Recovery Management

Release Data: March 18, 2012

Prepared by:

Thomas Bronack

Section Table of Contents

Section Table of Figures

8. Recovery Management

8.1. Introduction to Recovery Management

This section describes a methodology for the implementation of Recovery Management within an I/S organization.

8.1.1. Definition

Recovery Management is the process of planning, testing, and implementing the recovery procedures ad standards required to restore service in the event of a component failure; either by returning the component to normal operation, or taking alternative actions to restore service. Recovery Management is the acknowledgement that failures will occur regardless of how well the system is designed. The intent is to anticipate and minimize the impact of these failures through the implementation of predefined, pretested, documented recovery plans and procedures.

8.1.2. Objectives

The primary objective of recovery Management is to ensure that service level requirements are achieved. This is accomplished by having recovery procedures in place that will restore service to a failing component as quickly as possible.

8.1.3. Scope

The scope of Recovery Management from an SMC perspective deals with normal day-to-day service delivery operations; for example, the usual hardware, software, application, operational, and environmental failures which occur everyday in the I/S environment.

Recovery Management does not include Business Recovery (Disaster Recovery) or vital records backup storage. Recovery Management will assist in providing the necessary requirements to support day-to-day service delivery in the event of a disaster event.

8.1.4. SMC Interfaces

The Recovery Management process has interfaces with other SMC disciplines and functions. In fact, some Recovery Management responsibilities may be carried out by these other disciplines or functions. Key interfaces are maintained with the areas listed below. Depending on site organization, responsibility for these disciplines and functions may reside in a single department with a single individual, across many departments, or any effective combination. It is not organization which is important, but the effective execution of Recovery Management responsibilities.

- **Batch Management**

Recovery Management ensures that recovery procedures are in place for batch processing. This includes recovery procedures from hardware, software and environmental failures affecting batch applications. In addition, Recovery Management will coordinate problems with batch recovery procedures.

- **Capacity and Performance Management**

Recovery Management interfaces with these disciplines to ensure that sufficient capacity is available to accommodate the peak loads experienced during recovery procedures and that system availability satisfies client needs.

- **Change Management**

All changes to the components are reviewed for proper backout procedures to allow for timely recovery in the event of an unsuccessful change installation. Additionally, all changes are reviewed for the potential impact to existing recovery procedures and to determine if any new or additional procedures are required as a result of the change. Information pertaining to the backout of recovery procedures are documented and reviewed in the change record as required.

8.1.5. On-line Management

Recovery Management ensures that recovery procedures are in place for network or on-line outages, and will coordinate problems with procedures in the event that network outages occur. All end user support personnel assigned to maintain the on-line systems must have a thorough understanding of on-line systems recovery methods and know the location of all recovery documentation. The Global Systems Help Desk must interface with Recovery Management to ensure that all on-line recovery procedures are up to date and accurate.

8.1.6. Problem Management

Problem Management manages the methods and guidelines used to document the impact of problems on service level commitments. Problem Management interfaces with Recovery Management on a daily basis to ensure that all component problems have been identified and properly recorded. Recovery Management uses this information to assess the results f component outages ad recovery capabilities. Although presented here as a separate subject, the Recovery Management process is an integral part of the Problem Management process. In practice and function the actual recovery action is part of the problem resolution process flow.

8.1.7. Service Level Management

Recovery Management supports the service level process by minimizing, to the extent possible, the time required to restore service after a component failure, and through post outage analysis. This is to minimize or prevent future failures of a similar nature. Through participation in Recovery Management meetings, for outages which have affected service level components, the Recovery Management Coordinator can assure that proper emphasis has been placed upon the service with current agreements, and that procedures and priorities are consistent with the services being offered.

8.1.8. Hardware Requirements and Planning

Recovery Management interfaces with requirements and planning to ensure that the CFIA document is current for reference purposes during a recovery situation.

8.1.9. Supplier of Service

The supplier of service, must understand the customer's needs and design the solution to meet or exceed the customer's requirements. The Supplier of Service must also provide a stable environment and maximize service availability and reliability.

8.1.10. Receiver of Service

The Receiver of Service, or designated representative, must provide an accurate picture of their needs, environment, and a forecast of any changes which may affect the level of service provided to them. They must be required to support those needs.

8.1.11. Site Recovery Management Coordinator

The Site Recovery Management Coordinator is the person responsible for documentation, execution, review, and control of the overall Recovery Management process. Other duties and responsibilities are:

- Review and analyze results for all recovery problems/action items.
- Act as the primary I/S representative for recovery procedure documentation, and concerns.
- Secure the assistance of all appropriate parties to assess all Recovery Management plans.
- Escalate appropriate recovery problems to management with supporting facts for proposed changes and recommended course of action. These escalated problems deal with conflicts that cannot be resolved between I/S functions.
- Periodically evaluate and revise, when necessary, Recovery Management process documentation.
- Perform the Recovery Management process self-assessment on a semi-annual basis.
- Act as the focal point for questions and concerns pertaining to the Recovery Management process.
- Attend weekly change control, technical assessments, and pre-install meetings to ensure that recovery procedures have been reviewed, updated, and tested prior to installation.
- Provide management direction on where and how well Recovery Management is performing.
- Provide reports to assess impact of the Recovery Management process on system outages.
- Analyze scheduled and unscheduled backup recovery exercises.

- Conduct semi-annual review of the Component Failure Impact Analysis (CFIA) document as well as all major recovery procedures. See "CFIA" document in appendix for more details.

- Coordinate annual recovery procedure testing.

8.1.12. Operations

Operations for systems, networks and client/server areas are responsible for:

- Maintaining, in the operations area, up-to-date recovery documents.

- Executing recovery procedures for all system/applications, with assistance from the support areas when needed.

- Testing of system/application recovery procedures semi-annually.

- Recording of pertinent information in the on-line Problem Management system, which includes documenting procedure problems.

- Logging and tracking system, component and application outages.

- Logging and tracking recovery time components of outages in regard to application, system, and component recovery.

- Ensuring that all recovery procedures have an eight character naming convention, and inform the operations analyst if there are procedures on the operations floor that have not been named.

- Reviewing and supplying the necessary updates to the Operations Reference Guide.

- Reviewing development phase project documents for impact to the Recovery Management process.

- Performing management initiated root cause analysis for all severity one outages immediately.

- Maintaining and updating the recovery matrix.

8.1.13. Technical Support

The Technical Support staff is responsible for implementing and maintaining procedures and standards to ensure recovery capabilities at all times. Other Technical Support duties and responsibilities are:

- Provide Operational recovery procedures.
- Provide numbered recovery procedures.
- Provide software contact support list.
- Test system and component recovery procedures prior to production installation.
- Ensure recovery methods are included in the operational procedures.
- Ensure existing recovery procedures are regression tested following system changes.
- Provide problem escalation support.

8.1.14. Application Support

The Application Support staff is responsible for implementing and maintaining the process, and standards to ensure recovery capabilities at all times. Other Application Support duties and responsibilities are:

- Ensure recovery methods are included in the development of new applications and changes to existing applications.
- Participate in application recovery process when needed to recover from outage.
- Ensure proper owner classification of proposed new applications.
- Test system recovery procedures prior to production installation.
- Ensure recovery methods are included in the operational procedures.
- Ensure existing recovery procedures are regression tested following system changes.
- Provide problem escalation support.

8.1.15. Management Responsibilities

Data integrity, timeliness, proper recording, proper documentation, root cause analysis, and permanent resolution are the responsibility of the department manager. These tasks may be delegated. However, ownership and accountability remain with the manager. The manager's responsibilities include:

Review and understand the Recovery Management process document.

Manage problem in accordance with criteria guidelines.

Manage problem out-of-criteria, identify and correct recurring problems.

Schedule Recovery Management education for the department as needed.

Ensure problem records are handled in accordance with the Recovery Management process.

8.1.16. Meetings

Recovery meetings are called to plan for new or changed component recoveries and to perform the post mortem analysis of an outage.

When a meeting post mortem is required, all participants involved review recovery actions taken during a disaster to identify any deficiencies. The deficiencies are recorded and tracked as action items and included as a part of the Business Improvement Analysis (BIA) process. BIA items are addressed through updated recovery plans and improvements to normal daily functions relating to critical components.

Periodic updates to recovery plans are conducted through planning meetings that address changes and new additions. Vital Record backup and recovery procedures are reviewed during these meetings, as well as the procedures used to recover from a range of outages that can affect the component.

8.2. Process Description

The mission of the Recovery Management process is to support service level commitments as defined in SLAs, by anticipating and minimizing the impact of system resource failures through the development of predefined procedures and recovery capabilities. If an SLA is not in place, recovery procedures are still needed.

The Recovery Management process described in this document deals primarily with day-to-day recovery for non-disaster type failures. When component recovery is required, Recovery Management utilizes the CFIA document, normal recovery procedures developed and maintained by operations, and all levels of problem support throughout the I/S organization.

The actual implementation of recovery or bypass actions will normally occur early in the problem determination process as an intricate part of the Problem Management process.

8.2.1. Procedure Testing

Documented recovery procedures used to restore service to a failing component will require periodic testing. Because of frequent changes to critical components recovery procedures will be tested on an annual basis (at a minimum). Testing must include:

- Power off and power on simulation testing,
- System backup and recovery capability (full system and incremental backups will be utilized for these tests), and
- Normal recovery capability.

The Recovery Management process requires that all recovery procedures used to restore service be documented using a standard naming convention, so that specific procedures can be easily recognized. This information can be used to track and assess the "mean time to restore" for procedures during a given outage. Ongoing testing and evaluation can reduce the number of procedures and down time required for annual testing. Testing recovery procedures will require assistance from all support groups: Technical Support, Application Support, Hardware Support, and System Scheduling Support.

8.2.2. Situation Management

Situation Management is an internal process which is implemented as part of the alert procedure for critical situations.

When a critical situation occurs, designated managers are notified and assume the role of Communication and Situation Managers.

The function of the Situation Manager is to interface with technicians involved with the problem at hand, and to provide management assistance and guidance until the situation is resolved. This activity includes interfacing with support groups and relieving the technicians of management update responsibilities, allowing them to concentrate on the resolution of the problem.

The Communications Manager interfaces with the Situation Manager and the world at large to shield the problem resolution team from interruptions. It is the Communications Manager who is responsible for disseminating information and providing updates to technical and management personnel on the status of the situation and progress made in its resolution.

By prior agreement with the management team, the Situation Manager has temporary use of the total resources of the entire organization until the situation s returned to normal.

8.2.3. Problem Definition and Assignment

A Problem is defined as:

- An impact of the Expected Service Delivery schedule,
- A deviation from Standards and Procedures.

When problems affect critical components and major outages occur, then a disaster situation can occur. When this happens, it is essential that the problem is reported and recovery procedures initiated.

Problems are assigned to Resolvers who are responsible for the operation of the failing component(s). The Global Systems Help Desk is used to coordinate the entry, assignment, tracking and escalation of problems until they are resolved. For this reason, a list of Resolvers is maintained by the Global Systems Help Desk. This matrix of components to the personnel responsible for support of the component is a critical piece of information, that will greatly aid in the disaster recovery process. Every effort should be made to maintain the matrix in a current and accurate fashion.

When problems are initially reported to the Global Systems Help Desk, first level support procedures are activated. These procedures include:

- Defining the problem with the Problem Reporter,
- Entering the Problem into the Problem Management System (Apriori),
- Examining past problems of the type being reported to assist in problem: definition, recovery, and resolution (1st Level Support).
- Assigning the problem to a Resolver (2nd Level Support),
- Tracking the problem until resolved,
- Escalating the problem after predefined time periods, or at management's discretion, and
- Performing problem closure processing when resolutions are provided.

8.2.4. Problem Escalation

Problem escalation is based on the relative importance of the failing component, its impact on delivering business service, and the duration of the outage. Escalation guidelines for URGENT problems are:

- 30 Minutes after Resolver has been called and has not arrived.
- 60 Minutes after Resolver has arrived, but has not formulated problem resolution.
- Upon management discretion, based on impact, duration of outage, and relative importance.

Problem procedures must be followed when disaster situation occur. It is through these procedures that diagnosis and resolution of encountered problems will occur. Refer to the Problem Management section of the Standards and Procedures Manual for additional information of diagnosing and repairing problems.

8.2.5. Application Recovery

Application recovery procedures are available to the operations controller in the event that an application failure occurs. Application recovery procedures explain how to return the failing application back to normal operation. Recovery Management, Application Support Analyst, and Operations Analyst have the responsibility to maintain, test, and ensure that the application procedures are current and recovery ready. Requirements for application recovery procedures are as follows:

- Application recovery procedures are to be located on the operations floor.
- Application recovery procedures should use a naming convention so that specific recovery procedures can be easily identified.
- When a new application goes into production, these procedures should be updated with steps required to enable an application recovery, if a hardware of software failure occurs.

When a failure occurs, the operations support specialist should follow problem bypass/circumvention procedures to work around the problem (if possible), while initiating recovery/restart procedures to re-establish the operating environment to the point just prior to the problem (last checkpoint restart point). The problem should sloe be reported and the Resolver notified, so that a permanent solution to the problem can be generated. By following these procedures, the outage will be kept to a minimum and business services restored as quickly as possible.

For this reason, it is essential that bypass/circumvention and recovery/restart procedures exist for all critical applications. An examination of the status of these procedures for critical applications should be conducted periodically and updates performed accordingly.

8.2.6. Recovery Outage Summary

Restore Time is defined as:

- The time it takes operations to restore service to the customer when an outage occurs.

Recovery Time is tracked for critical outages and post mortems conducted to determine the amount of time devoted to each element of Recovery Time, including:

- Problem definition,
- Bypass/Circumvention procedures,
- Recovery/Restore procedures, and
- Resolution time.

The elements of Recovery Time and their sequence are shown below.

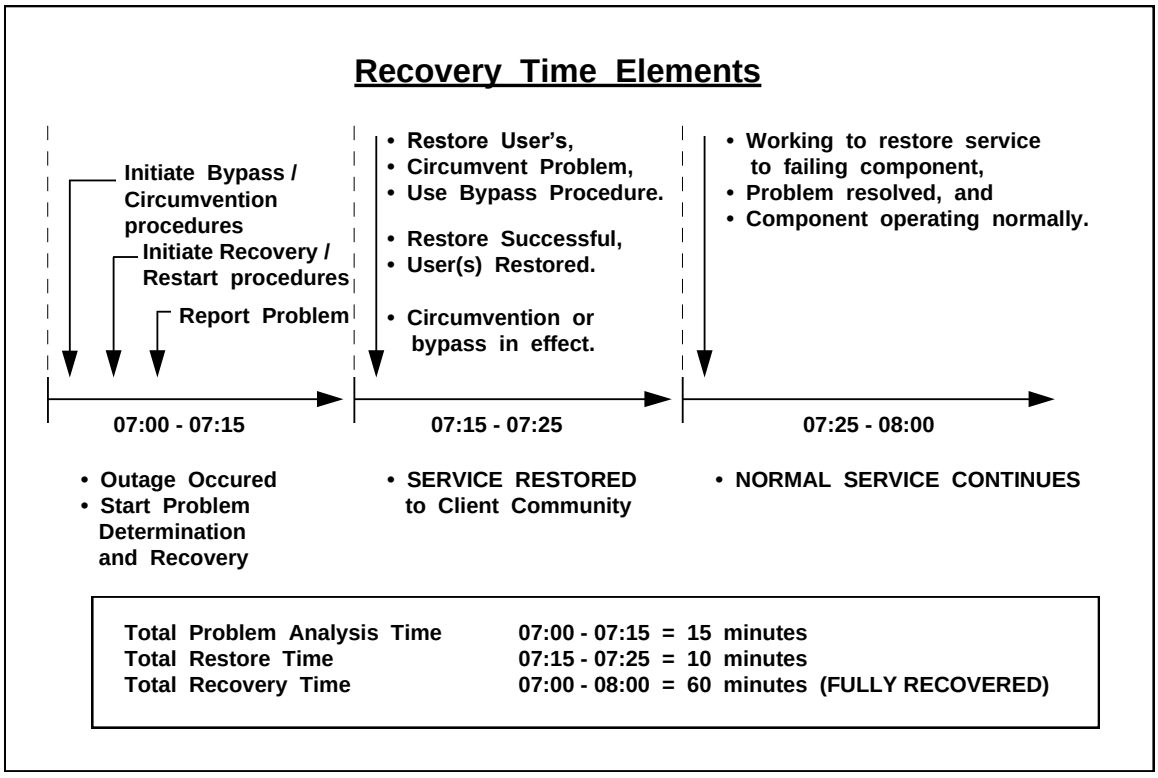


Figure 1: Restore and Recovery Time Elements

8.3. Recovery Process

8.3.1. Recovery Activity Process Flow

The basic activities which occur during recovery from an outage are outlined in the diagram below. These activities, for the most part, are performed by the System and Network operations personnel involved in the recovery.

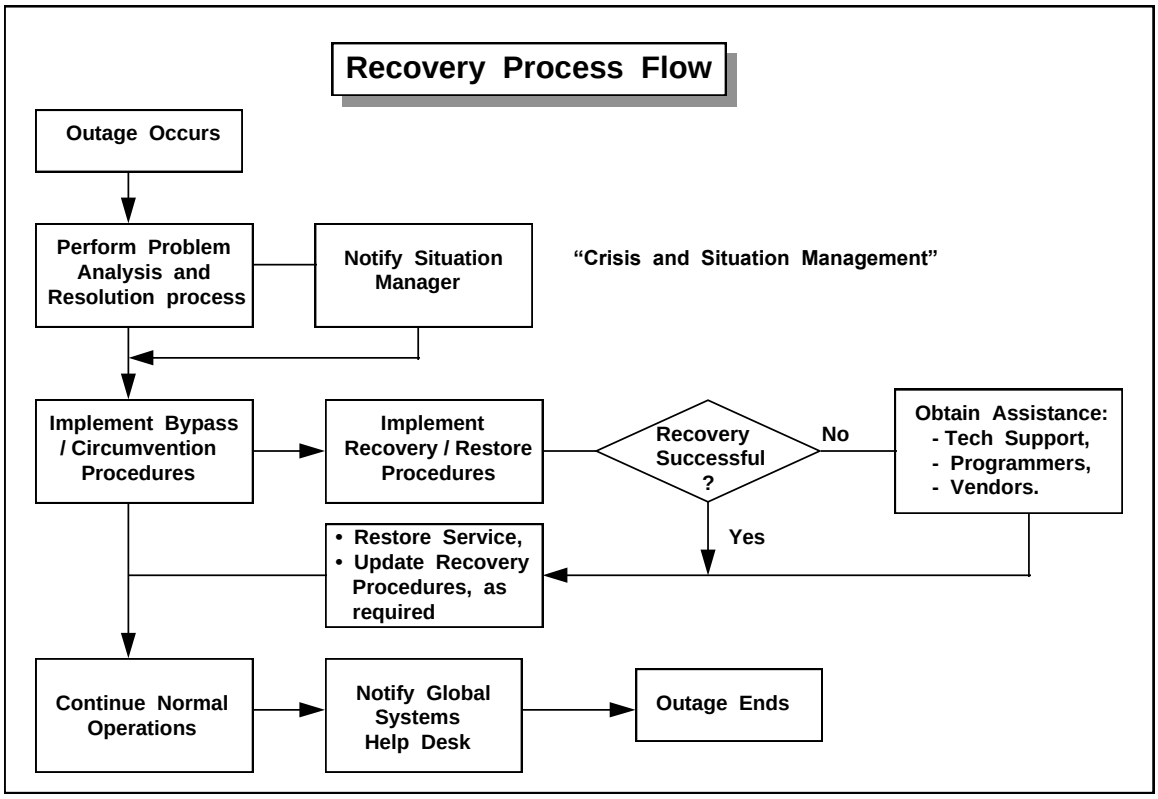
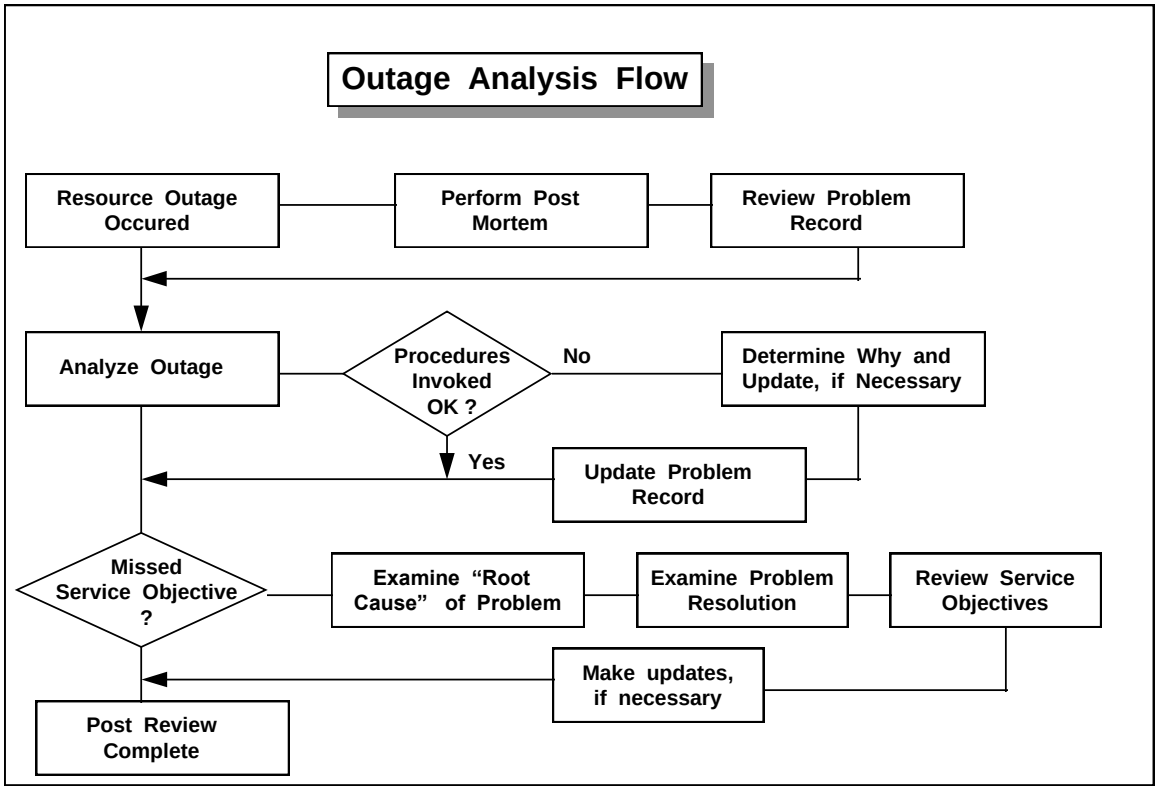


Figure 2: Recovery Process Flow Diagram

8.3.2. Recovery Analysis Process Flow

The figure below illustrates the activities of the Site Recovery Management Coordinator in the analysis of the outage and in establishing the need to perform a "Root Cause Analysis" (RCA) for a failing recovery procedure.



8.3.3. Recovery Management Process

This process begins with the detection of an outage r disruption to the environment which impacts clients and includes the following sub-processes:

The Recovery Management process ends with action items for continuous improvement.

- Recovery Management Sub-Process:
- Recognition of outage or disruption to the customer.
- Notification to problem resolver, management, and customer.
- Execution of recovery procedures.
- Analyzing the problem record.
- Post Mortem review of recovery.
- Validation of existing recovery procedures.
- **PROCESS INPUTS** include:
    - Problem Management process output.
    - Customer impact.
    - System / Application / Service degradation.
    - System / Application / Service outage
- **PROCESS OUTPUTS** include:
    - Alert notification,
    - Availability or service to the customer.

8.3.4. Customer Impact

The process of identifying problems prohibiting or inhibiting the client from utilizing committed services.

This process begins with the recognition of an impact by operations or the client and includes the following:

- Impact to a client's availability or accessibility.
- Deviations from standards and procedures.
- Outages.
- Duplicate outages within 24 hours.
- Outages that may not have proper recovery documentation available.

The process ends with a status update to management and the client.

PROCESS INPUTS include:

- An SLA impact.
- System / Application / Service degradation.
- System / Application / Service outage.
- Customer request.

PROCESS OUTPUTS include:

- Identify procedure to execute recovery.
- Document problem (execute Problem Management).
- Execute alert process.

8.3.5. Alert Process

The process of notifying management and clients of outages and estimated time of availability.

This process includes a status update from the crisis coordinator or the failing component, client, impact, and estimated time of availability to the client support, End user, and Global Systems Help Desk.

This process ends with status updates to management and to the client on the component failures impact and the time of recovery.

PROCESS INPUTS include:

- Problem Data,
- Input from crisis coordinator.

PROCESS OUTPUTS include:

- Updated status phone message,
- Updated management,
- Updated client.

8.3.6. Execute Recovery

The process of executing recovery procedures designed to bypass or restore committed service to the client.

This process begins with the execution of recovery procedures invoked by operations and includes:

- Outage time.
- Problem determination.
- Problem source identification.
- Problem data update.
- Execution of recovery procedures.

This process ends with availability to the client by restoring or bypassing the failing component.

PROCESS INPUTS include:

- Contact problem solver,
- Execute recovery procedures,
- Update problem record.

PROCESS OUTPUTS include:

- Bypass failing component,
- Restore failing component.

8.3.7. Analyze Problem Record

The process of analyzing the recovery process and problem data to determine the success of the recovery process.

This process begins when the Recovery Management coordinator analyzes the events that occurred during the execution of the recovery procedure. This includes reviewing documents of the problem and interviewing the Recovery Management team that participated in the recovery.

This process ends with an assessment of the recovery process to recover the failing component.

PROCESS INPUTS include:

- Analyze problem data,
- Analyze change data,
- Analyze recovery procedures,
- Gather input from recovery team.

PROCESS OUTPUTS include:

- Determine need for meeting,
- Update problem record,
- Update recovery procedure.

8.3.8. Post Review

The process of reviewing outages, description of failures, client impact, ad activities required to restore service to client.

This process begins with a technical assessment of the outage by the recovery coordinator and the recovery team, including:

- Review the execution of the recovery procedure.
- Analyze the problem flow.
- Review input from the recovery team.
- Understand the client impact.

This process ends with action items to improve the recovery procedure which was executed.

PROCESS INPUTS include:

- Problem data,
- Change data,
- Recovery data,
- Recovery team,
- Client,
- Client impact (SLA).

PROCESS OUTPUTS include:

- Execute Root Cause Analysis (RCA),
- Develop action items, such as:
  - Update existing recovery procedures,
  - Create new recovery procedures,
  - Update CFIA.
- Evaluate process,
- Identify process improvements.

8.3.9. Testing Recovery Procedures

This process simulates and validates existing recovery procedures, begins with an outlined plan to test recovery procedures and includes the following tasks:

- Identify procedure to test by operations or support.
- Schedule the test (using change management).
- Staff with skills to perform the test.
- Execute procedures.

This process ends with updates to recovery procedures and information records with a status of the test.

PROCESS INPUTS include:

- Identify the procedure,
- Create a change record and schedule the test,
- Decide skills ad resources needed to execute procedure.

PROCESS OUTPUTS include:

- Execute the recovery procedures,
- Identify problems with procedure (Problem Management),
- Record system / application outages (Problem Management),
- Updated recovery procedure, if applicable,
- Update education matrix,
- Update training matrix,
- Update CFIA, if applicable,
- Close problem record,
- Close change record.

8.3.10. Measurements

The process of measuring the Recovery Management process.

The process begins recording outage data related to recovery outages, and includes:

- Record of outage times in the problem record documented by operations.
- Rate the recovery effectiveness.

The process ends with reporting the measurements to the client and I/S management communities

PROCESS INPUTS include:

- Update of the problem record with outage times,
- Assign record to problem solver,
- Execute report.

PROCESS OUTPUTS include:

- Report measurement to client and management, with:
  - Mean time to restore,
  - Mean time to recover.
- Re-Evaluate existing recovery procedures,
- Identify the need to establish new recovery procedures based on measurements.

8.3.11. Recovery Management Documentation

All problems relating to system and major application outages are recorded in the on-line Problem Management data base. These problems are reviewed and tracked daily by the Problem and Recovery Management coordinators. All information relating to recovery are included as part of the permanent record. Recovery procedure action plans are also recorded in the same record to provide a means of tracking the results of post-recovery reviews.

All changes are recorded in the on-line Change Management data base. Information addressing the recovery installation or backout procedures may be reviewed in the change record.

- **Critical Business Documentation**

When multiple outages occur, the most critical systems and applications must be recovered first. The order of recovery, based on the business need of the system or application is documented and is used by system and network operations to prioritize the recovery effort, thereby ensuring maximum availability of critical business applications.

- **CFIA Document**

The CFIA document is a configuration document designed to assist in system recovery. Once a system failure or outage occurs and normal recovery has failed, the CFIA document is used to find ways to bypass or circumvent the problem using alternate paths to restore service until the failing component has been fully restored.

- **CFIA Contents, include:**

1. DASD Volume locator charts,
2. I/O cabling configurations,
3. Tape subsystem configuration,
4. Channel to channel configurations,
5. Teleprocessing Control Unit configurations,
6. Diagrams to assist in understanding the hardware,
7. Recovery procedures or directions to the required recovery procedures.

In addition to providing recovery procedures, the CFIA is used in the following activities:

Planning Changes - system modifications are checked against the existing configuration to ensure proper system design.

Determining system exposures - the existing switching and backup capabilities can be easily analyzed to give a broad view of the possible alternative means of accessing components while minimizing system outages.

Determining cable configurations - these are contained in the document and are used by Customer Engineers to make specific hardware changes.

Laying out DASD packs - the CFIA provides a guide to recovery actions.

Determining device addresses - problem determination may be aided by using the addressing information contained in the document.

Locating devices on the floor - actual floor positions of system components are indicated for all devices.

Determining tape and tape controller configurations - all tape and controller configurations are included.

Circuit breaker identification and location - breakers are listed for each system component.

Identifying and locating power source - power source for each circuit breaker is listed.

- **Major Component and CPU Recovery Plan**

Necessary recovery action in the event a major component or CPU failure should be defined and specified within the CFIA document.

The CFIA document recovery procedure is used to assist bypass/circumvention in the event that existing recovery procedures fail.

- **Non-distributed Systems**

After standard vendor recovery documented procedures are applied and recovery is unsuccessful, the CFIA document is referenced, and appropriate actions are taken to bypass and circumvent the problem.

For example: Assume a 3380 DASD unit has an I/O error, data check, or some other error that would render it inoperable. The system controller would see the message on the system console and the message would give the controller the address of the failing DASD device.

In our example, we will use SY4B DASD with an address of C82. The controller would look in the table of contents in the EPCT document and find the page that SY1F DASD address C82 is on. The controller would turn to that page and find the following:

DASD Address Chart

3380 IU18	AD4 A9487				BD4 F8455			
PACK ADDRESS	C80	C81	C82	C83	C84	C85	C86	C87
PACK NAME	HSMD33	IMS812	HSMD34	IMS813	HSMD35	MIGD12	MISD16	MISD17
PRIME: SY4B SHARED:	STG	PRV	STG	PRV	STG	PRV	PRV	PRV
GENERIC:	SYSDA	SYSDA	SYSDA	SYSDA	SYSDA	SYSDA	SYSDA	SYSDA
RECOVERY	D11	D11	D11	D11	D11	D11	D11	D11

Figure 3: DASD Address Table

The controller would find the entire bank of DASD that C82 is connected to. Directly under the address C82 on the last printed line, the controller would find three alphanumeric characters. This is the recovery action and in this example would be D11.

The controller would then look at the end of the DASD section under DASD recovery procedures. T The D11 instruction would be followed by the controller. The D11 instructions explain whether there should be immediate Data Management attention or delayed notification.

The method of using the recovery procedures for the CPU, DSEs. CHIPDs and other I/O is basically the same. Find the device in the table of contents, go to the page indicated, go down the correct column to the recovery action, and carry out the recovery action.

8.4. Process Evaluation

8.4.1. Annual Self Assessment

The process of ensuring controls are in place to effectively manage the recovery process.

This process begins with questions on controls of the process.

This process includes questions to be answered by the recovery coordinator to ensure the site is in compliance with a efficient and effective Recovery Management process. This process ends with a complete assessment.

PROCESS INPUTS include:

- Questionnaire including evaluation questions that probe the effectiveness of the Recovery Management process.

PROCESS OUTPUTS include:

- Action item document providing specific plans to improve the effectiveness of the Recovery Management process,
- Completed questionnaire documenting the results of the self-assessment.

8.4.2. Measures of Effectiveness

The key success indicators for Recovery Management are:

- Mean time to restore for Recovery Management community.
- Mean time to recovery for the failing component or application.
- Accuracy of the procedures for restore and recovery.

This data is collected in the Problem Management data base.

All system outages, corrective actions, or resolutions are recorded in the Problem Management data base. This data is used to calculate and determine process effectiveness. Process measurements are documented and distributed monthly to operations management.

The key process measurement reports are:

- **Mean Time to Recover, by Environment** - this report shows total recovery time for a failing component.

- **Mean Time to Restore, by Problem Type** - this report shows total recovery time as it relates to SLA objectives for system outage types. For example, hardware, software, facilities, and others.

- **Accuracy of the Procedures for Restore and Recovery** - this measurement will provide the rating for the accuracy of the procedures. This rating will be determined by the number of open and abeyant problem reports against recovery procedures. A rating of 1-10 will be given.

Monthly analysis of the above measurements provide an overall indication of the process effectiveness. Specific data on individual systems is available as needed or as indicated by the overall measurements. Information is accumulated in the Problem Management data base. Each outage can be identified by its date of occurrence, system, duration, and cause code.

Data can be analyzed by categories, problem type, environment, or time of day, to determine if a common cause for several outages exists. The time to recover is statistically analyzed on a regular basis to produce trend analysis reports.

8.4.3. Recovery Management Self-Assessment Questionnaire

Annually, each site should perform a self-assessment using the following list of questions. Any areas for which a negative answer is given should be addressed immediately. For each positive answer, a site should explain how they would demonstrate their effectiveness in that area. The self-assessment results should be documented along with any action plans which result from the self-assessment.

The questions in the following table are answered using one of the responses shown in the response list below:

- **Response List**

Response list:

- **Y** = Yes, effective.
- **I** = Incomplete. An explanation and action plan is required.
- **N** = No. An explanation and action plan is required.
- **na** = Not Applicable. An example is required.
- **<note>** Adjacent to each question and answer is a response column in which to amplify the answer.

Figure 4: Response List

Question	Answer	Response
Is the Recovery Management process communicated to all affected areas within the organization?		
Do you have a documented process for Recovery Management (body of this document)?		
Does the Recovery Management process interface with other SMC disciplines?		
Are schedules and work flows documented (e.g., daily, weekly, monthly, etc...)?		
Are major changes to Recovery Management process submitted and controlled through the Change Management discipline?		
Have appropriate tools been implemented to assist owner / client management in managing passwords and classified information?		
Are procedures in place for controlling and logging unusual occurrence's and reporting them to Problem Management?		
Is there a procedures for taking corrective action when Recovery Management process service levels provided do not meet the service level agreements?		
Is the Recovery Management process periodically reviewed and updated to ensure its effectiveness?		
Are reports prepared for use by appropriate levels of personnel in their day-to-day operation?		

Figure 5: Recovery Management Self-Assessment form (part 1 of 3)

Are post-recovery reports prepared for use by appropriate levels of management (measurement)?		
Are summary reports prepared as defined by management?		
Is the Recovery Management process communicated to all affected areas within the organization (i.e., distributed to all I/S departments)?		
Does the Recovery Management process interfaces with other SMC disciplines?		
Is periodic analysis done to evaluate the impact of a systems resource failure (including components such as hardware, software, data communications, environmental, etc.) on major application and services?		
Is periodic analysis done to assess current backup, recovery capabilities and to consider alternatives designed to improve availability (i.e., Post Recovery Outage Reviews)?		
Are recovery procedures documented for systems and applications that are critical to the business (i.e., CFIA, Major Component and CPU Recovery Plan)?		
Are the recovery procedures periodically reviewed and tested (CFIA updates from test and experiences - Testing Recovery Procedures)?		
Have availability and recovery service levels been defined with clients in service level agreements (i.e., mean time to recover from outages or disasters)?		

Figure 6: Recovery Management Self-Assessment for (part 2 of 3)

Are specific recovery procedures documented and followed for: • Control Elements ad Restricted Utilities? • Sensitive Programs (Recovery responsibility and Critical Business documents)? Are these documents contained within the CFIA?		
Are specific recovery procedures documented and followed for: • System compromise? • System penetration (recovery responsibility and Critical Business documents)? Are these documents contained within the CFIA?		

Figure 7: Recovery Management Self-Assessment for (part 3 of 3)

- **Checklist**

Based on the responsesto the above questions, the following checklist is marked and offered to show overall compliance for this discipline:

____ C = In compliance.

___ CR = In compliance - Risk accepted. Risk acceptance statement is on record with operating unit I/S management and has the concurrence of operating unit line management. A copy is to be submitted to the operating unit SMC Program Manager with the Systems Management Controls Report form.

___ N = Not in compliance. A consolidated explanation with action plan is required and is to be submitted to the operating unit - SMC Program Manager with the Systems Management Controls Report form.

___ NA = Not applicable. An explanation is required and is to be submitted to the operating unit SMC Program Manager with the Systems Management Controls Report form.

Site Process Coordinator Name: _____ Date: ___/___/___

Figure 8: Recovery Management Evaluation Checklist