Contingency Planning

- Information systems are vulnerable to a variety of disruptions, ranging from mild to severe
Contingency Planning

Vulnerability
may be minimized or eliminated through management, operational, or technical controls; however, it is virtually impossible to completely eliminate all risk.
Contingency planning is designed to mitigate the risk of system and service unavailability by providing effective and efficient solutions to enhance system availability.
Types of Plans

- **Information system contingency planning** represents a broad scope of activities designed to sustain and recover critical system services following an emergency event.

- An organization would use a **suite of plans** to properly prepare response, recovery, and continuity activities for disruptions affecting the organization.

- Because there is an **inherent relationship** between an information system and the mission/business process it supports, there must be **coordination** between each plan to ensure that recovery strategies and supporting resources neither negate each other nor duplicate efforts.
Business Continuity Plan (BCP) focuses on sustaining an organization’s mission/business processes during and after a disruption.

- BCP may be written for mission/business processes within a single business unit or may address the entire organization’s processes.

- BCP may be used for long-term recovery in conjunction with the COOP plan, allowing for additional functions to come online as resources or time allow.
Continuity of Operations Plan (COOP) focuses on restoring an organization’s mission essential functions at an alternate site and performing those functions for up to 30 days before returning to normal operations.

- Additional functions, or those at a field office level, may be addressed by a BCP.
- Minor threats or disruptions that do not require relocation to an alternate site are typically not addressed in a COOP plan.
Continuity of Operations Plan

Standard elements of a COOP plan:

- Program plans and procedures
- Risk Management
- Budgeting and acquisition of resources
- Essential functions

- Order of succession
- Delegation of authority
- Continuity facilities
- Continuity communications
- Vital records management

- Human capital
- Test, training, and exercise
- Devolution
- Reconstitution
Organizations should document standard procedures for internal and external communications in the event of a disruption using a **Crisis Communications Plan**.

- Often developed by the organization responsible for public outreach.
- Plan provides various formats for communications appropriate to the incident.
- Typically designates specific individuals as the *only* authority for answering questions from or providing information to the public regarding emergency response.
- May also include procedures for disseminating reports to personnel on the status of the incident and templates for public press release.
- Crisis communication plan procedures should be communicated to ensure that the plans include clear direction and that only approved statements are released to the public by authorized officials.
Critical Infrastructure Protection Plan

- Critical infrastructure and key resources (CIKR) are those components of the national infrastructure deemed so vital that their loss would have a debilitating effect of the safety, security, economy, and health of the United States.

- A Critical Infrastructure Protection (CIP) Plan is a set of policies and procedures that serve to protect and recover these national assets and mitigate risks and vulnerabilities.

- CIP Plan should define the roles and responsibilities for protection, develop partnerships and information sharing relationships, implement the risk management framework defined for CIKR assets, and integrate federal, state and local emergency preparedness, protection, and resiliency of critical infrastructure.
A **Cyber Incident Response Plan** establishes procedures to address cyber attacks against an organization’s information systems.

These procedures are designed to enable security personnel to identify, mitigate, and recover from malicious computer incidents:
- Unauthorized access to a system or data
- Denial of Service
- Unauthorized changes to system hardware, software or data (virus, worm, Trojan horse)

This plan may be included as an appendix of the BCP.
The **Disaster Recovery Plan (DRP)** applies to major, usually physical disruptions to service that deny access to the primary facility infrastructure for an extended period.

- Is an information system-focused plan designed to restore operability of the target system, application, or computer facility infrastructure at an alternate site after an emergency.

- May be supported by multiple information system contingency plans to address recovery of impacted individual systems once the alternate facility has been established.

- A DRP may support a BCP or COOP plan by recovering supporting systems for business processes or mission essential functions at an alternate location.

- Only addresses information system disruptions that require relocation.
Information System Contingency Plan

- An Information System Contingency Plan (ISCP) provides established procedures for the assessment and recovery of a system following a system disruption.

- Provides key information needed for system recovery, including:
  - Roles and responsibilities
  - Inventory information
  - Assessment procedures
  - Detailed recovery procedures
  - Testing of a system
Information System Contingency Plan

- ISCP differs from a DRP primarily in that the ISCP procedures are developed for recovery of the system regardless of site or location.

- An ISCP can be activated at the system’s current location or at an alternate site.

- In contrast, a DRP is primarily a site-specific plan developed with procedures to move operations of one or more information systems from a damaged or uninhabitable location to a temporary alternate location.

- Once the DRP has successfully transferred an information system site to an alternate site, each affected system would then use its respective ISCP to restore, recover, and test systems, and put them into operation.
The **Occupant Emergency Plan (OEP)** outlines first-response procedures for occupants of a facility in the event of a threat or incident to the health and safety of personnel, the environment, or property.

- Fire
- Bomb threat
- Chemical release
- Domestic violence in the workplace
- Medical emergency

Shelter-in-place procedures for events requiring personnel to stay inside the building rather than evacuate are also addressed in OEP.

OEPs are developed at the facility level, specific to the geographic location and structural design of the building.

The facility OEP may be appended to the COOP or BCP, but is executed separately and as a first response to the incident.
## Summary of Types of Plans

<table>
<thead>
<tr>
<th>Plan</th>
<th>Purpose</th>
<th>Scope</th>
<th>Plan Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Business Continuity Plan (BCP)</td>
<td>Provides procedures for sustaining mission/business operations while recovering from a significant disruption</td>
<td>Addresses mission/business processes at a lower or expanded level from COOP MEFs</td>
<td>Mission/business process focused plan that may be activated in coordination with a COOP plan to sustain non-MEFs</td>
</tr>
<tr>
<td>Continuity of Operation (COOP) Plan</td>
<td>Provides procedures and guidance to sustain an organization's MEFs at an alternate site for up to 30 days; mandated by federal directives</td>
<td>Addresses MEFs at a facility; information systems are addressed based only on their support of the mission essential functions</td>
<td>MEF focused plan that may also activate several business unit-level BCPs, ISCPs, or DRPs, as appropriate</td>
</tr>
<tr>
<td>Crisis Communications Plan</td>
<td>Provides procedures for disseminating internal and external communications; means to provide critical status information and control rumors</td>
<td>Addresses communications with personnel and the public; not information system-focused</td>
<td>Incident-based plan often activated with a COOP or BCP, but may be used alone during a public exposure event</td>
</tr>
<tr>
<td>Critical Infrastructure Protection (CIP) Plan</td>
<td>Provides policies and procedures for protection of national critical infrastructure components</td>
<td>Addresses critical infrastructure components that are supported or operated by an agency or organization</td>
<td>Risk management plan that supports COOP plans for organizations with critical infrastructure and key resource assets</td>
</tr>
<tr>
<td>Cyber Incident Response Plan</td>
<td>Provides procedures for mitigating and correcting a cyber attack, such as a virus, worm, or Trojan horse</td>
<td>Addresses mitigation and isolation of affected systems, cleanup, and minimizing loss of information</td>
<td>Information system focused plan that may activate an ISCP or DRP, depending on the extent of the attack</td>
</tr>
</tbody>
</table>
### Summary of Types of Plans

<table>
<thead>
<tr>
<th>Plan</th>
<th>Purpose</th>
<th>Scope</th>
<th>Plan Relationship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Disaster Recovery Plan (DRP)</td>
<td>Provides procedures for <strong>relocating information systems operations to an alternate location</strong></td>
<td>Activated after major system disruptions with long-term effects</td>
<td>Information system focused plan that activates one or more ISCPs for recovery of individual systems</td>
</tr>
<tr>
<td>Information System Contingency Plan (ISCP)</td>
<td>Provides procedures and capabilities for <strong>recovering an information system</strong></td>
<td>Addresses single information system recovery at the current or, if appropriate, alternate location</td>
<td>Information system-focused plan that may be activated independent from other plans or as part of a larger recovery effort coordinated with a DRP, COOP, and/or BCP</td>
</tr>
<tr>
<td>Occupant Emergency Plan (OEP)</td>
<td>Provides coordinated procedures for <strong>minimizing loss of life or injury and protecting property damage</strong> in response to a physical threat</td>
<td>Focuses on personnel and property particular to the specific facility; not mission/business process or information system-based</td>
<td>Incident-based plan that is initiated immediately after an event, preceding a COOP or DRP activation</td>
</tr>
</tbody>
</table>
Interrelationships

Plans may be implemented in coordination with one another

* One or more BCPs should be activated
** One or more ISCPs should be activated

- Business/mission process-focused plan
- Assets/personnel-focused plan
- Information system-focused plan
There are 7 steps to develop and maintain an effective information system contingency plan:

1. Develop the contingency planning policy
2. Conduct the Business Impact Analysis (BIA)
3. Identify preventive controls
4. Create contingency strategies
5. Develop an information system contingency plan
6. Ensure plan testing, training and exercises
7. Ensure plan maintenance
- These steps represent key elements in a comprehensive information system contingency planning capability and are designed to be integrated into each stage of the system development life cycle.

<table>
<thead>
<tr>
<th>Develop Contingency Planning Policy</th>
<th>Conduct Business Impact Analysis</th>
<th>Identify Preventative Controls</th>
<th>Create Contingency Strategies</th>
<th>Develop Contingency Plan</th>
<th>Plan Testing, Training, and Exercises</th>
<th>Plan Maintenance</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Identify statutory or regulatory requirements</td>
<td>• Determine business processes and recovery criticality</td>
<td>• Identify controls</td>
<td>• Backup &amp; recovery</td>
<td>• Document recovery strategy</td>
<td>• Plan testing</td>
<td>• Review and update plan</td>
</tr>
<tr>
<td>• Develop IT contingency planning policy statement</td>
<td>• Identify outage impacts and estimated downtime</td>
<td>• Implement controls</td>
<td>• Identify roles &amp; responsibilities</td>
<td>• Train personnel</td>
<td>• Coordinate with internal/external organizations</td>
<td></td>
</tr>
<tr>
<td>• Publish policy</td>
<td>• Identify resource requirements</td>
<td>• Maintain controls</td>
<td>• Address alternate site</td>
<td>• Plan exercises</td>
<td>• Control distribution</td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Identify recovery priorities for system</td>
<td></td>
<td>• Identify equipment and cost considerations</td>
<td>• TT&amp;E activities</td>
<td>• Document changes</td>
<td></td>
</tr>
</tbody>
</table>
1. Develop Contingency Planning Policy

- A *formal policy* should be created that provides the *authority and guidance* necessary to develop an effective contingency plan.
- To be effective and to ensure that personnel fully understand the organization’s contingency planning requirements, the contingency plan must be based on a *clearly defined policy*.

- Policy statement should define the organization’s overall *contingency objectives* and establish the organizational *framework and responsibilities* for system contingency planning.
- To be successful, senior management, most likely the CIO, must support a contingency program and be included in the process to develop the program policy.
- Policy should reflect the impact levels and the contingency controls that each impact level establishes.
1. Develop Contingency Planning Policy

Key policy elements should include the following:

- Roles and responsibilities
- Scope as it applies to common platform types and organization functions (telecommunications, legal, media relations) subject to contingency planning
- Resource requirements
- Training requirements
- Exercise and testing schedules
- Plan maintenance schedule
- Minimum frequency of backups and storage of backup media
2. Conduct Business Impact Analysis

**Business Impact Analysis (BIA)** helps identify and prioritize information systems and components critical to supporting the organization’s mission/business processes.

Three steps are typically involved in accomplishing the BIA:

1. Determine mission/business processes and recovery criticality
2. Identify resource requirements
3. Identify recovery priorities for system resources
2. Conduct Business Impact Analysis

Supported mission/business processes should then be analyzed with the process owners, leadership and business managers to determine the acceptable downtime if a given process or specific system data were disrupted or otherwise unavailable.

Downtime can be identified in several ways:

- **Maximum Tolerable Downtime (MTD)**: The total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations.

- **Recovery Time Objective (RTO)**: The maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the MTD.

- **Recovery Point Objective (RPO)**: The point in time, prior to a disruption or system outage, to which mission/business process data can be recovered (given the most recent backup copy of the data) after an outage.
During the BIA, it should be determined what the **optimum point** is to RECOVER the information system while BALANCING the **cost of system inoperability** against the **cost of resources** required for restoring the system and its overall support for critical mission/business processes.
3. Identify Preventive Controls

- In some cases, the outage impacts identified in the BIA may be mitigated or eliminated through preventive measures that deter, detect, and/or reduce impacts to the system.

- Where feasible and cost effective, preventive methods are preferable to actions that may be necessary to recover the system after a disruption.
Some common preventive control measures are listed below:

- Uninterruptible power supplies to provide short-term backup power to all system components (including environmental and safety controls)
- Gasoline- or diesel-powered generators to provide long-term backup power
- Air-conditioning systems with adequate excess capacity to prevent failure of certain components, such as a compressor
- Fire suppression systems
- Fire and smoke detectors
- Water sensors in the computer room ceiling and floor
- Heat-resistant and water-proof containers for backup media and vital non-electronic records
- Emergency master system shutdown switch
- Offsite storage of backup media, non-electronic records and system documentation
- Technical security controls, such as cryptographic key management
- Frequent scheduled backups including where the backups are stored (onsite or offsite) and how often they are recirculated and moved to storage
4. Create Contingency Strategies

Organizations are required to **adequately mitigate the risk** arising from use of information and information systems in the execution of mission/business processes.

The challenge for organizations is in implementing the **right set of security controls**.

Contingency strategies are created to mitigate the risks for the contingency planning family of controls and cover the full range:

- **Backup**
- **Recovery**
- **Contingency planning**
- **Testing**
- **Ongoing maintenance**
5. Develop Contingency Plan

- **Information system contingency plan development** is a critical step in the process of implementing a comprehensive contingency planning program.

- The plan contains the following associated with restoring an information system following a disruption:
  - Detailed roles
  - Responsibilities
  - Teams
  - Procedures

- The information system contingency plan should document technical capabilities designed to support contingency operations and should be tailored to the organization and its requirements.

- Plans need to balance detail with flexibility; usually, the more detailed the plan, the less scalable and versatile the approach.
There are typically five main components of a contingency plan:

1. **Supporting Information**
   - BIA
   - POC lists
   - Procedures

2. **Activation and Notification Phase**
   - Activation criteria
   - Notification procedures
   - Outage assessment

3. **Recovery Phase**
   - Sequence recovery activities
   - Recovery procedures
   - Escalation and notifications

4. **Reconstitution Phase**
   - Concurrent processing
   - Testing
   - Notifications
   - Cleanup
   - Offsite data storage
   - Backup
   - Documentation

5. **Appendices**
   - BIA
   - POC lists
   - Procedures
Supporting information component includes an introduction and concept of operations section providing essential background or contextual information that makes the contingency plan easier to understand, implement and maintain:

These details aid in understanding the following:
- Applicability of the guidance
- In making decisions on how to use the plan
- In providing information on where associated plans and information outside the scope of the plan may be found
The introduction section orients the reader to the type and location of information contained in the plan. Generally, this section includes the following:

**Background**
- Establishes the reason for developing the ISCP and defines the plan objectives

**Scope**
- Identifies the impact level and associated Recovery Time Objectives (RTOs) as well as the alternate site and data storage capabilities

**Assumptions**
- Includes the list of assumptions used in developing the ISCP as well as a list of situations that are not applicable
The concept of operations section typically includes the following:

- **System Description**
  - General description of the information system addressed by the contingency plan
  - Should include the information system architecture, locations, and any other important technical considerations
  - Input/output diagram and system architecture diagram, including security devices are useful

- **Overview of three phases**
  - ISCP recovery is implemented in three phases
    - Activation & Notification
    - Recovery
    - Reconstitution

- **Roles & Responsibilities**
  - Presents the overall structure of contingency teams, including the hierarchy and coordination mechanisms and requirements among the teams
  - Provides an overview of team member roles and responsibilities in a contingency situation
5. Develop Contingency Plan

2 Activation and Notification Phase

The **Activation and Notification Phase** defines initial actions taken once a system disruption or outage has been detected or appears to be imminent.

- Notify recovery personnel
- Conduct an outage assessment
- Activate the Plan

*Activation criteria* include:
-Extent of any damage to the system (physical, operational, or cost)
- Criticality of the system to the organization’s mission
- Expected duration of the outage lasting longer than the RTO
Notification procedures should be documented in the plan outages or disruption that occur with or without prior notice:

- Should describe the methods used to notify recovery personnel during business and non-business hours.
- Call tree should be included and account for primary and alternate contact methods and discuss procedures to be followed if an individual cannot be contacted.
- Type of information to be relayed should be documented in the plan:
  - Nature of the outage or disruption
  - Any known outage estimates
  - Response and recovery details
  - Where and when to convene for further instructions
  - Instructions to prepare for relocation for estimated time period
  - Instructions to complete notifications using the call tree.
5. Develop Contingency Plan

2 Activation and Notification Phase

Outage assessment should be completed as quickly as the given conditions permit, with personnel safety remaining the highest priority

- Conducted to assess the nature and extent of the disruption
- Should address the following at a minimum:
  - Cause of outage or disruption
  - Potential for additional disruptions or damage
  - Status of physical infrastructure
  - Inventory and functional status of system equipment
  - Type of damage to system equipment or data
  - Items to be replaced
  - Estimated time to restore normal services
5. Develop Contingency Plan

3. Recovery Phase

The **Recovery Phase** begins after the ISCP has been activated, outage assessment has been completed, personnel have been notified, and appropriate teams have been mobilized:

- Focuses on implementing recovery strategies to restore system capabilities, repair damage, and resume operational capabilities at the original or new alternate location.
- It is feasible that only system resources identified as high priority in the BIA will be recovered in this stage.
- ISCP should provide detailed procedures to restore the information system or components to a known state.
- Recovery procedures should be written in a straightforward, step-by-step style.
- No steps should be assumed or omitted.
SAMPLE Recovery Process for the LAN Recovery Team:
These procedures are used for recovering a file from backup tapes. The LAN Recovery
Team is responsible for reloading all critical files necessary to continue production.

1. Identify file and date from which file is to be recovered.
2. Identify tape number using tape log book.
3. If tape is not in tape library, request tape from recovery facility; fill out with
   appropriate authorizing signature.
4. When tape is received, log date and time.
5. Place tape into drive and begin recovery process.
6. When file is recovered, notify LAN Recovery Team Leader.
5. Develop Contingency Plan

3. Recovery Phase

- Including an **escalation and notification** component with the Recovery Phase helps to ensure that overall, a repeatable, structured, consistent, and measurable recovery process is followed.

- Effective escalation and notification procedures should define and describe the events, thresholds, or other types of triggers that are necessary for additional action.

- Action would include additional notifications for more recovery staff, messages and status updates to leadership, and notices for additional resources.
Reconstitution Phase

The Reconstitution Phase defines the actions taken to test and validate system capability and functionality:

- Recovery activities are completed and normal system operations are resumed.
- If original facility is unrecoverable, the activities in this phase can also be applied to preparing a new permanent location to support system processing requirements.
- Phase consists of validating system recovery and deactivation of the plan.
4 Reconstitution Phase

- Validating system recovery typically includes these steps:
  
  **Concurrent Processing**
  - Concurrent processing is the process of running a system at two separate locations concurrently until there is a level of assurance that the recovered system is operating correctly and securely.

  **Validating Data Testing**
  - Data testing is the process of testing and validating recovered data to ensure that data files or databases have been recovered completely and are current to the last available backup.

  **Validation Functionality Testing**
  - Functionality testing is a process for verifying that all system functionality has been tested, and the system is ready to return to normal operations.
4. Reconstitution Phase

- **Deactivation of the plan** is the process of returning the system to normal operations and finalizing reconstitution activities to prepare the system against another outage or disruption and includes the following activities:

  - **Notification**
    - Upon return to normal operations, users should be notified by the ISCP Coordinator using predefined notification procedures.
  
  - **Cleanup**
    - Process of cleaning up work space or dismantling any temporary recovery locations, restocking supplies, returning manuals or other documentation to their original locations, and readying the system for another contingency event.

  - **Offsite Data Storage**
    - If offsite data storage is used, procedures should be documented for returning retrieved backup or installation media to its offsite data storage location.

  - **Data Backup**
    - As soon as reasonable following reconstitution, the system should be fully backed up and a new copy of the current operational system stored for future recovery efforts.

  - **Event Documentation**
    - All recovery and reconstitution events should be well documented, including actions taken and problems encountered during the recovery and reconstitution efforts.
5. Develop Contingency Plan

Appendices

Contingency plan appendices provide key details not contained in the main body of the plan:

- Contact information for contingency planning team personnel
- Vendor contact information, including offsite storage and alternate site POC’s
- BIA
- Detailed recovery procedures and checklists
- Detailed validation testing procedures and checklists
- Equipment and system requirement lists of hardware, software and other resources required to support system operations
- System interconnections
- Vendor SLAs, reciprocal agreements with other organizations
6. Plan Testing, Training, and Exercises

- Organizations should conduct **test, training and exercise events** periodically, following organizational or system changes or as otherwise needed.

- Execution of testing, training and exercise events assists organizations in determining the plan’s effectiveness, and that all personnel know what their roles are in the conduct of each information system plan.

- For each test, training, and exercise activity conducted, results should be documented in an after-action report, and a “Lessons Learned” corrective action captured for updating information in the information system contingency plan.
7. Plan Maintenance

- To be effective, the plan must be maintained in a ready state that accurately reflects system requirements, procedures, organizational structure, and policies.

- Information systems undergo frequent changes because of shifting business needs, technology upgrades, or new internal or external policies.

- It is essential that the information system contingency plan be reviewed and updated regularly as part of the organization’s change management process to ensure that new information is documented and contingency measures are revised if required.
Financial Institutions are required by the FFEIC to have Business Continuity Planning that meets the requirements of 12 CFR Part 748 and 749.

Items that regulators will typically ask you to provide:
- Business Continuity Plan (BCP)
- Business Impact Analysis (BIA)
- Recovery procedures
- Data center tour
- Results of recent disaster recovery tour, including scope of test procedures performed
- Summary of insurance policy coverage for e-commerce, electronic crime, and loss of records/equipment
6 Core BCP Items Regulators Will Check For

1. Have you **developed a program** to prepare for a catastrophic act?
2. Have you performed a **Business Impact Analysis (BIA)**?
3. Does your program incorporate a **risk assessment** to determine critical systems and necessary resources?
4. Does the **written plan address all necessary items**?
5. Are internal controls in place for **reviewing** the plan at least annually and for **revising** the plan as circumstances warrant?
6. Is the Business Continuity Plan **tested** on an annual basis?
1. Have you developed a program to prepare for a catastrophic act?
A **Business Impact Analysis** is the first step to developing a **Business Continuity Program**

Management should determine **possible threats** to the credit union’s business continuity

Threats vary with each organization’s unique situation:

- Terrorism
- Equipment failure
- Employee sabotage
- Flood
- Power failure
- Fire
- Theft

The amount of time and resources spent on performing the BIA will depend on the size and complexity of the organization

BIA should include **all business functions and departments**, not just data processing

Management **should identify critical business functions and prioritize them**

It should estimate the **maximum allowable downtime** for critical business processes and the **costs** associated with that downtime
Does your program incorporate a risk assessment to determine critical systems and necessary resources?

- At a minimum, all credit unions should establish **maximum allowable downtimes** for critical business functions.
- These may also be referred to as **recovery time objectives (RTOs)**.
- Some business functions may require near 24/7 uptime, while others may not be immediately critical but become critical if down for more than a few days.
Comprehensive Business Continuity Program

Does the written plan address all necessary items?

- **Personnel** with authority to enact the plan
- Preservation and ability to **restore vital records**
- A **method for restoring vital member services** through identification of alternate operating locations or mediums to provide services
  - Telephone centers
  - Shared service centers
  - Agreements with other organizations
  - Other appropriate methods
- **Communication methods** for employees and members
4 Does the written plan address all necessary items?  continued

- Notification of regulators via a **Catastrophic Act Report**
  - **5 business days** for any federally insured financial institution
  - A catastrophic act is any disaster, natural or otherwise, resulting in physical destruction or damage to the organization or causing an interruption in vital member services projected to last **more than two consecutive business days**
  - Within a reasonable time after a catastrophic act occurs, the organization needs to ensure that a **record of the incident is prepared and filed** at its main office
  - It should include information sufficient to indicate the office where the catastrophic act occurred; when it took place; the amount of the loss, if any; whether any operational or mechanical deficiencies might have contributed to the catastrophic act; and what has been done or is planned to be done to correct the deficiencies
Comprehensive Business Continuity Program

Does the written plan address all necessary items?  continued

- **Training** and *documentation of training* to ensure all employees and volunteer officials are aware of procedures to follow in the event of destruction of vital records or loss of vital member services

- **Testing procedures**, including a means for *documenting the testing results*
  - Several methods for testing and/or exercising contingency plans to identify potential weaknesses
    - Checklist
    - Walk-through/tabletop
    - Simulation: parallel, full interrupt
  - Contingency plan testing and/or exercises include a determination of the effects on organizational operations and assets and individuals arising due to contingency operations in accordance with the plan
Are internal controls in place for reviewing the plan at least annually and for revising the plan as circumstances warrant?

- Do they address changes in the organization’s operations?
- Changes might include new services offered or outsourcing decisions regarding which business functions the organization performs in-house
Testing of Plan

6 Is the Business Continuity Plan Tested on an annual basis?
**Additional questions** regulators may try to determine based on the size and complexity of your organization:

- Does the credit union's business continuity and/or disaster recovery plan (BCP/DRP) **address the timely recovery of its IT functions** in the event of a disaster?
  - Is the BCP/DRP appropriate for the size and complexity of the organization?
  - If the organization relies heavily on internet, web, or electronic services and communications to conduct business, then the BCP/DRP should address all appropriate delivery avenues.
  - The plan should address the following:
    - Timely recovery of services in the event of a disaster or other event that causes the system to be down
    - Environmental risks when determining the location of alternate processing sites
    - Alternate communication methods and paths
    - Alternate service providers
Comprehensive Contingency Plan

- Does the **contingency plan** address all necessary items?
  
  - A Contingency Plan should be part of an overall organizational program for achieving continuity of operations for mission/business operations

  - Contingency planning should address both **information system restoration** and **implementation of alternative business processes** when systems are compromised
  
  - Information system **recovery objectives** should be consistent with applicable laws, directives, policies, standards, or regulations
  
  - In addition to information system availability, contingency plans should address other security-related events resulting in a reduction in business effectiveness, such as malicious attacks compromising the confidentiality or integrity of the information system
Does the contingency plan address all necessary items? (continued)

- **Essential missions and business functions** and associated contingency requirements
- **Recovery time objectives, restoration priorities, and metrics**
  - Restoration priorities should follow a logical sequence due to interdependencies between systems. For example, the core system must be up before Internet banking is restored.
- **Contingency roles, responsibilities, and contact information** for personnel that support the plan
  - Should include emergency contact information for employees, officials, regulatory offices, and vendors used to support critical business processes
- Maintaining essential missions and business functions despite an information system disruption, compromise, or failure
- **Eventual, full information system restoration** without deterioration of the security measures originally planned and implemented
Comprehensive Contingency Plan

- Does the **contingency plan** address all necessary items? (continued)

  - **Review and approval** by designated officials within the organization
    - The contingency planning policy can be included as part of the general information security policy for the organization
    - Contingency planning procedures can be developed for the security program in general and for a particular information system, when required
    - The organizational risk management strategy is a key factor in the development of the contingency planning policy
  
  - **Revisions to address changes** to the organization, information system, or environment of operation
  
  - **Problems encountered** during contingency plan implementation, execution, or testing
Alternate Site and Equipment

- Has the organization’s management provided the following:

  - Established an **alternate storage site** including necessary agreements to permit the **storage and recovery** of information system backup
  - Ensured **equipment and supplies** required to resume operations are available at the alternate site or contracts are in place to support delivery to the site in time to support the organization-defined time period for resumption
Alternate Telecommunications Services

- Has the organization established alternate telecommunications services including necessary agreements to permit the resumption of information system operations for essential business functions when the primary telecommunications capabilities are unavailable?

  - Should attempt to identify and eliminate single points of failure across telecommunications infrastructure
  - Should consider the telecommunications diversity necessary for the organization’s size and complexity
  - This may include arrangements with multiple telecommunications providers
  - A key consideration in choosing a backup provider with adequate diversity is whether it uses the same sub-carrier or local access service provider
Backup and Recovery

- Has management established appropriate backup policies and procedures to ensure the timely restoration of critical services?
  
  - Backup and recovery policies should include:
    - Systems to be backed up
    - Method and type of backup
    - Frequency of backup
    - Storage and encryption of backup media
    - Rotation schedule
    - Restoration procedures
    - Testing
  
  - Procedures should include system-level information such as system-state information, operating system and application software, and licenses
Backup and Recovery

- Does management periodically test backup and retention of data as well as the erasure and release of media when retention is no longer required?
  - It is important that the completion of the backup process is logged and that management review these logs
  - Policies, procedures, standards, and guidance regarding management's review of backup logs should include:
    - Frequency of review
    - Assignment of responsibility
    - Documentation produced during backup process
    - Assessment of successful and timely backup
  - Backup policies, procedures, standards, and guidance should be followed to ensure the availability of data significant to the organization’s operations
  - The organization must provide for the recovery and reconstitution of the information system to a known state after a disruption, compromise, or failure
Backup and Recovery

- Are updated hardware and software inventories maintained, including version numbers for software?
Backup Power

- Does the organization have adequate **uninterruptible power supply (UPS) protection** to perform an orderly systems shutdown in case of power loss?
  - UPS is a power supply that includes a battery to maintain power in the event of a power outage
- Has management ensured that critical systems are **connected to a backup power source**?
- Are backup power sources **periodically tested**?
About TWHC

Turner, Warren, Hwang & Conrad AC (TWHC), based in Los Angeles, California, is a full-service CPA firm built on principles that ensure its clients receive value. TWHC was established in 1987, and its charter partners all worked together at a previous firm that was driven by similar principles.

TWHC has a diversified clientele. In addition to traditional individual and small business tax services, the firm has three specialty practices: Financial Institutions, Retirement Plans and Not-For-Profit. TWHC employs close to 50 employees who provide our clients with best-in-class service. This, in turn, helps our clients to meet their objectives.

For three decades, TWHC has developed numerous services to help its clients improve their operations and take advantage of efficiencies that they may not otherwise be aware of.

The firm continues to celebrate its heritage by adding to its long list of distinguished clients who have tried large firms but were not able to receive the level of service they were looking for. Today, TWHC is recognized in various markets as being the largest provider serving that market.

TWHC has been able to accomplish this because of its core values and the fact that it never takes its eye off of what is most important: the client. With two offices, one in San Francisco and one in Los Angeles (Burbank), TWHC serves clients all over the United States.

The most valuable capital that TWHC has is its loyal clients, who themselves are very aware of what is best for their companies. The most valuable support for TWHC is its work force and its tradition of outstanding service.