Part 749, the following actionable steps are proposed:

1. **Testing and Backup Documentation**:
   - Schedule and conduct a full-scale BCP test as soon as possible and ensure tests occur annually at a minimum.
   - Update the BCP to include comprehensive backup procedures and align documentation with actual backup practices.
2. **Power and Redundancy**:
   - Evaluate and implement long-term alternate power solutions, such as a backup generator, to mitigate reliance on UPS devices.
   - Implement staggered patching schedules to avoid simultaneous vulnerabilities in primary and backup data centers.
3. **Vendor Interaction**:
   - Plan and conduct regular exercises with core and significant vendors, including tabletop and live recovery simulations, to validate coordination during incidents.
4. **Backup and Recovery Practices**:
   - Regularly review and update the documented backup program to ensure alignment with operational practices.
   - Continue quarterly backup testing and document results for audit purposes.

Notes

Tuesday, September 3, 2024 7:05 AM

Verified that the business continuity program (BCP) demonstrated robust compliance with regulatory requirements and the credit union is adequately prepared to manage disruptions and safeguard member information. Reviewed backup and recovery plans, verified backup frequency against recovery time objectives (RTOs) and recovery point objectives (RPOs), and confirmed that backups were securely stored, immutable and segregated from the internet. Reviewed the Business Impact Analysis (BIA), including documentation of critical business functions, interdependencies, and financial impact assessments for various disaster scenarios. Verified that the BIA had been updated following significant business or IT changes and had received senior management approval. Reviewed the establishment and documentation of training programs for employees with disaster recovery roles, adherence to a testing schedule for contingency plans, and the effectiveness of various tests, such as tabletop exercises and full-scale simulations. Test results were reviewed to ensure they were documented and used to improve recovery strategies. Verified that a formal reporting process to the Board was in place, including reports with key metrics, test outcomes, and updates to business continuity plans. Reviewed board meeting minutes to confirm discussions on these reports and demonstrate oversight of the program.