

8 Business Continuity Categories Your Credit Union Should Be Reviewing Annually

Timothy Daugherty CBCP CCP



For credit unions, an effective Business Continuity Management (BCM) Program is more than a regulatory expectation – it is a strategic capability that protects member trust, operational integrity and organizational resilience. Each year, your BCM program should undergo a structured cycle of activities that ensure it remains current, actionable and aligned with evolving risks. With increasing cyber

events, third party dependencies and member service expectations, annual BCM tasks must be intentional, repeatable and outcome driven.

1. Refresh the Business Impact Analysis (BIA)

The BIA remains the foundation of continuity planning. Each year, credit unions should:

- Validate critical processes, RTOs/RPOs and peak transaction periods.
- Update system dependencies, staffing levels and vendor reliance.
- Confirm impacts of outages across digital banking, payments, lending and member channels.

This annual refresh helps ensure that your recovery strategies reflect current operations, technology changes and member experience expectations.

2. Conduct a Comprehensive Threat & Risk Assessment

From hurricanes to ransomware, the threat landscape for credit unions is expanding. Annually:

- Reevaluate natural hazards, cyber threats, fraud trends and operational risks.
- Assess third party vulnerabilities and concentration risks.
- Consider real world events and disruptions faced by peer institutions.

This assessment drives more accurate planning and strengthens your operational resiliency posture.

3. Review and Update Continuity, Crisis Management and Emergency Response Plans

Plans should never sit on a shelf. At least annually:

- Update departmental continuity procedures and team assignments.
- Validate contact lists, vendor communication protocols and escalation paths.
- Review crisis leadership frameworks to ensure clarity in roles, authority and decision-making.

Regulators expect governance structures that can be activated quickly and confidently during disruptions.

4. Execute Annual Testing and Exercises

Testing is where credit unions truly learn how they respond under pressure. Each year:

- Conduct at least one tabletop exercise – ideally covering cyber disruption, vendor outages or facility inaccessibility.
- Validate remote work capabilities and alternate site preparedness.
- Perform functional tests for critical systems (e.g., core banking, digital banking, telephony).

Exercises should evaluate not just recovery, but communication, decision-making and member experience impacts.

5. Evaluate Vendor Continuity and Resilience

Vendor dependency is a top supervisory concern. Annually:

- Collect and review vendor SOC reports, continuity attestations and cyber documentation.
- Validate vendor recovery time commitments against your member service requirements.
- Ensure contingency plans exist for high risk third parties, including payment processors, digital providers and cloud platforms.

A failure in your vendor ecosystem is still a failure in your member service.

6. Update Training and Awareness

People are the backbone of continuity. Each year:

- Provide refresher training for crisis teams and departmental recovery owners.
- Conduct staff-wide awareness on emergency procedures, communication channels and response expectations.
- Onboard new employees with continuity basics.

A trained workforce responds faster and reduces organizational confusion during disruptions.

7. Perform Governance Reviews and Report to Leadership

Strong governance is central to modern resiliency frameworks. Annually:

- Deliver a Board level BCM program report summarizing risks, testing results, maturity and improvement plans.
- Review BCM policies for alignment with NCUA and FFIEC expectations.
- Conduct an internal or external audit to verify compliance and program effectiveness.

Transparent governance strengthens trust across leadership, regulators and members.

8. Conduct a Post Year Program Assessment

To close the BCM cycle:

- Document lessons learned from incidents, exercises and operational challenges.
- Update risk scores, improvement tasks and resiliency metrics.
- Define next year's roadmap based on maturity goals and organizational priorities.

This promotes continuous improvement – a key expectation under operational resilience frameworks.

Final Takeaway

A strong annual BCM program is not just a compliance requirement, it is a strategic investment in member trust, reputation and operational stability. By completing these core annual tasks, your credit union strengthens its ability to withstand disruption, protect members and maintain confidence in every situation.