Contingency Planning

State Of Arizona
Office Of The Auditor General
Jennie Snedecor & Katie Morris
Part I - Overview of IT Controls and Best Practices

Part II - Identifying Users and Limiting Access

Part III - Network Controls

Part IV - Contingency Planning
Contingency Planning Issues Covered in this Webinar

- What is Contingency Planning and why is it important?
- Creating a Contingency Plan (CP)
- Testing the Contingency Plan
- Best practices, tools, and resources
What is Contingency Planning?

- Incident Management
- Contingency Planning
- Business Process Continuity
- Disaster Recovery
What is Contingency Planning

• Procedures and measures may include:
  • Use of alternate equipment
  • Use of alternate/manual processing
  • Moving to an alternate location
  • Implementing controls
What is a Disruption (in relation to IT)?

Interruption of service or destruction of hardware

- Adversarial
- Accidental
- Structural
- Environmental
Management and IT roles in Contingency Planning

Management
- Risk Assessments
- Business Impact Analysis
- Contingency Plans
- Training/Testing

IT Staff
- Contingency Plans for IT-only systems
## Risk Management

<table>
<thead>
<tr>
<th>Disruption /Threat</th>
<th>Threat Type</th>
<th>Range of Effects</th>
<th>Likelihood of occurrence</th>
<th>Vulnerabilities</th>
<th>Severity</th>
<th>Likelihood Event Results in Adverse Impact</th>
<th>Overall Likelihood</th>
<th>Level of Impact</th>
<th>Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>lightning at Data Center</td>
<td>Environmental</td>
<td>High</td>
<td>Moderate</td>
<td>Contingency Plan does not exist for all systems</td>
<td>High</td>
<td>High</td>
<td>Moderate</td>
<td>Moderate</td>
<td>Moderate</td>
</tr>
</tbody>
</table>

NIST SP 800-30r1 and NIST SP 800-39
Why is Contingency Planning important?

- Reduces risk system and service unavailability
- Minimizes effect of system and service unavailability
- Allows for continuity of operations
- Prevents worsening the actual disruption
Does One Size Fit All?

Contingency plans should:
• Fit the size of the district
• Be tailored to the district’s needs
• Address individual information systems
Contingency Planning Process

- Develop the contingency planning policy
- Conduct the Business Impact Analysis
- Identify preventive controls
- Create contingency strategies
- Develop an information system contingency plan
- Ensure plan testing, training, and exercises
- Ensure plan maintenance
Develop the Contingency Planning Policy

- Roles and Responsibilities
- Scope
- Resource Requirements
- Training Requirements
- Testing Schedules
- Plan Maintenance Schedule
- Backup Requirements
Contingency Planning Process

1. Develop the contingency planning policy
2. Conduct the Business Impact Analysis
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
Conduct the Business Impact Analysis

1. Determine the mission/business process supported by the system and recovery criticality

- Identify outage impacts and estimated downtime
- Recovery Point Objective (RPO)
- Recovery Time Objective (RTO)
- Work Recovery Time (WRT)
- Maximum Tolerable Downtime (MTD)
Conduct the Business Impact Analysis - Estimated Downtime

- Last backup or point where data is in a usable state
- Disaster Strikes
- RPO = 12hrs
- RTO = 4hrs
- MTD = 6hrs
- Recovery
- WRT = 2hrs
- Resume Operations
Conduct the Business Impact Analysis

2. Identify resources required to resume mission/business processes:

- Facilities
- Personnel
- Equipment
- Software
- Data Files
- System Components
- Vital Records
Conduct the Business Impact Analysis

3. Identify recovery priorities:
   Creating a system recovery hierarchy based on critical business processes, outage impacts, MTD, and system resources
Contingency Planning Process

1. Develop the contingency planning policy
2. Conduct the Business Impact Analysis
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
Identify Preventative Controls

Environmental Controls
• Protect power equipment and cabling
• Short-term uninterruptible power supply (UPS)
• For data centers, server rooms, and mainframe computer rooms provide:
  • Emergency shutoff switches
  • Automatic emergency lighting
  • Fire suppression and detection devices
  • Temperature and humidity levels monitoring
  • Master shutoff for water or isolation valves
Contingency Planning Process

1. Develop the contingency planning policy
2. Conduct the Business Impact Analysis
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
Create Contingency Strategies

**Backups**
- Policies should designate:
  - Frequency
  - Scope
  - Location of stored data
  - File naming
  - Rotation frequency
  - Method for transporting data offsite

**Alternate Processing Site**
- Cold sites
- Warm sites
- Hot sites
- Mirrored sites

**Third Party Agreements**
- Specify emergency maintenance service
- For third party hosts (including county) - Contingency Plan is still required
- Responsibilities of each party included in plan and vendor contracts
Contingency Planning Process

1. Develop the contingency planning policy
2. Conduct the Business Impact Analysis
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
Developing a Contingency Plan - Supporting Information

**Introduction**
- Background
- Scope
- Assumptions

**Concept of Operations**
- System Description
- Overview of 3 Phases of Plan
- Roles & Responsibilities
Developing a Contingency Plan -
Activation and Notification

- Activation Criteria
- Notification Procedures
- Outage Assessment
Developing a Contingency Plan - Activation and Notification

• Activation criteria should be based on:
  • Extent of damage to the system
  • Importance of the system to the district’s mission
  • Expected duration of the outage is within the RTO
Notification Procedures

- Utilize a call tree
  - Include primary and alternate contact methods
  - Include contacts for vendors and third party service providers
  - Document the type of information that should be passed along during notification
Developing a Contingency Plan - Activation and Notification

- Cause of outage or disruption
- Potential for additional disruption or damage
- Status of physical infrastructure
- Inventory & functional status of equipment
- Damage to system equipment or data
- Items that need replacement
- Estimated time to restore normal services

Outage Assessment
Developing a Contingency Plan - Recovery

- Ranking of Recovery Activities
- Detailed Recovery Procedures
- Recovery Escalation & Notification

Recovery Phase
Developing a Contingency Plan - Recovery

Sequential Order of Recovery Activities
- Align with the MTD
- Reflect priorities identified in BIA
- Include escalation steps to address:
  - Actions not completed within expected timeframe
  - Completion of key steps
  - Need to purchase item(s)
  - System-specific concerns
Developing a Contingency Plan - Recovery

Detailed Recovery Procedures

- Obtaining authorization to access damaged facilities and/or geographic area
- Notifying internal and external system owners/users
- Obtaining necessary office supplies and work space
- Obtaining and installing necessary hardware components
- Obtaining and loading backup media
- Restoring critical operating system and application software
- Restoring system data to a known state
- Testing system functionality including security controls
- Connecting system to network or other external systems
- Operating alternate equipment successfully
Developing a Contingency Plan - Recovery

Recovery Escalation & Notification
- Describe events, thresholds, or other triggers that require additional action
- Establish clear set of events, actions, and results

- Additional damage to hardware discovered
- Notify District Officials
- Purchase additional resources
Developing a Contingency Plan - Reconstitution

Actions taken to test and validate system capability and functionality

<table>
<thead>
<tr>
<th>Validation</th>
<th>Deactivation</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Concurrent Processing</td>
<td>• Notifying Users</td>
</tr>
<tr>
<td>• Validation Data Testing</td>
<td>• Cleanup</td>
</tr>
<tr>
<td>• Validation Functionality Testing</td>
<td>• Offsite Data Storage</td>
</tr>
<tr>
<td></td>
<td>• Data Backup</td>
</tr>
<tr>
<td></td>
<td>• Documentation of events</td>
</tr>
</tbody>
</table>
# Developing a Contingency Plan - Appendices

<table>
<thead>
<tr>
<th>Appendix</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Contact information for team personnel</td>
<td></td>
</tr>
<tr>
<td>Vendor contact information</td>
<td></td>
</tr>
<tr>
<td>Business impact analysis</td>
<td></td>
</tr>
<tr>
<td>Detailed recovery procedures</td>
<td></td>
</tr>
<tr>
<td>Detailed validation testing procedures</td>
<td></td>
</tr>
<tr>
<td>Equipment and system requirements lists</td>
<td></td>
</tr>
<tr>
<td>Alternate business processing procedures</td>
<td></td>
</tr>
<tr>
<td>Contingency plan testing</td>
<td></td>
</tr>
<tr>
<td>System interconnections</td>
<td></td>
</tr>
<tr>
<td>Vendor SLAs, agreements with other organizations, and other vital records</td>
<td></td>
</tr>
</tbody>
</table>
Contingency Planning Process

1. Develop the contingency planning policy
2. Conduct the Business Impact Analysis
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
**Training**

**Who**
- Only personnel required for each systems contingency plan

**When**
- At least annually
- Employees newly assigned to contingency role

**What**
- Purpose of the plan
- Reporting procedures
- Security requirements
- Individual responsibilities for activation & notification, recovery, and reconstitution
Testing the Contingency Plan

Who
• All personnel involved in the contingency plan process

When
• At least annually
• Change in circumstance (system, personnel)

What
• Notification procedures
• System recovery on alternate platform from backup media
• Internal and external connectivity
• System performance using alternate equipment
• Restoration of normal operations
• Other areas as needed
Testing the Contingency Plan

Tabletop Exercises
- Discussion based
- Scenarios presented/discussed
- No equipment/resources used

Functional Exercises
- Simulation based
- Vary in complexity
- Roles/responsibilities executed
Contingency Planning Process

1. Develop the contingency planning policy
2. Conduct the Business Impact Analysis
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
Best practices, tools, and resources

National Institute of Standards and Technology (nist.gov)
- **Special publication 800-34** (Contingency planning guide)
- **Special publication 800-53 r4** (Assessing security and privacy controls)
- **Special publication 800-30 r1** (Guide for Conducting Risk Assessments)
- **Special publication 800-39** (Managing Information Security Risk)

Arizona Office of the Auditor General (azauditor.gov)
- Reports and Publications/School Districts/Manuals/Memorandums
  View USFR. Information Technology (page 235)
Questions

Questions?

• Contact Us:
  • By phone: 602-553-0333
  • By email: asd@azauditor.gov
References


• Swanson, M., Bowen, P., Phillips, A. W., Gallup, D., & Lynes, D. (2010). Contingency planning guide for federal information systems. doi:10.6028/nist.sp.800-34r1