Department of Budget & Management

State of Maryland
Information Technology (IT)
Disaster Recovery Guidelines
Version 4.0

July 2006

TABLE OF CONTENTS

RECORD OF CHANGES PAGE

Issue	Date	Pages Affected	Description
Original Draft		N/A	N/A
Revision	April 30, 2003	Pg #2, 4, 11, & 13 Pg #5, 8, & Appendix C & E Appendix C Appendix C	Typographical Added RPO Sample IT D/R Exercise Testing Template Added staffing and spacing requirements to BIA Template Added Damage Assessment Template
3.0	July 20, 2003	Various pages	Typographical
4.0	July 2006	Various Pages	Removed contractor references. Included references to National Institute of Standards and Technology (NIST) 800-34 and 800-30 Removed obsolete references, appendices, and format.

STATE OF MARYLAND

INFORMATION TECHNOLOGY (IT) DISASTER RECOVERY GUIDELINES

1.0 INTRODUCTION

1.1 Purpose

The purpose of this document is to provide statewide guidance to personnel responsible for preparing and maintaining Information Technology (IT) Disaster Recovery Plans (DRP). The DRP is an IT-focused plan designed to restore operability of targeted systems, applications, or a computer facility due to a natural or man-made extended interruption of an agency's business services.

These guidelines provide fundamental planning principles and practices that support the State's IT Disaster Recovery Planning and Security Policies.

1.2 Scope

The scope of this document is to provide recommended disaster recovery planning principles to design and implement recovery and restoration procedures for data, hardware, and software that is necessary for an agency to restart operations.

This document focuses on the Disaster Recovery Plan and does not provide contingency planning guidance for business processes. The State of Maryland recommends that the following National Institute of Standards and Technology (NIST) be used in the development of related IT plans such as the Continuity of Operations (COOP), Business Impact Analysis (BIA), and Risk Analysis (RA).

- NIST 800-34 Contingency Planning Guide for Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf; and
- NIST 800-30 Risk Management Guide for Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf

1.3 Policy/Authorization

The Maryland Code, *Law Pertaining to Information Processing, State Finance and Procurement*, Title 3, Subtitle 4, 3-401 to 3-413 authorizes these guidelines. Section 3-403 (a) charges the Secretary, Department of Budget and Management (DBM), with responsibility "for developing, maintaining, revising, and enforcing information technology policies and standards." Section 3-410 authorizes the State Chief of Information Technology (CIT) to carry out certain duties for the Secretary, DBM. Section 3-410 (d) (1) charges the Chief to be responsible to the Secretary DBM for carrying out the duty of "developing, maintaining, and enforcing statewide information technology standards, policies, and procedures."

1.4 Background

These guidelines are intended to support and promote the development and implementation of a consistent statewide IT disaster recovery program. Agencies should use these guidelines to develop an effective plan that complies with statewide policy and promotes security of State IT resources. Existing plans should be evaluated for compliance with these guidelines.

1.5 Maintenance Process

Changes to this document will be recorded on the Record of Changes page immediately following the Table of Contents. The State CIT is responsible for maintaining and distributing these guidelines.

1.6 Assumptions

In developing these guidelines the following assumptions were made:

- The State CIT supports development and implementation of these guidelines as a tool to promote a consistent approach to DRP for State agencies.
- Agency heads will support, and promote the use of these guidelines.
- This guidance pertains to disaster recovery planning for IT systems and components only. A comprehensive continuity of operations program relies on supplemental facility and business resumption plans for a comprehensive recovery effort. This guideline document assumes such business and facility plans exist or will exist.

1.7 Coordination with Other Plans

IT disaster recovery fits into a much broader emergency preparedness environment that includes organizational and business process continuity and recovery planning. Ultimately, an organization would use a suite of plans to properly prepare response, recovery, and continuity activities for disruptions affecting the organization's IT systems, business processes, and operating facility. Because there is an inherent relationship between an IT system and the business process it supports, there should be coordination between each plan during development and updates to ensure that recovery strategies and supporting resources neither negate each other, nor duplicate efforts. The guidelines provided in this document address the recovery of the organization's IT systems. This planning guide does not address facility-level or organizational contingency planning.

The Maryland Emergency Management Agency (MEMA) provides additional information and guidance on Continuity of Operations (COOP) via the link below: http://www.mema.state.md.us/MEMA/content_page.jsp?TOPICID=coop.

1.8 Roles and Responsibilities

The State CIT is responsible for:

- Ensuring the State's IT disaster recovery planning program is established and implemented in compliance with State laws and regulations;
- Enforcing Agency compliance to State IT Disaster Recovery Guidelines;
- Developing policy, guidelines, best practices, IT disaster recovery planning, and incident response capability;
- Ensuring State IT Disaster Recovery Plans are maintained and exercised at appropriate intervals; and
- Coordination with State Agency CIO's, Federal Government, County Governments, and private industry;

Agency Heads are responsible for:

- Ensuring agency disaster recovery planning policies and procedures are consistent with these guidelines; and
- Having a contingency plan that includes the IT DRP that documents how business functions will be performed in the event their IT systems are unavailable (short and long-term unavailability).

Business/Information Owners are responsible for:

- Completing or assisting in the completion of the Business Impact Analysis (BIA);
- Defining the maximum amount of tolerable downtime for each of the identified functions. This becomes the recovery time objective (RTO) for the recovery solutions developed;
- Defining the point in time to which data must be restored in order to resume processing. This becomes the recovery point objective (RPO) for the recovery solutions developed. (i.e. how recent must the data used in the recovery be?);
- Using input from information gathered in the BIA, the RTO, and the RPO to define recovery priorities to be used in developing recovery procedures; and
- Wording contractual and service level agreements (SLAs) with external entities in a manner that ensures compliance with these guidelines.

Vendors/Contractors are responsible for:

- Compliance with these guidelines.

1.9 Document Disclosure – IT Disaster Recovery Plans

Please note that an IT Disaster Recovery Plan will contain information that is not for general viewing. The plan should be protected with the same level of controls used to protect sensitive data from unwarranted disclosure.

2.0 IT DISASTER RECOVERY PLANNING PROCESS

IT systems are vital elements in most State business processes. Because these IT resources are critical to an organization's success, it is essential that the services provided by these systems are able to operate effectively without excessive interruption. The IT Disaster Recovery Planning Guidelines contained in this section support this requirement by establishing a proven and structured approach to developing IT disaster recovery plans and procedures that enable a system to be recovered quickly and effectively following a service disruption or disaster. These guidelines use a three-phased approach, consisting of the Pre-Planning, Planning, and Post-Planning phases.

2.1 Pre-Planning Phase

The Pre-Planning Phase is composed of the following:

1. Business Impact Analysis (BIA)
2. Risk Assessment (RA)

The BIA and RA clearly identify what systems need to be recovered, how soon, in what priority, and also identify which risks need to be mitigated.

2.1.1 Business Impact Analysis (BIA)

To prepare or update a DRP, an agency will need to conduct a BIA to identify IT resources, identify outage impacts and allowable outage times, and develop recovery priorities. The BIA determines the focus of the IT DRP by providing the needed input to identify IT components that are essential to support agency business functions.

The data that is input to the BIA is gathered by collecting the following information from system or application users:

1. Identify business functions that are necessary to carry out State or Agency missions and mandated functions.
2. Define the maximum amount of tolerable downtime for each of the identified functions. This becomes the recovery time objective (RTO) for the recovery solutions developed.
3. Define the point in time to which data must be restored in order to resume processing. This becomes the recovery point objective (RPO) for the recovery solutions developed. (i.e. how recent must the data used in the recovery be?)
4. Using input from information gathered in step 1 through 3 above, develop recovery priorities that drive recovery procedures.

NIST 800-34 Contingency Planning Guide for Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-34/sp800-34.pdf offers guidance in developing a BIA and provides a sample template.

2.1.2 Risk Assessment (RA)

The purpose of a risk assessment is to help develop appropriate strategies and controls to maintaining information assets. As with the BIA, a RA must be conducted on each IT system relating to an agency's business function. Once risks have been identified, risk mitigation can be implemented to reduce the probability of the risk to an acceptable level.

Residual risks are defined as those risks observed to remain after mitigation actions have been undertaken to reduce known risks. A vulnerable physical location (i.e. near a flood zone, located over a parking garage, etc.) or lack of alternate cold, warm or hot site would be examples of observed residual risk. Any residual risks must be identified and preventive controls or recovery activities documented in the DRP. It is suggested that a high-level Agency official signoff on the assumptions of the risks to ensure both accountability and awareness.

NIST 800-30 Risk Management Guide for Information Technology Systems http://csrc.nist.gov/publications/nistpubs/800-30/sp800-30.pdf offers guidance in developing a RA and provides a sample template.

2.2 Planning Phase

This planning phase includes recovery strategies that may be required as the result of a natural or man-made disaster. Recovery strategies should be developed for technical components that support agency business functions as identified through the BIA. The strategies should also be developed to address any residual risks documented in the RA. The remainder of this section provides additional guidance on activities performed during this phase.

2.2.1 Development of Recovery Strategies

The purpose of a DRP is to document the recovery strategies and create a road map of predetermined actions that will reduce required decision-making during a disaster and systematically provide a documented recovery path. Although the likelihood of a catastrophic disaster is remote, the devastation and potential loss of the ability to perform services requires that advance planning occur in order to respond in an effective and responsible manner.

The recovery strategies developed should provide a means to restore IT components quickly and effectively following a service disruption. The selected recovery strategies should align and address the BIA and RA findings.

2.2.1.1 Backup Procedures

IT Disaster Recovery Plans must document backup procedures. Procedures should specify backup frequency based on data criticality and the frequency that new data is introduced. Backups should occur daily (at a minimum). Backup procedures should designate the location of stored data, retrieval procedures, backup test procedures, file-naming conventions, media rotation frequency, method for transporting data off-site, and a description of off-site storage facility. (Note: Backup procedures should be

documented as part of the standard operating procedures and are not required to be repeated in the DRP.)

The following should be included in the backups located off-site:

- Copy of IT Disaster Recovery Plan
- Data files (e.g., daily, weekly, monthly, etc.)
- Program files and source code
- Procedures
- Software licenses
- O/S scripts such as IBM JCL, Unix shell scripts, DEC command procedures, etc.
- Scheduling instructions

2.2.1.2 Testing Backup Procedures

Once backup procedures are documented, they should be tested. This test should include the successful restoration of data. This includes retrieval procedures to obtain off site data. Testing backup procedures will identify missing files, missing applications, and faulty procedures. Testing backup procedures also increases the likelihood of discovering procedural inconsistencies before an emergency, rather than during one.

2.2.1.3 Offsite Storage Considerations

The following should be considered when selecting an offsite storage facility or vendor:

- Geographic area – distance from the organization and the probability of the storage site being affected by the same disaster
- Accessibility – length of time allowable to retrieve data from storage and storage locations hours of accessibility
- Security – security capabilities of the storage facility and employee confidentiality must meet the data's sensitivity and security requirements
- Environment – structural and environmental conditions of the storage facility (i.e., temperature, humidity, fire prevention/suppression, and power management controls)
- Cost – costs of shipping, operational fees, and disaster response/recovery services

2.2.1.4 Alternate Sites

The selected recovery, or alternate site, must be able to support the recovery of essential IT resources that support business functions as defined in the IT disaster recovery plan.

Alternate Site Agreement: Agencies may use a memorandum of understanding (MOU) or memorandum of agreement (MOA) with another government entity to ensure that space, equipment, and/or staffing will be available at the alternate site. Vendors may also provide this service via a contract.

The agreement/contract should address the following:

- Contract/agreement duration
- Cost/fee structure for disaster declaration and occupancy (daily usage), administration, maintenance, testing, annual cost/fee increases, transportation support cost (receipt and return of offsite data/supplies, as applicable), cost/expense allocation (as applicable), and billing and payment schedules
- Disaster declaration (i.e., circumstances constituting a disaster, notification procedures)
- Site/facility priority access and/or use
- Site availability
- Site guarantee
- Process to negotiate extension of service
- Guarantee of compatibility
- IT system requirements, including any special needs
- Security requirements
- Staff support provided/not provided
- Facility services provided/not provided
- Testing, including scheduling, availability, test time duration, and additional testing, if required
- Records management (onsite and offsite), including electronic media and hardcopy
- Service level management (specify performance measures and service levels or quality of IT service provided)
- Workspace requirements as applicable (desks, telephones, PCs, chairs, etc.)
- Supplies provided/not provided
- Additional costs not covered elsewhere
- Other contractual issues, as applicable
- Other technical requirements, as applicable.

Recommended sections of the agreement include:

- Listing of other clients subscribing to same resources and site
- Contract/agreement change or modification process
- Contract/agreement termination conditions

- Change management and notification requirements, inclusive of hardware, software, and infrastructure

2.2.1.5 Equipment Replacement

Recovery strategies must consider damage or destruction of IT systems or unavailability of the primary site. Necessary hardware and software will need to be acquired and/or activated quickly at the alternate location. The following are the basic strategies considered in addressing equipment replacement:

- Vendor Agreements – As the IT DRP is being developed, SLAs with hardware, software, and support vendors may be made for emergency maintenance and replacement services. These agreements should stipulate what priority status the organization will receive in the event of a catastrophic disaster involving multiple vendor clients. The SLAs should be maintained and filed as an appendix to the IT DRP.
- Equipment Inventory – To simplify the process of acquiring compatible IT replacement equipment, the DRP should contain an inventory of IT equipment, its function, and its configuration. Required equipment may be purchased in advance and stored at an offsite location. An obvious drawback to this is the financial commitment to equipment that may never be used. This equipment will also need to be refreshed on the same schedule as the primary system's equipment.
- Existing Compatible Equipment- Equipment currently housed and used by the contracted hot site or another agency or system may be designated for use in a disaster situation. Agreements between organizations must specify that compatible equipment will be available for disaster recovery use by the organization.

2.2.1.6 Roles and Responsibilities

A Disaster Recovery Team (DRT) (or teams) must be selected, trained, and ready to deploy in the event of a disruptive situation requiring plan activation. Team members must understand their role on the team and the procedures necessary to execute the DRP. Each team must have a team leader that directs overall activities and keeps appropriate management briefed.

Planners should understand that some or even most of the DR team members could be unavailable in the event of an emergency. The line of succession to identify personnel responsible to assume authority for executing the IT disaster recovery plan in the event key designated staff are unavailable or unable to do so should also be determined and included in the plan.

2.2.2 Develop IT Disaster Recovery Plan

This section describes statewide guidance regarding the expected contents of an IT disaster recovery plan. IT Disaster Recovery plans should contain a supporting information section that documents conceptual and background information relevant to

document development. These details should provide context that aids in understanding, implementing, and maintaining the plan. Information should be presented in a clear and concise manner. The subsections below provide an example of the contents for this section.

2.2.2.1 Section 1: Introduction

The introduction section orients the reader to the type and location of information contained in the plan. The following are suggested elements to be included in the introduction:

- Purpose. This sub-section documents the purposes and objectives of the plan.
- Applicability. This sub-section documents the organizations supported by the plan and identifies any related or supportive plans. Related plans, such as the BCP and the OEP and should be included as appendices to the plan. Sections 1.2 and 1.8 discuss these related plans.
- Scope. The scope states specifically what situations, conditions, and locations are covered by the plan, as well as identifying the target system. It also lists any assumptions made.
- References/Requirements. This sub-section identifies agency, state, or federal requirements for disaster recovery planning.
- Record of Changes. This sub-section documents how changes to the plan will be handled. The IT disaster recovery plan is a living document that is required to change to reflect system, operational, or organizational changes. It is recommended that a Record of Changes page similar to the one following the Table of Contents for this document be used for this purpose.
- Supporting Exhibits (Optional): This sub-section is included in the document if Section 1, the Introduction, requires additional background information, which, if included in the body of the supported sub-section would impact the document's clarity or flow.

2.2.2.2 Section 2: Concept of Operations

The agency's Concept of Operations explains:

- What should happen;
- When it should happen; and
- At whose direction

The Concept of Operations section should contain the following:

- The general sequence of actions before, during, and after the emergency situation.
- Roles and responsibilities of team members in specific detail. It is recommended that roles be assigned to team positions rather than by name as this reduces

confusion if the member is unavailable to respond and it also helps minimize changes to the plan in instances of staff turnover;

- A statement about when and how the emergency plan will be implemented;
- An organization chart; and
- Documentation of the line of succession to identify personnel responsible to assume authority for executing the IT disaster recovery plan in the event the designated person is unavailable or unable to do so.

2.2.2.3 Section 3: Notification and Activation

This section documents the initial actions taken once a system disruption or emergency has been detected or appears to be imminent.

2.2.2.3.1 Notification Procedures

Notification procedures that describe the methods to notify recovery personnel during business and non-business hours should be developed and documented. These procedures should also cover events with and without prior notification. Primary and alternate contacts must be included along with procedures to be followed if an individual cannot be contacted. While this section lists contacts by team position, an emergency contact list that identifies personnel by the team position, name, and contact information (e.g., home, work, cell, pager numbers, e-mail addresses, and home addresses) should be appended to the plan.

The type of information to be communicated to those being notified should also be documented in the plan.

Note: The State CIT's Office should always be contacted as part of the notification procedures.

2.2.2.3.2 Plan Activation

This section of an IT DRP documents decision criteria used to activate the plan. Activation should occur when the damage assessment indicates one or more of the activation criteria for the system are met. In most instances the Agency Chief Information Officer (CIO) or the IT Disaster Recovery Planning Coordinator will activate the plan. Activation of the plan may be based on, but not limited to, the following:

- Safety of personnel and/or extent of damage to the facility;
- Extent of damage to a specific system or systems;
- Ability to meet the agency's mission; and
- Anticipated duration of disruption in relation to Recovery Time Objective (RTO).

2.2.2.3.3 Damage Assessment

This section documents damage assessment procedures to quickly assess the nature and extent of the damage. Once the assessments are made, the appropriate team(s) should be

notified of the updated information and planned response to the situation using the procedures documented in the DRP. It is recommended that damage assessment checklists be developed for quick assessment of the facility, environment, and IT components (e.g., hardware, software, and telecommunications infrastructure). The damage assessment should include:

- Cause of the emergency or disruption
- Potential for additional damage or disruptions
- Area affected by the emergency
- Status of physical infrastructure (e.g., structural integrity of computer room, condition of electric power, telecommunications, heating, ventilation, and air-conditioning)
- Inventory and functional status of IT equipment
- Type and extent of damage to equipment or data
- Items requiring replacement
- Estimated time to restore normal services

A template for assessing damage is included in Appendix B. If the Agency does not have the expertise to perform the damage assessment in an efficient and timely manner the State CIT's office should be contacted. The State CIT's Office will determine who should be engaged to assess the damage.

2.2.2.3.4 Supporting Exhibits (optional)

This sub-section is included in the document if the Notification and Activation Phase requires additional background information, which, if included in the body of the supported sub-section would impact the document's clarity or flow.

2.2.2.4 Section 4: Recovery

Recovery activities begin once the plan has been activated and recovery team(s) mobilized. Recovery phase activities focus on disaster recovery measures to execute temporary IT processing capabilities, repair damage to the system, and restore operational capabilities at the original or new facility.

Recovery procedures must be documented in sequential format with step-by-step instructions to restore system components in a logical manner consistent with priorities identified in the BIA. The procedures should also indicate who is responsible for taking each action and document any coordination between activities. Because recovery procedures are likely to change frequently, it is recommended that recovery procedures and supporting exhibits be maintained as a separate document.

2.2.2.5 Section 5: Reconstitution

All IT disaster recovery plans should contain a section that provides procedures for a transition back to normal operations once the original system and facility is ready to

resume operational status. This part of the plan should be as detailed as the actual IT Disaster Recovery Plan itself. This should include designation of team(s) responsible for restoration activities that must include testing of necessary IT equipment and telecommunications connections. This section should also include the following components:

- Concurrent Processing Procedures. Procedures and responsibilities should be outlined, per necessary team, to operate the IT disaster recovery system in coordination with the recovered or reconstituted system at the original or new site. This should include specific procedures to address the following:
    - Testing of the recovered or reconstituted system to demonstrate readiness to resume operational status
    - Shutdown procedures for the disaster recovery system
- Plan Deactivation. The plan should include procedures for formally deactivating. These procedures should include procedures to include shutdown of the alternate site including retrieval of any materials, equipment, and backup media. It is recommended that a meeting of the DRT occur to debrief and identify lessons learned in conjunction with formal deactivation.

2.2.2.5.1 Supporting Exhibits (optional)

This sub-section is included in the document if the Reconstitution Phase requires additional background information, which, if included in the body of the supported sub-section, would impact the document's clarity or flow.

2.2.2.6 Section 6: Disaster Recovery Plan Appendices

Disaster Recovery Plan appendices contain key information referenced, or applicable to the main body of the plan. Disaster Recovery Plan appendices may include:

- Contact information for IT disaster recovery planning teams
- Vendor contact information
- Offsite storage information, including contact information and data retrieval procedures
- Standard operating procedures and checklists for system recovery, including configuration information and start up and shut down instructions for IT equipment
- Equipment inventory and system requirements including lists of hardware, software, firmware, and other resources required to support system operations, including model or version number, specifications, and quantity
- SLAs, MOUs, or MOAs
- Description of, and directions to, the alternate site
- The BIA and Risk Assessment conducted during the pre-planning phase

- Recovery strategies
- Related plans, such as the OEP or BRP
- Schedule listing when the plan was tested

2.3 Post Planning Phase

The Post Planning phase ensures that appropriate staff members are familiar with the plan. It also ensures that the plan is tested and maintained.

2.3.1 Awareness and Training Programs

Training and awareness programs are essential to a successful IT disaster recovery program. Personnel with recovery responsibilities should receive training at least annually. New personnel with plan responsibilities should receive training as soon as possible after they are identified. The goal of the training is to educate staff to the extent that they are able to execute their respective recovery procedures without aid of the actual DRP. The following elements should be covered in the training program:

- Purpose of plan
- Cross-team coordination and communication requirements
- Reporting procedures
- Security requirements
- Team and phase-specific processes (Notification/Activation, Recovery, and Reconstitution)
- Individual responsibilities in each phase

2.3.2 DRP Testing and Maintenance

The Assessment Checklist provided in Appendix C is designed to assist in determining whether an IT Disaster Recovery Plan meets the standards set forth in these guidelines. The checklist is not the only method that should be utilized for evaluating a plan. A reviewer should use their judgment in assessing the adequacy of the documentation and the available review time should determine the amount of "proof" required for each question.

Plan testing is an essential element of a viable IT disaster recovery capability. The first benefit of testing the DRP is that it provides an opportunity to train personnel to execute the plan. Without practice, the key staff may have no idea what their roles are within the DRP.

Secondly, periodic testing is important because it validates the effectiveness of the backup and recovery procedures. One of the key elements of a successful DRP is the ability of the recovery team to locate a current copy of the core data to replicate. If the backup and recovery activities used in the data center are not effective or fail to comply with the requirements of the BIA, a DRP test will very quickly indicate this shortcoming.

The third importance of testing is not that the test succeeds without problems, but that you review the test results and problems encountered and use these results to update or revise the current procedures and plans.

Many agencies do not have the resources to performing a full recovery with system downtime. A total system test is ideal. If a total system test cannot be performed, individual sections or sub-systems of the DRP may be tested separately in order to confirm the recoverability of the plan as a whole. Thorough testing should include the following:

- System recovery on an alternate platform from backup media
- Coordination among recovery teams
- System performance using alternate equipment
- Restoration of normal operations
- Notification and activation procedures

Test results should be documented, reported to senior management, and kept on file. The IT Disaster Recovery Plan is a living document and the maintenance of the plan should be included in the general business plan. It must be updated regularly to remain viable based on the most current system architecture or environment. Each IT Disaster Recovery Plan must document plan maintenance procedures and responsibilities. This should include reassessment of the plan at least annually and a process to update the plan to reflect changes in hardware, software, and personnel.

Appendix A: IT Disaster Recovery Planning Considerations

This section complements the main body of this document by providing technical considerations for IT systems. All IT disaster recovery-planning procedures and recovery solutions should be consistent with and support State security policies. IT Disaster Recovery solutions should offer the same level of security as the normal operating procedure so that sensitive data is not compromised or disclosed.

Because each system is unique, the Disaster Recovery Planner must assess each system using the results of the BIA to determine the appropriate recovery solutions. The items below are not intended to be an all-inclusive list of considerations, but rather to provide solid examples of considerations that can be expanded and customized as specific technical environments dictate.

- Hardware
  - Documented configurations
  - Vendor contact information
  - Minimum system requirements
- Software
  - Vendor contact information
  - Customized software applications
  - Commercial Off the Shelf (COTS)
- Communications
  - Internal
  - External
  - Cabling
  - Remote Access
- Back-up Data
  - Off site storage
  - Types of backups
  - Frequency of backups
- Redundant Solutions
  - Disk replication
  - Redundant Array of Independent (or Inexpensive) Disks (RAID)
  - Virtual Tape Libraries
  - Network Attached Storage (NAS)
  - Storage Area Network
  - Redundant communication links
- Local Area Networks
  - Physical Diagram
  - Logical Diagram
- Wide Area Networks
  - Contact information for service providers
- Physical Facility
  - Space
  - Power

    - HVAC
    - Accessibility
    - Vendor Support
- Inter-Agency Support
- Personnel
    - Accurate recall lists
    - Multiple contacts
    - Skill sets
- Security
- Emergency Purchase Orders

Appendix B: Sample Damage Assessment Template

1. Cause of emergency or disruption
2. Potential for additional damage or disruptions
3. Status of physical infrastructure (e.g., structural integrity of computer room, electric power, telecommunications, HVAC, etc.)
4. Estimated time to restore normal services

Inventory Item	**Functional (Y/N)**	**Requires Replacement (Y/N)**	**Type of Damage**
Note: Should be pre-filled			

Appendix C: Assessment Checklist

	N/A	IP	Yes	No
Pre-Planning Phase				
1. Has the IT Disaster Recovery plan been integrated with other applicable plans (e.g., Business Continuity or Resumption Plan, Occupant Evaluation Plan, etc.)? (Reference 1.7)				
2. Has the Agency Head ensured that the disaster recovery planning policies and procedures are consistent with State Policy? (Reference 1.8)				
3. Has the Agency Head ensured the development of a disaster recovery plan that documents how business functions will be performed in the event that their IT systems are unavailable (short and long-term unavailability)? (Reference 1.8)				
4. Are all vendors/contractors aware that they must comply with the Disaster Recovery Planning Guidelines? (Reference 1.8)				
5. Is the access to the Disaster Recovery plan restricted to only the appropriate personnel? (Reference 1.9)				
6. Have the Business Owners defined recovery priorities based on the information from the BIA, RTO, and RPO? (Reference 2.1)				
7. Has a BIA been conducted? (Reference 2.1.2)				
8. Have the Business Owners completed or assisted in the completion of a BIA? (Reference 2.1.1)				
9. Have the Business Owners defined the maximum amount of tolerable downtime (recovery time objective) for each of the functions identified in the BIA? (Reference 2.1.1).				
10. Does the BIA identify business functions that are necessary to carry out State or Agency missions and mandated functions? (Reference 2.1.1)				
11. Does the BIA identify the RTO and RPO for each business function? (Reference 2.1.1)				
12. Does the BIA identify the hardware resources needed to support the business functions? (Reference 2.1.1)				
13. Does the BIA identify the software resources needed to support the business functions? (Reference 2.1.1)				
14. Does the BIA identify all other resources needed to support the business functions? (Reference 2.1.1)				
15. Has a Risk Assessment been performed on each IT system identified in the BIA? (Reference 2.1.2)				
16.				
17. Does the Risk Assessment document risks and identify the threats to the business functions? (Reference 2.1.2)				
18. Has an analysis been performed for each risk identified to determine the likelihood and impact of occurrence? (Reference 2.1.2).				
19. Have controls that mitigate or eliminate the risks identified in the above steps been developed? (Reference 2.1.2)				
20. Have controls that mitigate or eliminate the risks identified in the above steps been implemented? (Reference 2.1.2)				
21. Have the implemented controls reduced the level of risk to the				

	N/A	IP	Yes	No
systems to an acceptable level? (Reference 2.1.2)				
22. Has a high-level Agency Official signed off acknowledging the existence and acceptance of the residual risks? (Reference 2.1.2)				
Planning Phase				
23. Have recovery strategies been developed and documented for the technical components that support business functions as identified in the BIA? (Reference 2.2)				
24. Does the Disaster Recovery Plan (DRP) document the recovery strategies? (Reference 2.2.1)				
25. Does the DRP document system backup procedures? (Reference 2.2.1.1)				
26. Does the DRP specify the backup frequency? (Reference 2.2.1.1)				
27. Does the DRP designate the retrieval procedures of the stored data? (Reference 2.2.1.2)				
28. Does the DRP designate an off-site storage location for the backup of data? (Reference 2.2.1.3)				
29. Does the DRP provide a description of the off-site storage facility? (Reference 2.2.1.3)				
30. Is the off-site storage facility accessibly 24 X 7 X 365? (Reference 2.2.1.4)				
31. Does the DRP specify how equipment will be replaced? (Reference 2.2.1.4)				
32. Has a disaster recovery team been defined? (Reference 2.2.1.6)				
33. Has the disaster recovery team been adequately trained? (Reference 2.2.1.6)				
34. Has the DRP considered a scenario where a majority of the designated disaster recovery personnel will be unavailable? (Reference 2.2.1.6)				
35. Does the DRP clearly identify a line of succession to assume authority for executing the disaster recovery plan in the event key designated staff is unavailable? (Reference 2.2.1.6)				
36. Does the DRP supporting information “Introduction” section include the following information? (Reference 2.2.2.1) • Purpose • Applicability • Scope • References/Requirements • Record of Changes				
37. Does the DRP provide a sequence of action before, during, and after an emergency? (Reference 2.2.2.2)				
38. Does the DRP supporting information “Notification and Activation” section include the following information (Reference 2.2.2.3): • Notification Procedures • Plan Activation • Damage Assessment				
39. Do the notification procedures describe the methods for notifying recovery personnel during both business and non-				

	N/A	IP	Yes	No
business hours? (Reference 2.2.2.3.1)				
40. Do the notification procedures designate both primary and secondary contacts? (Reference 2.2.2.3.1)				
41. Does the plan activation section detail the decision criteria used to activate the plan? (Reference 2.2.2.3.2)				
42. Have damage assessment checklists been developed for quick assessment of the facility, environment, and IT components? (Reference 2.2.2.3.3)				
43. Do the recovery procedures sequentially document step-by-step instructions to restore system components in a logical manner consistent with priorities? (Reference 2.2.2.4)				
44. Do the reconstitution procedures detail testing and cutover back to the primary facility? (Reference 2.2.2.5)				
45. Do the plan appendices include the following (Reference 2.2.2.6): • Contact information for recovery teams • Vendor contact information • Offsite storage information • Standard operating procedures • Equipment and system requirements • SLAs, MOUs, or MOAs • Description of, and directions to, the alternate site • The BIA and Risk Assessment • Related plans, such as the OEP or BRP				
Post Planning Phase				
46. Are training and awareness programs in place for educating personnel on the disaster recovery plans? (Reference 2.3.1)				
47. Does the training and awareness program include the following (Reference 2.3.1): • Purpose of the plan • Cross-team coordination • Reporting procedures • Security requirements • Team and phase-specific processes				
48. Is the disaster recovery plan tested? (Reference 2.3.2)				
49. Does the testing include the following: (Reference 2.3.2) • System recovery on an alternate platform from the backup media • Coordination among recovery teams • System performance using alternate equipment • Restoration to normal operations • Notification and activation procedures				
50. Is the disaster recovery plan updated regularly? (Reference 2.3.2)				

N/A – Not Applicable
IP – In Progress

Appendix D: Glossary

The following words and terms, when used within this document, shall have the following meanings:

Activation: When all or a portion of the recovery plan has been put into motion.
Agency-Wide: A policy or function applicable to the entire agency and not just one single department.

Alternative Site: A location, other than the normal facility, used to process data and/or conduct business functions in the event of a disaster. ***SIMILAR TERMS***: Alternate Processing Facility, Alternate Office Facility, And Alternate Communication Facility.

Application System - A series of automated processes in full production that serve the needs of some part or all of an agency.

Assumptions: Basic understandings that the disaster recovery plan are based on.
Back Office Location: An office or building, used by the organization to conduct support activities, that is not located within an organization's headquarters or main location.

Backup: An alternate source or resource to be used in the event the primary resource is no longer available for use.

Business Continuity Planning (BCP): An all-encompassing, "umbrella" term covering both disaster recovery planning and business resumption planning. Also see disaster recovery planning and business resumption planning.

Business Impact Analysis: The process of analyzing all business functions and the effect that a specific disaster may have upon them.

Checklist Test: A method used to test a completed disaster recovery plan. This test is used to determine if the information such as phone numbers, manuals, equipment, etc. in the plan is accurate and current.

Cold Site: An alternate facility that is void of any resources or equipment except air-conditioning and raised flooring. Equipment and resources must be installed in such a facility to duplicate the business functions of an organization. Cold-sites have many variations depending on their communication facilities, UPS systems, or mobility. ***SIMILAR TERMS***: Shell-site; Backup site; Recovery site; Alternative site.

Communications Failure: An unplanned interruption in electronic communication between a terminal and a computer processor, or between processors, as a result of a failure of any of the hardware, software, or telecommunications components comprising the link. (Also refer to Network Outage.)

COOP: Continuation of Operations Plan. The operations piece of business continuity planning ***SIMILAR TERMS***: Business Resumption Planning and Disaster Recovery Planning

Crisis: A critical event, which, if not handled in an appropriate manner, may dramatically impact an agency's reputation or ability to operate.

Damage Assessment: The process of assessing damage, following a disaster, to computer hardware, network components, office facilities, etc. and determining what can be salvaged or restored and what must be replaced.

Data Center Recovery: The component of Disaster Recovery which deals with the restoration, at an alternate location, of data centers services and computer processing capabilities. ***SIMILAR TERMS***: Mainframe Recovery.

Data Center Relocation: The relocation of an organization's entire data processing operation.

Dedicated Line: A pre-established point-to-point communication link between computer terminals and a computer processor, or between distributed processors, that does not require dial-up access.

Disaster: Any event that creates an inability to provide services for some predetermined period of time. ***SIMILAR TERMS***: Business Interruption; Outage; Catastrophe.

Disaster Recovery: The ability to respond to an interruption in services by implementing a disaster recovery plan to restore an organization's business functions.

Disaster Recovery Manager (DRM): The individual responsible for coordinating and documenting recovery activities and tracking recovery progress.

Disaster Recovery Period: The time period between a disaster and a return to normal functions, during which the disaster recovery plan is employed.

Disaster Recovery Plan (DRP): The document that defines the resources, actions, tasks and data required to manage the recovery process in the event of a service interruption or failure.

Disaster Recovery Planning: The technological aspect of business continuity planning. The advance planning and preparations that is necessary to minimize loss and ensure continuity of the business functions of an organization in the event of disaster. ***SIMILAR TERMS***: Contingency planning; business resumption planning; corporate contingency planning; business interruption planning; disaster preparedness.

Disaster Recovery Team (DRT): A group of individuals responsible for directing the development and on-going maintenance of a disaster recovery plan. This team is also tasked with providing direction during the recovery process.

Electronic Vaulting: Transfer of data to an offsite storage facility via a communication link rather than via portable media. Typically used for batch/journal updates to critical files to supplement full backups taken periodically.

Emergency: A sudden, unexpected event requiring immediate action due to potential threat to health and safety, the environment, or property.

Extended Outage: A lengthy, unplanned interruption in system availability due to computer hardware or software problems, or communication failures.

Facilities: A location containing the equipment, supplies, voice and data communication lines, to conduct transactions required to conduct business under normal conditions. ***SIMILAR TERMS***: Primary Site, Primary Processing Facility, And Primary Office Facility.

File Backup: The practice of dumping (copying) a file stored on disk or tape to another disk or tape. This is done for protection in case the active file gets damaged and data must be restored.

File Recovery: The restoration of computer files using backup copies.

File Server: The central repository of shared files and applications in a computer network (LAN).

Hot site: An alternate facility that has the equipment and resources to recover the business functions affected by the occurrence of a disaster. Hot-sites may vary in type of facilities offered (such as data processing, communication, or any other business functions needing duplication). Location and size of the hot-site will be proportional to the equipment and resources needed. ***SIMILAR TERMS***: Backup site; Recovery site; Recovery Center; Alternate processing site.

Interruption: An outage caused by the failure of one or more communications links with entities outside of the local facility.

LAN (Local Area Network): Computing equipment, in close proximity to each other, connected to a server that houses software that can be accessed by the users. This method does not utilize a public carrier. SEE ALSO WAN.

Loss: The unrecoverable business resources that are redirected or removed as a result of a disaster. Such losses may be, public image, facilities, or operational capability.

Loss Reduction: The technique of instituting mechanisms to lessen the exposure to a particular risk. Loss reduction is intended to react to an event and limit its effect. Examples of Loss Reduction include sprinkler systems, insurance policies, and evacuation procedures. ***SIMILAR TERM***: Risk Mitigation Strategy

Mission Critical Components: Business activities or information that could not be interrupted or unavailable for several business days without significantly jeopardizing operation of the organization.

Network Architecture The basic layout of a computer and its attached systems, such as terminals and the paths between them.

Network Outage: An interruption in system availability as a result of a communication failure affecting a network of computer terminals, processors, or workstations.

Outsourcing: The transfer of performing certain functions to an independent third party.

Record Retention: Storing historical documentation for a set period of time, usually mandated by state and federal law or the Internal Revenue Service.

Recovery Action Plan: The comprehensive set of documented tasks to be carried out during recovery operations.

Recovery Process: The critical path followed during a recovery effort. This process is documented in the disaster recovery plan.

Recovery Team: SEE Disaster Recovery Team.

Recovery Time: The period from the disaster declaration to the recovery of the functions.

Risk Assessment/Analysis: The process of identifying and minimizing the exposures to certain threats, which an organization may experience. ***SIMILAR TERMS****:* Risk Assessment; impact assessment; corporate loss analysis; risk identification; exposure analysis; exposure assessment.

Risk Management: The discipline that ensures that an organization does not assume an unacceptable level of risk.

Scheduled Systems Downtime: A planned interruption in system availability for scheduled system maintenance.

Simulation Test: A test of recovery procedures under conditions approximating a specific disaster scenario. This may involve designated units of the organization actually ceasing normal operations while exercising their procedures.

Structured Walk-Through Test: Team members walk through the plan to identify and correct weaknesses.

System Outage: An unplanned interruption in system availability as a result of computer hardware or software problems, or operational problems.

Test Plan: The recovery plans and procedures that are used in a systems test to ensure viability. A test plan is designed to exercise specific action tasks and procedures that would be encountered in a real disaster.

WAN (Wide Area Network): Like a LAN, except that parts of a WAN are geographically dispersed, possible in different cities or even on different continents. Public carriers like the telephone company are included in most WANs; a very large one might have its own satellite stations or microwave towers.

Warm Site: An alternate processing site which is only partially equipped (as compared to Hot Site which is fully equipped).