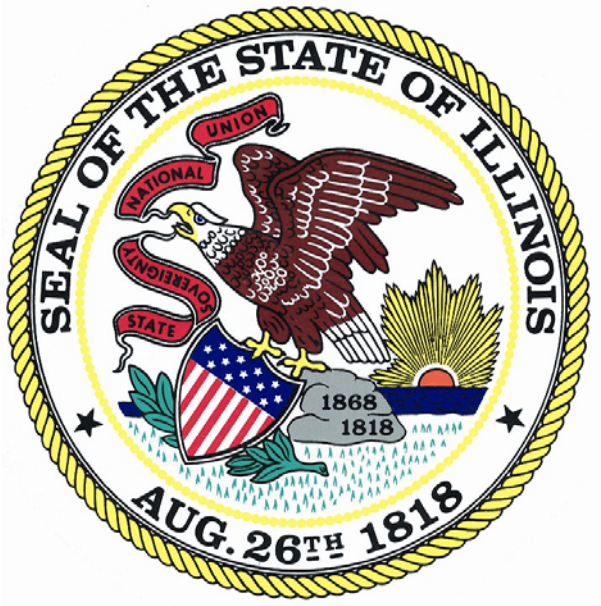

State of Illinois
Department of Central Management Services
Bureau of Communication and Computer Services

Recovery Methodology

Effective date: January 01, 2010

Central Management Services
Bureau of Communication and Computer Services
RECOVERY METHODOLOGY

TABLE OF CONTENTS

This page intentionally left blank

REVISION HISTORY

Revisions to this methodology will be tracked by the Recovery Services Manager. The Recovery Services Manager also reserves the right to decide when substantial modifications require management staffing for review and subsequent signature.

Amendment Date	Amendment Description	Section Modified	RMT member initials
12/11/08	Major Revisions, Continuity references changed to Recovery, Title Page, Signature Page, Reference to the Information management System removed, replaced Business Impact Analysis Appendix, Removed reference to document that are outside the scope of this document.. Recovery Management Team structure revised		SI
02/27/2009	Clarifications to section 2.2.6		SI
05/26/09	Audit Corrective Action Review	Entire	RCD

FOREWORD

ACKNOWLEDGMENTS

The decisions, processes, and procedures contained within are based on industry best practices as recommended by the Disaster Recovery Institute International's (DRII) Professional Practices for Business Continuity Planners. The *National Incident Management System* (NIMS) is also referenced to help provide a consistent nationwide template to enable Federal, State, tribal, and local governments, nongovernmental organizations (NGOs), and the private sector to work together to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity. This consistency provides the foundation for utilization of NIMS for all incidents, ranging from daily occurrences to incidents requiring a coordinated Federal response. The directive requires Federal departments and agencies to make adoption of NIMS by State, tribal, and local organizations a condition for Federal preparedness assistance (through grants, contracts, and other activities).

SCOPE

This methodology addresses recovery of information processing capabilities only. Recovery will be addressed only after the health and safety of Illinois citizens and state staffs have been secured. This methodology does not address the Business Continuity Plan (BCP) which focuses on sustaining an organization's business functions during and after an emergency. To the extent that the key business functions depend on information processing capability, the BCP may refer to this methodology. This methodology does not address the Continuity of Operations (COOP) plan which addresses specific facility level and organizational level contingency planning. Please refer to the National Institute of Standards and Technology (NIST) Special Publication, SP 800-34, "Contingency Planning Guide for Information Technology Systems", Table 2-1 for the contents of typical BCP, COOP and other related plans. Please refer to the Federal Emergency Management Agency (FEMA) Guidance FPC 65, "Federal Executive Branch Continuity of Operations" for guidance on COOP.

ASSUMPTIONS

1. Health, safety, and emergency response concerns have been addressed.
2. Public Authorities (Police, Fire, IEMA, FEMA, etc.) will be in charge until safety issues are resolved.
3. Official Declaration of Disaster has been made by the President of the United States, Governor of Illinois, IEMA, FEMA, or CMS/BCCS Management.
4. In the event a disruption affects more than one agency (e.g. a regional disaster), the Governor's Office and/or the Department of Central Management Services will establish priorities and direct statewide recovery efforts.
5. All CMS/BCCS employees are deemed essential. Employee availability will be determined at time of disaster.
6. All public relations and crisis management activities (discussion with news media, emotional stress of employees, etc.) are to be coordinated through the Director's Office or CMS Information Services.

7. A recovery processing facility will be available, although it may not be the primary recovery site. A business continuity / disaster recovery contract is available and current, providing vendor supplied recovery services.
8. The off-site storage facility is unaffected and therefore able to deliver backup resources to the recovery facility.
9. CMS/BCCS executive management actively supports recovery efforts through allocation of resources, review of recovery services plan documents, exercise rehearsal plans, and exercise results, awareness campaign to stakeholders of policy, service, need to maintain critical IT application recovery procedures, the need for a well-developed and rehearsed recovery plan, and funding of vendor services.

PURPOSE

This methodology provides direction and recommendations to produce effective and detailed instructions necessary to recover critical information processing systems and services in order to reduce the consequences of a disruption to acceptable levels.

Key Objectives:
1. Minimize disruption effects, minimize damage and losses.
2. Continue to meet the agency's mission; continue to provide services to the citizens of the state.
3. Assist in determining critical systems, functions, communications, services, and recovery time objectives (RTO).
4. Assign responsibility, define procedures, facilitate effective coordination of recovery efforts, and provide guidelines for decisions, in advance, in order to resume critical processing as quickly and effectively as possible.

1. PLANNING, ADMINISTRATION, & COORDINATION

1.1. Justification

A well-developed and practiced recovery plan expedites the recovery process to ensure critical systems and services continue to be provided. Operational readiness is reinforced through recovery planning efforts. In addition, federal and/or state legislated mandates require business continuity and recovery services planning.

1.2. Authority

Effective recovery planning requires executive management support since recovery efforts affect multiple organizational units within the agency. Approval by agency executive management (the director, internal auditors, etc.) elevates the methodology to policy level.

1.3. Recovery Services Management

Continuity and recovery planning is an iterative process - ***not*** a onetime effort – ***not*** an annual event or project. It must be an on-going commitment in order to reflect current, up-to-date operational environments and business needs.

To be effective, a team should be appointed with responsibility of ensuring that changes to the recovery information are reflected in a timely manner. CMS/BCCS has a dedicated Recovery Services unit in the Security and Compliance Solutions Division that is responsible for overseeing the maintenance of this process. In addition, CMS/BCCS Recovery Management Team members are the management-designated leaders for their appointed area of expertise. As such, they are responsible for the accuracy and completeness of the information pertaining to their area contained within relevant recovery information.

1.4. Change Management

Agency internal procedures need to be developed, documented, and disseminated throughout the agency in order to keep recovery processes current when systems or software is upgraded; when personnel change; when critical business functions change; when major functions change locations; etc.

General change management activities related to updating the contents of the recovery information are provided in the Maintenance section of this methodology. CMS/BCCS standard operating procedures for providing change notification to Recovery Services are as follows:

1. All changes are entered and tracked through the BMC Remedy Service Management system.
2. Recovery Services is notified of the weekly coordinator meetings where all changes affecting the facilities are discussed. Any changes that may require modification of the continuity plan are noted.

1.5. Budget/Recovery Costs

Known business continuity costs should be appropriated through normal fiscal and budgeting processes. Costs may include, but are not limited to those associated with backup media, exercising plans, transportation, accommodations, communication, equipment, personnel, etc. At time of recovery, emergency procurements procedures may be followed.

The following is a list of information technology and recovery contracts required for effective recovery capabilities:

5. recovery services of information technology infrastructure 'cold/warm/hot' site recovery,
6. off-site vaulting of backup media,
7. off-site remote recovery work facility,
8. hardware/software/tools/system components/service, and
9. network systems/service.

2. BUSINESS IMPACT ANALYSIS (BIA)

2.1. BIA Goal & Objectives

A Business Impact Analysis (BIA) assists agency management in determining the amount of resources to commit in order to prevent or reduce loss from a negative event. The effects of a loss should be expressed in quantitative terms (dollars, number of clients served, punitive damages, etc.) if possible or in qualitative terms (public confidence, image, service deliverables, etc.).

Specific objectives of a BIA include:

1. Identifying major risks, that could cause a failure to meet agency objectives, and documenting associated controls that mitigate or lessen the agency's vulnerability;
2. Assessing the impact of a negative event based on the agency's mission and legislated mandates;
3. Identifying critical business resources (functions, processes, systems, services, personnel) etc. that support the agency's mission and enable meeting legislated mandates and expected levels of service; and
4. Determining the time criticality (recovery time objective) for each critical resource identified above (recovery time objective is the maximum length of time that can elapse before the unavailability of the resource becomes unacceptable and places the agency at risk of failing to meet their mission).

2.2. BIA Development

The objectives listed above are recommended for use in the development of an organizationally unique BIA. A sample BIA provides a framework for collecting the information discussed in this section.

A Sample Business Impact Analysis form is provided in Appendix A.

2.2.1. Major Risks and Mitigating Controls

Identifying risks aids in instituting controls that mitigate adverse effects of a disruption. Evaluating the overall effectiveness of a mitigating control in conjunction with the risk probability establishes the vulnerability exposure to a given risk.

2.2.1.1. Major Risks:

- Natural: tornado, earthquake, rain/flood, and lightning strikes, fire.
- Man-Made: cable cuts, chemical/toxic spill, natural gas leak/explosion, asbestos, broken water pipe, fire (arson and accidental), strikes, riots, terrorism, bomb threat/detonation, vandalism/theft, sabotage, disgruntled staff, intruder, fraud/embezzlement.
- Proximity: (surrounding neighbor's or essential supplier disruption) nearby an airport, armed service's ammunition depot, railroad, etc.

2.2.1.2. Mitigating Controls:

Mitigating controls are specific policies, procedures, practices, etc. that reduce either the probability of occurrence OR the negative impact of an occurrence.

See Additional Mitigating Risks and Controls in Appendix B.

2.2.2. Impact Assessment

The consequence of a negative event should be assessed in terms of its effect on each agency function and service. The assessment should be expressed in degrees of **maximum**, **minimum**, or **inconsequential** regarding the correlation to meeting the agency's mission and mandates.

2.2.3. Agency Mission

Review the agencies mission to ensure the BIA is addressing goals and objectives of the agency's mission.

2.2.4. Legislative, Regulatory, Statutory Mandates

Legislated, regulatory, statutory mandates (due dates, time restraints, penalties, etc. to be used in establishing Recovery Time Objectives) for major agency functions and services should also be addressed in the BIA.

2.2.5. Critical Resource Identification

As a result of completing the impact assessment, all agency functions and services can be ranked as to the importance relative to meeting the agency's mission and should be assigned a value based on quantitative or qualitative criteria.

Recovery priority determines the order in which resources are restored and the extent to which alternate restoration methods are/will be applied. As an example, if only one person is knowledgeable in restoring the operating system and that person is not available during recovery, the agency may need to contract with key vendors (IBM, HP, Microsoft, software providers, etc.) to complete this task, which is essential for all other software recoveries.

In the event a disruption affects more than one agency (e.g. a regional disaster), the Governor's Office and/or the Department of Central Management Services will use the agency's recovery priority values found in the Business Reference Model (BRM) application as a starting point in directing statewide recovery efforts.

CMS/BCCS uses two major criteria for determining the recovery order of supported critical applications – State-Wide Recovery Category and Recovery Stage. These are explained in detail below.

2.2.5.1. HUMAN SERVICE IMPACT (also known as State-Wide Recovery Categories):

As approved by the Governor's Office, the following categories will determine the order in which applications will be recovered in the event multiple agencies are competing for limited recovery resources. The final decision as to which resources are recovered first in a regional/multi-agency recovery will be made by the Governor's Office and/or CMS.

HUMAN SAFETY: (Category One)
Resources that directly impact the lives and safety of Illinois citizens, including state employees.
Examples: Police, Fire, Medical, Corrections, Child Welfare, etc...

WELFARE HUMAN SERVICE: (Category Two)
Resources that directly impact the well-being of Illinois citizens.
Examples: Assistance, Benefits, Vital Records, etc...

NON-WELFARE HUMAN SERVICE: (Category Three)

A human service resource that indirectly impacts the welfare of Illinois citizens. Examples: Registries, Licensure, Tracking, Vendor related, etc...

ADMINISTRATIVE STATE FUNCTIONS & PROCESSES: (Category Four)
Resources that support the administration of state processes.
Examples: Payroll, Compensation, Procurement, Accounts Payable, etc...

SUPPORT OF SPECIFIC AGENCY FUNCTIONS & PROCESSES: (Category Five)
Resources related to the maintenance of a specific agency function or process. Examples: Laboratory, Utilities, Diagnostics, Statistical systems, Application Code Tools, etc.

2.2.6. Recovery Time Objective (RTO)

RTO is the maximum length of time the agency can be without a resource before the agency mission or mandate is severely impacted. When figuring the RTO, dependencies on outside entities should be included and counted as the length of time the entity takes to complete their portion of the function under normal operations.

Assignment of an RTO to each major resource:

1. establishes a recovery timeline for each resource (when recovery *must* begin);

2. determines the maximum amount of time that can elapse before the agency must decide whether to declare a disaster to alert any third-party vendor of the possibility of use of recovery services.

As an example, if a federal mandate requires weekly submission of a report – or the agency can be assessed severe financial penalties - then the maximum RTO for delivering that report would be one week. However, if the report (or computer tape) must be mailed, then the RTO becomes 5 days because you must account for and allow time for mailing. If, in addition, it takes a day to review the report and write a commentary on the results, then the RTO for producing the report is reduced to 4 days.

2.2.6.1. Recovery Stages

CMS restores IT processing in a phased, orderly approach referred to as stages. Stage is defined as a numerical value ranging from 0 to 2 representing the recovery phase (tier, order, priority) in which the business function will be restored. Because an IT capability is linked to a business function, the stage of the business function is the recovery priority of the IT capability.

A recovery time objective (RTO) must be assigned to each business function in order to assign a recovery stage to that business function. The RTO is assigned based on impact (as identified in a business impact analysis) and the risk level (as identified in a risk assessment).

Listed below is the recovery time objective (RTO) for each stage.

RTO in Hours	Recovery Stage
0 to 72	Stage 0
72 to 168	Stage 1
>168	Stage 2

2.2.6.2. Recovery Order

The sequences in which applications are recovered are determined by the Stage and Category applied to the application.

The first applications to be recovered are the Stage 0 and they are recovered in order of Category, Category one (1) being the first, and Category two (2) being second and so on. After all Stage 0 applications are recovered, Stage 1 applications will be recovered with Category 1 being the first, Category 2 being the next and so on.

Thus a Stage 0 Category 2 would be recovered before a Stage 1 Category 1.

According to this schema, it is anticipated that all stage 2 applications will be recovered when normal information technology processing is resumed.

3. DISRUPTION LEVELS

The level of disruption determines which recovery actions are followed and the amount of agency and non-agency effort is assigned to recovery efforts. Disruption level criteria are based on a combination of estimated time to recover and extent of damage.

3.1. Minor

Effect: Processing capability damaged

Suggested solution: Even though there may be a partial outage there is a work around to address the problem while it is being resolved. An example would be a hardware equipment problem requiring replacement of a component. Standard operating procedures will maintain processing of category one critical applications if possible while repair to the damaged component is underway.

Recovery Plan usage: In this type of instance a recovery plan would probably not be activated.

Time*: Less than 12 hours.

3.2. Major

Effect: Facility inaccessible

Suggested solution: The current configuration would require the CMS computing facility to run in a diminished state, if possible, allowing only category one critical applications to process for the prescribed period of downtime.

Recovery Plan usage: Instigating a plan is a possibility, but normally not necessary.

Time*: More than 12 hours and less than 72 hours.

3.3. Catastrophic

Effect: Facility lost

Suggested solution: Upon discovery of the event, CMS/BCCS Recovery Services may place the recovery services provider and CMS RMT on alert status. Once initial damage assessment has been completed or a full and proper disaster declaration made by an authorized entity, the category one critical applications would be moved to the recovery services provider recovery center for an unspecified period of time.

Recovery Plan usage: A plan will more than likely be activated.

Time*: 72 hours or more from point of official declaration.

** Time refers to time estimated to return to normal processing. These times are for illustration purposes only.*

4. RECOVERY PLANNING

The following section provides guidelines to facilitate recovery decisions.

4.1. Contents/Elements

Recovery planning should include but is not limited to:

1. Immediate Response which includes initial/preliminary actions, alert notifications, event notification, initial declaration for continuity plan activation, activation of the Recovery Management Team, initial damage assessment;
2. Secondary Response which includes notification of the full recovery team, perform detailed damage assessment;
3. Declaration which includes recovery strategies and official notification of declaration to state entities, governor's office;
4. Relocation which includes movement of equipment, people, data, etc.;
5. Resumption which includes recovery functions, restoration of systems and data;
6. Migration which includes movement to an interim or permanent site;
7. Synopsis/Evaluation which is a summary of all recovery efforts;
8. Exercise which includes actions taken to validate the plan, and
9. Supporting Documentation – revision of recovery plans and process.

4.2. Recovery Packets

Recovery packets should be developed for each environement/application that will be recovered. The packets contain detailed, technical instructions to aid the recovery of the restored services. They may contain the following:

1. the remote host system basic configuration,
2. remote access to the system console,
3. Virtual Private Network (VPN) access from the recovery command center to the remote host,
4. the remote host service provider contacts,
5. the remote host site network equipment configuration for LAN access and VPN,
6. and contacts for the technical specialists.

As an example, a high-level list of the major tasks follows for restoring a mainframe infrastructure:

1. Initialize Storage
2. Configure Network equipment
3. Restore Operating System and associated components
4. Modify Operating System parameters
5. Initial Program Load (IPL)
6. SYNC POINT
7. Functional verification of operating systems

8. Confirm Network Connectivity
9. SYNC POINT
10. Contact Customers
11. Verify Customer Restoration
12. Verify Restored Services
13. Completion SYNC POINT 1

4.3. Pre-Planning Actions and Decisions

Pre-planning enhances the effectiveness and timeliness of recovery efforts by reducing time and effort spent on selecting a course of action or determining specific tasks. The list of pre-planning issues includes:

1. Distribution of the agency escalation policy/procedure so staff are aware of notification procedures in case of a disruption or significant event.
2. Identification of possible recovery command center locations/sites.
3. Identification and coordination of recovery teams.
4. Creation of a specification of minimum configuration requirements for a new location. This should include but not limited to the following: geographical location, security, floor space, power, cooling, network connectivity, processing (mainframe, distributed), media devices (storage), and office space.

4.4. Recovery Teams

Effective recovery requires an organizational structure that includes a recovery management team and multiple sub teams. A recovery management team is a group of individuals assigned oversight management responsibility such as, team assignment, structure, configuration, and recovery team membership. These will depend on agency structure, organization, and critical systems/services to be recovered.

> *Suggested Recovery Team definitions are contained in Appendix C*
> .

4.5. Recovery Command Center Configuration

DESIRABLE FEATURES OF ROOM:

1. Size 15 X 20 feet.
2. Separate Conference Room from work area with video conference preferred
3. Wall space for charts, maps, diagrams; 150 square feet.
4. Communications:

a. Mail service
b. Telephone (15 lines)
c. Fax Machine
d. Internet Capabilities

5. Furnishings:

a. Workstation tables
b. Workstations(15)
c. Server(LAN)
d. 15 speakerphones
e. 3270 capability
f. Internet
g. Printer
h. Fax
i. Tables
j. Copier
k. White Board
l. Chairs
m. Various PC software (Word Processing- MSWORD, Spreadsheet EXCEL and LOTUS 123, MSPowerPoint, VisioPRO, Internet, 3270 emulation, Blue Zone 3270 emulation, VPN client, Electronic Mail, etc.)

4.6. Escalation and Notification Planning

Standard operating procedures for emergency contact of management and technical staff are to be followed under all circumstances. If the building is damaged during office hours and everyone in the building is unaccounted for, the designated Recovery Management Team member representing agency management must initiate the recovery process.

Escalation of sustained service outage affecting critical IT applications of many agencies to the category of a 'disaster' may go through different stages. Incidents of outage due to many causes (predictable such as severe weather and other unpredictable ones) may be reported to the CMS/BCCS IT Service Desk. The IT Service Desk may assign the trouble ticket related to the incident to the Command Center for mainframe computing. Incidents may grow to 'problems'. If a 'problem' remains persistent for an extended period of time, it may become a 'major outage'. Major outages are assigned to the CMS/BCCS 'Major Outage Response Center' (MORT) whose membership includes the RMT Chairman and vice chairman. The IT Service Desk or the MORT Duty Manager will open the dedicated conference bridge. When the MORT Duty Manager recognizes the symptoms of a 'disaster' during a major outage, the steps outlined in an activation document, namely, initial response, and secondary response will be followed before a 'declaration' is made.

The Contact Lists contained in a notification plan will be used to begin the necessary notifications. The call lists should be constructed by team assignment, with the team leader being number one in the calling order. The lists should contain personal and office contact information.

A calling tree should be established by providing each team leader with a copy of the information for their recovery team. The team leader shall be responsible for conducting calls to their team members.

Team leaders are to call back to the recovery command center and report contact status when calls to reach all team members have been attempted and/or completed.

Call status is collected from RMT team leaders and recorded on a master contact list at the recovery command center.

5. AWARENESS

Recovery response awareness is performed on multiple levels from the individual up to the agency. Prior planning, training and rehearsals are key elements of an awareness campaign. This training and rehearsal includes but is not limited to all facets of assignment education, recovery process and procedures

Agency staff members should be made aware of their level of involvement in planning for and participating in the recovery of agency services. Key personnel should be made aware through the planning process and recovery rehearsals. Recovery management teams maintain the responsibility for designating and informing their staff of team assignment.

Agency bureaus and in some cases, sections or units of a bureau, are responsible for designating a recovery coordinator. This coordinator has the responsibility of keeping recovery teams and staff informed of specific recovery actions.

CMS/BCCS maintains communication of recovery related events through their Recovery Services Manager. This manager oversees and directs the CMS/BCCS Recovery Management Team. Each recovery management team member is considered a team leader and has specific staff assigned on their particular recovery team. The Recovery Team member is responsible for planning, documentation, communication of recovery needs to the CMS/BCCS Recovery Services Manager and disseminating information among their team members. The Recovery Management Team meets for vendor presentations, annual workshops, key recovery exercises, post-exercise reviews, and special seminars. Recovery management team members are expected to participate in all exercises and recovery plan maintenance.

6. EXERCISES

Exercising recovery plans, in part or in whole, validates the plans.

1. Exercises may be conducted as a table top[1], simulation[2], component[3], or comprehensive[4]. It is possible to have a comprehensive desk check as well as a component simulation.
2. Exercises involving CMS/BCCS main computing facilities and services are conducted at alternate local and remote computing facilities.
3. Exercises involving CMS/BCCS computing facilities and services must be scheduled in advance with the following documentation:
    a. Enterprise Service Request with dates for exercise
    b. Exercise plans; including application and functionality to exercise, hardware requirements, connectivity requirements, backup / tape recovery requirements
    c. Application recovery scripts
    d. User rehearsal scripts
    e. Exercise documentation including; results, contingencies, changes, remediation steps, corrective action plan
4. For Category 1 / Stage 0 applications, documentation of the exercise should be filed with the appropriate recovery coordinator. Annually, documentation should also be filed with CMS/BCCS Recovery Services.
5. CMS/BCCS maintains a contract for storage and retrieval of essential recovery information in a robust, off-site vault.

See Additional Roles and Responsibilities in Appendix D.

[1] Table Top check means to review the plan as it is documented on paper; simulating disruption scenarios while sitting at a table; no resource is relocated or redirected.

[2] Simulation means that normal resources are unavailable and that the recovery site will be used to restore processing. The production environment is not affected.

[3] Component means that only limited/selected pieces of the plan are included in the exercise.

[4] Comprehensive means that all components of the plan are exercised.

7. MAINTENANCE

7.1. Change Management

Updates of basic, essential, crucial business information must be made a process to ensure that during recovery, the most current and accurate information is being used as the basis of recovery decisions and actions. Updates to recovery related information should *not* be simply an annual project.

Documents should be disseminated to those individuals designated to receive a copy.

7.1.1. Suggested Internal Change Management Triggers

The following possible triggers should be used to update the recovery information:

1. New initiatives and critical applications or systems.
2. Changes to critical systems/services and respective recovery scripts.
3. Changes to versions of operating systems and utilities.
4. Additions and or upgrades to existing equipment.
5. Changes in personnel and team assignments (internal personnel unit).
6. Changes in backup procedures.
7. Changes in vendor/critical contacts.

7.1.2. Update the Statewide Recovery Repository:

Minimally on an annual basis and more frequently, if needed, the following are examples of the information that should be filed with CMS/BCCS Recovery Services for inclusion in for the Statewide Recovery Repository.

1. Approved plans.
2. Updated equipment configuration changes for critical systems or services.
3. KEY personnel updates such as changes of Recovery Services personnel, Agency Recovery Coordinators or Recovery Team contacts.
4. Exercise documentation.
5. Critical Application Information for all platforms.
6. Vendor contracts.

7.2. Recovery Plan Storage Locations

Recovery Plans that are contained in the Statewide Recovery Repository will be stored off-site in at least one location in 'hot' boxes for immediate use during a recovery. Additional storage locations may be added depending upon the nature of the plan information.

APPENDICES

Appendix A	Business Impact Analysis Guidelines
Appendix B	Risk Management Sample Matrix
Appendix C	Recovery Team Definitions
Appendix D	Recovery Services Roles and Responsibilities

Appendix A: BUSINESS IMPACT ANALYSIS GUIDELINE

Business Impact Analysis Interview Checklist

Section 2, "Recovery Methodology Plan", Department of Central Management Services / Bureau of Communication and Computer Services

Specific objectives of a Business Impact Analysis (BIA) include:

- ❑ Identifying major risks, that could cause a failure to meet agency objectives, and documenting associated controls that mitigate or lessen the agency's vulnerability;
- ❑ Assessing the impact of a negative event based on the agency's mission and legislated mandates;
- ❑ Identifying critical business resources (functions, processes, systems, services, personnel) etc. that support the agency's mission and enable meeting legislated mandates and expected levels of service; and
- ❑ Determining the time criticality (recovery time objective) for each critical resource identified above (recovery time objective is the maximum length of time that can elapse before the unavailability of the resource becomes unacceptable and places the agency at risk of failing to meet their mission).

1. Failed Application: *(example: Email)*

   _____

2. Identify the Business Process that uses the Application as an integral part:

   _____
   _____
   _____
   _____

3. Business Process Manager (Name): _____
   (Title): _____
   (Email address): _____
   (Phone): _____

4. Business Process description:

   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____
   _____

5. Choose the peak time(s) of business activity associated with your Business Process.

Please check all that apply

☐	January	☐	Monday	☐	End of Week
☐	February	☐	Tuesday	☐	End of Month
☐	March	☐	Wednesday	☐	End of Quarter
☐	April	☐	Thursday	☐	End of Fiscal Year
☐	May	☐	Friday	☐	End of Calendar Year
☐	June	☐	Saturday	☐	Other (specify below)
☐	July	☐	Sunday	☐	
☐	August	☐		☐	
☐	September	☐		☐	
☐	October	☐		☐	
☐	November	☐		☐	
☐	December	☐		☐	

6. Does your Business Process interact with other Business Processes?
(*example: Inventory System automatically feeds data to General Accounting System*)

☐Yes ☐ No

If you answered "yes" please list the other Business Processes and explain each:

_____
_____
_____
_____
_____
_____

7. Please list the essential documents you receive for use by your Business Process:
(*examples: reports, print-outs, brochures, news letters, bills*)

_____
_____
_____
_____

8. Please list the essential documents your Business Process generates:
(examples: reports, print-outs, brochures, news letters, bills)

_____

_____
_____
_____

9. Do you plan any changes to your Business Process in the next 12 months?

   ☐Yes ☐ No

   If you answered "Yes", please explain:

_____
_____
_____

10. Number of employees in your business group that would be affected by the failure of the Application: _____

11. How long could your Business Process continue to function without the Application?

    Please assume an Application failure during your busiest time-period.
    Please check only one.

    ☐ Less than 1 day
    ☐ Up to 2 days
    ☐ Up to 4 days
    ☐ Up to 1 week
    ☐ Up to 2 weeks
    ☐ Up to 1 month
    ☐ Up to 3 months

Comments: _____
_____
_____
_____

12. Tangible impact(s) of application failure:
    (Please check all that apply)
    a. ☐ Reduced Productivity
    b. ☐ Increased Expense
    c. ☐ Delayed collection of funds
    d. ☐ Delayed payment of funds
    e. ☐ Lateness Penalties
    f. ☐ Other (explain): _____

13. Please give your best estimate of the cost of this impact:
(Please check one)
    a. ☐ Less than $1,000
    b. ☐ Between $1,000 and $10,000
    c. ☐ Between $10,000 and $100,000
    d. ☐ Between $100,000 and $500,000
    e. ☐ Between $500,000 and $1,000,000
    f. ☐ Over $1,000,000

14. Intangible Impact(s) of application failure:
(Please check all that apply)
    a. ☐ Human Safety
    (Resources that directly impact the lives and safety of Illinois citizens, including state employees. *Examples: Police, Fire, Medical, Corrections, Child Welfare, etc*.)

    b. ☐ Welfare Human Service
    (Resources that directly impact the well being of Illinois citizens.
    Examples: Assistance, Benefits, Vital Records, etc.)

    c. ☐ Non-Welfare Human Service
    (A human service resource that indirectly impacts the welfare of Illinois citizens.
    Examples: Registries, Licensure, Tracking, Vendor related, etc.)

    d. ☐ Admin State Functions & Processes
    (Resources that support the administration of state processes.
    Examples: Payroll, Compensation, Procurement, Accounts Payable, etc.)

    e. ☐ Support of specific Agency Functions and Processes
    (Resources related to the maintenance of a specific agency function or process.
    Examples: Laboratory, Utilities, Diagnostics, Statistical systems, Application Code Tools, etc)

    f. ☐ Other (explain): _____

    Comments:
    _____
    _____
    _____
    _____

15. Are there documented alternate procedures that can be used to support your Business Process if the Application fails?
    ☐Yes ☐ No

16. How is the alternate procedure documentation stored?
    ☐ electronic
    ☐ paper
    ☐ other (explain) _____

17. Where is the alternate procedure documentation located? _____

18. Have you tested the alternate procedure? ☐Yes ☐ No

19. When was the last time you tested? _____ *(dd/mm/yyyy)*

20. What additional office supplies are required for the alternate procedure? *(example: paper, specialized forms, office furniture)*
    _____
    _____
    _____
    _____

21. What additional IT hardware is required by the alternate procedure?
    (example: stand-alone PC, software, printer, time-stamp machine, fax machine)
    _____
    _____
    _____
    _____

22. What additional resources are required by the alternate procedure *(example, security personnel, specialized mail delivery, courier service, temporary office workers, specific documents from primary work location)*?
    _____
    _____
    _____
    _____

23. Please estimate the percent level of normal Production that could be maintained using the alternate procedure:

% of Normal = _____

24. Please estimate the maximum time frame that you could use the alternate procedure:

_____ Days
or
____ Months

Appendix B: RISK MANAGEMENT SAMPLE MATRIX

RISK	PROBABLITY OF OCCURRENCE	MITIGATING CONTROL
1. Tornado	Low	Data & Operating Sys regular & offsite Backups; remote recovery facility & tested recovery plan
2. Flood	Low	Periodic maintenance, warning systems
3. Fire (Natural)	Low	Auto sprinkler, Direct/Auto alarm to fire dept., FM200
4. Fire (Arson)	Low	Auto sprinkler, Direct/Auto alarm to fire dept., 24/7 Security Guards Patrol, secure building, FM200
5. Fire (Accidental)	Low	Auto sprinkler, Direct/Auto alarm to fire dept, 24/7 Security Guards Patrol, secure buildings, FM200
6. Strike	Low	Union contract controlled, admin and mgmt staff cross-trained
7. Chemical Spill	Low/Unlikely	Work location not in path of transportation, no buildings storing chemicals within a block radius, but several paint business within a two block radius.
8. Natural: earthquake, ice storm, lightening strikes	Medium/Low	Remote recovery host site and vaults are far removed from earthquake centered at the main data center; loss of utility electric power is compensated for by the local UPS, and diesel generators with reserve fuel.
9. Man-Made: cable cuts, chemical/toxic spill, natural gas leak/explosion, asbestos, broken water pipe, fire (arson and accidental), pickets, strike, riots, terrorism, bomb threat/detonation, vandalism/theft, sabotage, disgruntled staff or intruder (client), fraud/embezzlement.	Low	24/7 Security, on-site maintenance people, well constructed buildings
10. Proximity: (surrounding neighbor's or essential supplier disruption) nearby airport, military munitions depot, railroad, etc	Low	Business in the area may store chemicals at time. 3 blocks from major rail line, but line not used for high-risk transport.

Appendix C: RECOVERY TEAM DEFINITIONS

TEAM NAME	MAJOR RESPONSIBILITY
1. Administrative	Acquire furniture, desks, supplies, temp workers, etc.
2. Applications System Recovery	Restore and configure applications to the recovery site system.
3. Coordination & Scheduling	Prioritizes tasks (using the plan as a guide but adjusting for current conditions) to ensure tasks completed in correct sequence
4. Damage Assessment	Assess severity/impact of event
5. Facilities	Assess, acquire, coordinate building use
6. Hardware Recovery	Install/configure hardware & operating systems at the recovery site.
7. Media Recovery	Acquire & transport media & documentation (includes data backups)
8. Migration	Coordinate movement out of service provider recovery site
9. Network Communications	Install/configure/test network communication capabilities & devices.
10. Operations	Restore & monitor data processing operating system software.
11. Public Relations	Communicate with external entities (public, press, etc.)
12. Recovery Management	Coordinate agency response & declare disaster if necessary
13. Restoration	Could include operations, system software, and application software teams.
14. Salvage	Retrieve data & equipment from original work site
15. Scribe	Record (electronically, video, audio, or hardcopy) damage assessments & other pertinent info
16. Security	Ensure people, data, & equipment are kept secure
17. System Software Recovery	Restore & monitor system software including utilities.
18. Procurement	Acquire critical resources through emergency processes

Appendix D: Recovery Services Roles and Responsibilities

CMS/BCCS and participating agencies are subject to, but not limited to, the following roles and responsibilities. These define the most critical components of the Recovery Services process that are essential to its success. Continued discussions in the planning process may reveal further roles and responsibilities depending on the complexity and specificity of the environment being recovered. Responsibility for a given role is denoted by an "X" in the appropriate column. Those roles that fall under dual responsibility will be clarified during the planning process.

Role	BCCS	Agency	Remarks
1. Business Impact Analysis		X	
2. Risk Assessment		X	
3. Manage IT Recovery Teams	X	X	Each organization should develop the appropriate teams.
4. Regionally exercise all Category 1 applications	X	X	BCCS will provide the infrastructure and exercise coordination.
5. Initiate recovery plans by opening an ESR		X	Agencies will open a service request to begin recovery planning process.
6. Manage Statewide IT recovery plan repository	X	X	Agency updates, BCCS review and store
7. Develop agency recovery approach/strategy		X	
8. Coordination for recovery planning	X	X	BCCS and agency will coordinate plans
9. Ensure approach conforms to Statewide DR methodology	X	X	Approach will be reviewed and verified to ensure conformity and feasibility.
10. Maintain Methodology	X		Agencies are welcome to comment and provide suggestions.
11. Define application categories, RTO, BRM entries		X	
12. Determine and communicate IT recovery needs		X	Including special requests for tools, products, and/or utilities
13. Define application requirements- application dependencies, high availability, change mgmt, database configuration files		X	Including all data stores, access configuration, execution scripts, etc…
14. Define infrastructure requirements	X		BCCS will validate with the agency
15. Define data backup method, schedules, off-site storage	X	X	Will be coordinated to define the specifications for the recovered environment.

Role	BCCS	Agency	Remarks
16. Define application recovery script		X	
17. Define infrastructure recovery script	X		
18. Execute system restore and notify results	X		
19. Request for data/file restore, execute application restore and verify results		X	
20. Identify notification process, escalation process, call tree, individual responsibilities	X	X	As required by each agency
21. Develop, update, maintain and store activation plans	X	X	Plans will be stored in the State-wide recovery file
22. Train recovery personnel	X	X	BCCS – infrastructure; Agency - applications
23. Schedule recovery plan exercise	X	X	BCCS – infrastructure; Agency – applications
24. Provide exercise facilities, infrastructure	X		
25. Exercise infrastructure activation plan	X		
26. Exercise application recovery activation plan	X	X	
27. Communicate exercise results and file exercise reports		X	Agencies to provide detailed exercise documentation in appropriate format
28. Store exercise results in statewide recovery file	X		
29. Mitigate problems discovered during exercise	X	X	Corrective action plans to be coordinated between BCCS and agency where appropriate.

-end of Recovery Methodology appendices-

1	https://www.drii.org/
2	http://www.fema.gov/emergency/nims/ImplementationGuidanceStakeholders.shtm
3	http://csrc.nist.gov/index.html