Auditing Contingency Recovery Plans and Implementing Business Continuation Strategies for the future.

Presented by:
Thomas Bronack, President

Prepared by:
Data Center Assistance Group, Inc.
15180 20th Avenue
Whitestone, NY 11357
Phone: (718) 591-5553 Cell: (917) 673-6992
Email: bronackt@dcag.com
# Schedule of Events

## I. Introduction and Overview of Seminar  
09:00

## II. Auditing Contingency Plans  
09:15

A. Contingency Planning Concerns  
09:30

B. Overview of Contingency Planning  
10:00

C. Auditing Contingency Recovery Plans  
10:30

D. Discussion of actual Recovery Audits  
11:00

Lunch  
12:00

## III. Strategies for Eliminating Audit Exceptions  
1:00

A. Implementing Contingency Recovery Practices  
1:20

B. Optimizing Data Processing Operations  
2:00

C. Getting Started and Project Plan  
3:00

D. Discussion and actual work experiences  
4:00

E. Closing statements and wrap-up  
4:30
Auditing Contingency Recovery Plans

I. Performing a Risk Assessment:

A. General Recovery Parameters:

1. Contingency Operations,
2. Business Restoration,
3. Lead Times,
4. Responsibility for Disaster Recovery.

B. Disaster Recovery Needs:

1. Develop Recovery Plans,
2. Enhance Project Life Cycle and Systems Management,
3. Test Recovery Plans,
4. Implement Recovery Operations,
5. Maintain Recovery Plans,
6. Insure protection of business assets,
7. Assure adherence to Regulatory requirements.

8. Assure Insurance requirements are met.
9. Assure Vendor Contracts and Reciprocal Agreements are in place and maintained.

C. Develop Recovery Plan(s), as per existing Standards and Procedures.

D. Monitor Recovery Test(s) and Post Mortem meetings.


II. Implementing Contingency Planning:

A. Risk Assessment.

B. Organizational Structure:
   1. Contingency Command Center,
   2. Contingency Coordinators,


D. Recovery Plan Testing.

E. Recovery Plan Maintenance.
III. Systems Management and Controls:

A. Problem and Crisis Management:
   1. Help Desk,
   2. Problem Escalation,

B. Change Management and Quality Assurance.

C. Inventory and Asset Management.

D. Operations and Network Control Center Operations.

E. Evaluation Process and Effectiveness Measurements.
DCAG Services

Company Overview:

* Established in 1979,
* Founder, Thomas Bronack, is president and CEO.

DCAG supplies Data Processing and Office Support services, which include:

* Full-range of Consulting Services,
* Permanent Placement,
* Temporary Placement,
* Outsourcing.
* Providing solutions for Information Systems problems.
* Unique understanding of Systems Management.
* Knowledge of Equipment Manufacturers, Software Suppliers, and Leasing.

* DCAG can assist through the following services:
  - Inventory and Configuration Management,
  - Analyzing the use of Resources to meet Business Needs,
  - Enterprise-Wide platform configurations and connectivity,
  - Disaster Avoidance and Contingency Planning procedures,
  - Asset Management,
  - Systems Management disciplines,
  - EDP Security and Access Controls,
  - Business Optimization,
  - Documentation and Training services,
  - Full range of Engineering, Development and Implementation services,
  - Full range of Support and Maintenance services.
Presentation Agenda:

• Contingency Planning concerns,

• Auditing Contingency Recovery Plans,

• Strategies for eliminating Audit Exceptions going forward,

• Implementing Contingency Recovery practices and testing recovery plans,

• Optimizing data processing operations, while safeguarding business facilities and processes.
Contingency Planning Concerns

- Why you need a Recovery Plan,
- Overview of Contingency Planning,
- Establishing Contingency Planning,
- Contingency Planning Functions and Responsibilities,
- Creating, Testing, and Implementing Contingency Plans,
- Supporting and Maintaining Contingency Plans.
Why you need a Recovery Plan

* Justifying the Need for a Recovery Plan.
  - Enterprise-Wide Commitment
  - Disaster and Business Recovery Planning implementation.
  - Risk Management implementation.

* Laws and Regulators.
  - Controller of the Currency (OCC).
    - OCC-177 Contingency Recovery Plan.
    - OCC-229 Access Controls.
    - OCC-226 End-User computing.

* Penalties.
  - Three Times the Cost of the Outage.
  - Jail Time is possible.

* Insurance.
  - Business Interruption Insurance.
  - Directors and Managers Insurance.

“For Contingency Planning to be successful, a company-wide commitment, at all levels of personnel, must be established and funded. Its purpose is to protect the company, its business, its shareholders, and its employees.”

“Define all Regulatory, Legal, Financial, and Industry rules and regulations that must be complied with, and assign the Risk Manager with the duty of insuring that these exposures are not violated”.

“Have the Legal and Auditing Departments define the extent of Risk and Liabilities, in terms of potential and real Civil and Criminal damages that may be incurred.”.

“Once you have defined your exposures, construct an insurance portfolio that protects the business from sudden damages that could result from a disaster event.”
The best Insurance against disasters.....

"The best protection against disasters is a current and accurate Recovery Plan, that is frequently tested...."

“Both Disaster Recovery Plan(s) for data centers, and Business Recovery Plan(s) for office locations must be implemented. Combining all recovery planning efforts will improve the organization’s ability to protect itself from encountered disaster events, while training personnel to react to potential disaster events and conditions.”
Overview of Contingency Planning

* Overview of data processing environment,
* Application Profile,
* Application Interconnections,
* Contingency Recovery Disciplines,
* Contingency Recovery Interfaces,
* Contingency Recovery Structure.
Overview of Data Processing

* General Overview,
* Job Development through Production Acceptance,
* Overview of Mid-Range Environments,
* Overview of Local Area Networks,
* Vital Records Management and Electronic Vaulting,
* Application Profile,
* Application Interconnections.
General Overview.

“Keeping data in sync at Primary and Alternate Site...”
Job Development through Production Acceptance

**Development**
- JOB
- PROC
- PGM
- CNTL
- Static Data
- Dynamic Data
- Job Run Book

**Testing**
- Test Data
- Bench Mark

**Quality Assurance**
- Job Analysis for flow and resource usage
- Job JCL Scanning for Standard Adherence
  - Delta Deck
  - Stage I
  - Stage II

**Production Acceptance**
- Automated Operator
- Library Management
- Disaster Recovery
- EDP Security
- DASD Management
- Job Setup & Scheduler
- Restart / Recovery

**Production**
- Override Library
- Job Library
- Scheduler Library

Endeavor for Component and Release Management

Delta Deck
Changes to JOB and its resources.

Input
Output

OK
Yes, Proceed
No, Return

OK
Yes, Proceed
No, Return
Overview of Mid-Range Environments

Legend:
1. Normal processing is conducted at site(s).
2. Data is backed-up from DASD to Tape for archival at Off-Site Vault.
3. Contingency Facility is used to process workload, if Production Location is lost.
Overview of Local Area Network Environments

- Gateway
- Server
- Data
- Pgms.

Shared Resources under Network Control

- To Other LAN environments
- To Mainframe and Mid-Range Systems
- Data
Vital Records Management and Electronic Vaulting

Company Facilities

Mainframe Computer

Local Area Network

Company Offices

Computer
Recovery Facility

Off-Site Vault

Mid-Range
Computer

Office
Recovery Facility

Recovery Facilities and Vital Records Management
“Prioritizing applications as to their criticality, is based upon business needs and feed files used to initiate the application in question. Because of this, the synchronization of Back-up and Restoration must be planned and implemented to satisfy application needs in the order of their critical importance and processing sequence.”
<table>
<thead>
<tr>
<th>* Auditing Contingency Recovery Plans</th>
</tr>
</thead>
<tbody>
<tr>
<td>* How disasters occur, and avoiding them,</td>
</tr>
<tr>
<td>* Contingency Recovery Disciplines,</td>
</tr>
<tr>
<td>* Contingency Recovery Interfaces,</td>
</tr>
<tr>
<td>* Contingency Recovery Structure,</td>
</tr>
<tr>
<td>* Contingency Recovery Standards and Procedures,</td>
</tr>
<tr>
<td>* Contingency Recovery Testing,</td>
</tr>
<tr>
<td>* Maintaining Contingency Recovery Plans.</td>
</tr>
</tbody>
</table>
“Since disasters are no more than problems affecting critical components, it stands to reason that the elimination of standards violations will reduce problems and avoid the likelihood of disasters.”

An unscheduled business interruption.

Problems cause disasters when they affect critical business services. Problems are defined as deviations from standards, or missed business delivery.

To safeguard against Disasters, insure that standards are validated for critical resources.
Contingency Command Center:

- Housed within Command Center,
- Activated during Emergencies,
- Relates problems to Recovery Plan,
- Activates appropriate Recovery Team(s),
- Coordinates Recovery Actions,
- Maintains status on disaster and crisis situations,
- Communicates with;
  - Network Control Center,
  - Operations Control Center,
  - Help Desk,
  - Technical Staff, and
  - Management.
- Will escalate recovery actions, if necessary.
Providing a centralized control point for application and communications support, the Command Center can recognize problems and activate appropriate recovery teams in response to crisis situations.
Specific Recovery Techniques

On-Line Recovery
Transaction Messages and Codes
Forward Recovery

Batch Recovery
Job Overrides
Proc Recovery Steps
Messages and Abend Codes

Data Recovery
DASD Management responsibilities
Data Base responsibilities
Backup and Restore procedures
Vital Records Management

Communications Recovery
Problem Circumvention’s

Automated Recovery via Communications Management Controller
Load Balancing and Error Recovery

Incorporating Recovery within Change Control
Error Messages and Abnormal Completion (ABEND) Codes
Testing Recoveries prior to Quality Control.

Help Desk
Problem Scripts

Diagnostic Approach

Job Card
Proc Steps
Proc COND Steps for Recovery

Job Override
Production Steps
Recovery Steps driven by COND statements on Production Steps.

Job Runbook
Job Profile,
Set-up,
Processing,
Balancing,
Output Distribution,
Error Conditions,
Recoveries,
Contacts.

Messages and Codes
Meaning
Actions to take
Possible Causes
Recovery Techniques and Personnel Involvement

Problem -> Capture Symptoms -> Analyze -> Circumvent -> Document -> Report

Operations Control Center (OCC) -> Network Control Center (NCC) -> Help Desk Staff

Tools:
Omegamon, AF / Operator.

Tools:
Omegamon, Netview.

Resolve

Log, Route, Escalate, Track

Comm. Support Staff -> Systems Support Staff -> Applications Support Staff -> Production Support Staff

3/17/2012
Auditing Contingency Plans Page: 26
Communications Sessions are established between users connected on terminals (or PCs) and mainframe resident applications. These sessions are transmitted over communications lines and through Transmission Communications Controllers (TCU’s), or Local Area network (LANs). Data can be forwarded through Private Networks (i.e., owned by company), or Public Network (i.e., the Internet, America On-Line, MSN, etc.).

When problems arise, the NCC Operator can take corrective action by varying the failing component off-line and activating a back-up component (if an alternate is available). The elimination of a Single-Point-Of-Failure, so that recovery operations can be accomplished, is the most advantageous method for maintaining availability within the communications environment.

Back-Up data files should be created for all critical information resident in the communications environment. These Vital Records should be safeguarded in the same fashion as was described for Data Recovery (Local, Remote and Off-Site Vaulting).
Contingency Recovery Disciplines

Contingency Planning

Disaster Recovery

Business Recovery

Risk Management

EDP Protection:
2. Data Sensitivity and Access Controls.
4. Mainframe / Mid-Range disaster recovery.

Corporate Asset Protection:
1. Inventory Control.
2. Asset Management.
3. Configuration Management.
5. Office Recovery.

Management Controls:
1. Exposures.
2. Insurance.
3. Legal / Regulatory Requirements.
5. Vendor Agreements.

Charter:
1. Eliminate Business Interruptions.
2. Ensure Continuity of Business.
4. Adhere to Legal / Regulatory Requirements.
“Establishing interfaces with key departments will allow for the inclusion of corporate-wide recovery procedures (i.e., Security, Salvage & Restoration, etc.) in department specific Recovery Plans.”
Contingency Recovery Structure

- **Corporate Level**
  - Contingency Command Center
  - Executive Management
    - Public Relations
    - Recovery Coordinator(s)
    - Recovery Administration

- **Divisional Level**
  - Business Recovery Coordinator

- **Departmental Level**
  - Disaster Recovery Team
    - Team Manager
    - Team Members
    - Team Tools
  - Disaster Recovery Team
    - Team Manager
    - Team Members
    - Team Tools
  - Disaster Recovery Team
    - Team Manager
    - Team Members
    - Team Tools
Contingency Recovery Standards and Procedures

* Regulatory Requirements,
* Critical Business Applications,
* Critical Support Services,
* Data Sensitivity and Access Controls,
* Contingency Structure and Teams,
* Develop, Test and Maintain Recovery Plans for Data Processing and Business Locations,
* Training for team members and awareness for entire staff.
Contingency Recovery Testing

* Unit testing for each Recovery Plan,
* System testing for various recovery scenarios,
* Tools for Recovery Teams,
* Log events and conduct Post Mortems,
* Include New Technology whenever possible,
* Upgrade company-wide Standards and Procedures, as needed.
Maintaining Contingency Recovery Plans

* Have hardcopy Contingency Plans numbered,

* Update Recovery Plans after tests, or when New Technologies are added,

* Provide reviews of Updated Plans,

* Distribute hardcopy versions of New Plans to designated individuals,

* Maintain Log of hardcopy Plans.
Strategies for Eliminating Audit Exceptions

* Production Acceptance, Quality Control and Project Life Cycle,

* Data Sensitivity and Vital Records Management,

* Utilizing Automated Tools,

* Elimination of Single-Point-Of-Failure concerns,

* Inventory / Asset Management,

* Problem and Crisis Management,

* Work-Flow automation through Re-Engineering processes,

* Training and Awareness programs.
Implementing Contingency Planning practices

* Contingency Recovery Goals,

* Disaster Recovery Objectives,

* Business Recovery Objectives,

* Risk Management Objectives.
Contingency Recovery Goals

* Safeguard against business interruptions,

* Protect Corporate Assets,

* Recover from encountered disasters, or prolonged outages.
Disaster Recovery Objectives

* Define critical jobs and their components,

* Coordinate Vital Records Management,

* Create / Test / Maintain Contingency Plans,

* Incorporate new technologies and practices that improve the recovery process,

* Maintain the Contingency Plans in a constant state-of-readiness.
Business Recovery Objectives

* Corporate Asset Protection,

* Inventory Control,

* Business Continuity,

* Office Recovery.
Risk Management Objectives

* Evaluate Risks and Exposures (Cost Justification),

* Obtain required insurance and formulate reciprocal agreements to protect resources,

* Assure proper EDP Security and Access Controls,

* Insure adherence to Legal and Regulatory needs,

* Formulate and manage Vendor agreements,

* Provide management reporting.
* Corporate and Departmental Recovery Responsibilities,

* Workload Re-Engineering to obtain information at the point of its inception, or alteration,

* Crisis and Problem Management drives Recovery Operations,

* Automated Recoveries incorporated into environment,

* Well trained staff and Frequently Tested Recovery Plans.
## Corporate and Departmental Recovery Responsibilities

### Corporate Responsibilities

**Security** Department for building access, Police, Fire, and Emergency Medical.

**Facilities** for Salvage & Restoration.

**Personnel** for casualties and First Aid Training.

**Public Relations** for statements to Press and other types of Media.

**Purchasing** for equipment acquisition.

**Administration** for office supplies and coordination of logistics and Essential Services / Suppliers.

**Leasing** to obtain equipment.

**Legal and Audit** departments to insure compliance to regulatory requirements.

**Audit** to review recovery plans for compliance to business needs.

### Recovery Planning

**Define Recovery Sections** to be completed by Corporation and individual Departments.

Define **Disaster Recovery Manual** sections, their format and content.

Establish **Contingency Recovery Organizational** Structure.

Formulate **Disaster Recovery Teams**.

**Create** Disaster Recovery Plans.

**Test and Implement** Disaster Recovery Plans.

Formulate **Disaster Definition and Declaration** procedures.

**Coordinate** disaster event to Disaster Team activation process.

**Maintain** Disaster Recovery Plans.

### Recovery Sites

**Contingency Command Center** - Small to Large, in relationship with scope of disaster event.

**Data Center Recovery Site**

**Office Recovery Site**

### Problem Management

**Problem** definition and escalation procedures.

**Change Management** for New and Altered applications and environments.

**Help Desk** procedures and scripts to address problem events, with escalation process in place for declaring disasters and activating Disaster Teams.
Contingency Recovery Functions and Responsibilities

Define Business and Regulatory Requirements.

- Risk Assessment and Data Sensitivity Study.
- Vital Records and Vault Management.
- Critical Job Stream analysis.
- Recovery Facility requirements definition.

Create, Test, and Maintain Contingency Plans.

- Formulate Recovery Teams, with Team Leaders and Recovery Coordinator.
- Establish a Contingency Command Center organization.
- Train recovery personnel and provide tools, if needed.
- Create Recovery Plans and test their ability to safeguard business operations.
- Insure that Recovery Plans are maintained in a current and accurate manner.
- Report to management on the corporations ability to recover business applications and continue supplying services to clients.
- Formulate recommendations to improve recovery operations through new technologies and procedures.

Use Automated Tools and Interfaces, if possible.
The ideal environment

* Informational areas automatically supply Contingency Recovery information.

* Contingency Plans automatically updated.

* Frequent Testing of Contingency Plans.

* Well trained staff.
Getting Started

* Strong Management Backing and Commitment.

* Contingency Planning Committee.

* Risk Assessment and Business Impact Analysis (BIA).

* Personnel Job Functions and Responsibilities.

* Contingency Plan Creations.

* Contingency Teams and Tools.

* Vendor and Reciprocal Agreements.

* Frequent Testing and Maintenance of Contingency Plans.
Project goals and deliverables.

1. Validated inventory of resources.

2. Work Load Analysis completed.

3. Work Station Configurations defined.
   - Upgradeable resources identified.
   - Obsolete resources identified for Surplus disposal.
   - Migration Plan for consolidating resources developed.

   - Critical Resource Review conducted.
   - Recovery personnel selected and trained.
   - Single point of failure identified and eliminated.
   - Problem Management procedures used to circumvent problem situations before they become a crisis.
   - Tested current and accurate Recovery Plan.
5. Asset Management System implemented.
   - Asset Management Repository implemented.
   - Vendor and Manufacturer Agreements negotiated.
   - Personnel interface activated.
   - Responsible for Asset Acquisition, Redeployment, and Termination.


7. Performance Optimization procedures in place.


9. Training provided to personnel.
Inventory Management System

<table>
<thead>
<tr>
<th>Resource Category</th>
<th>Type</th>
<th>Serial No.</th>
<th>Criticality</th>
<th>Location</th>
<th>Vendor</th>
<th>Contract Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hardware</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Software</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Fixed Asset</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personnel</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Personal Computers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LAN</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Inventory Management Tasks

* Validate inventory and financial records.

* Categorize resources by; owner, type, location and vendor.

* Identify inefficiencies in resource configurations.

* Formulate resource configurations that are best suited to support present and future business needs.

* Select vendor(s) to support business needs.

* Determine end-user cost allocations and charge-back.

* Negotiate Volume Purchase Agreements with vendors to optimize financial considerations for resources.

* Process is becoming easier through Windows/XP and Windows/NT accounting records and utilities.
1. Define environments to be monitored (Inventory).
2. Establish measurement criteria.
3. Implement Capacity and Performance reporting.
4. Analyze reported results and formulate conclusions.
5. Develop strategies to resolve performance flaws.
6. Implement resolutions and continue to monitor and analyze reported information.
## Define Work Station Configurations

<table>
<thead>
<tr>
<th>Job Function:</th>
<th>LAN</th>
<th>PC Configuration</th>
<th>Applications</th>
<th>Tools</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

1. Define configurations needed to support Job Functions, by type.
2. Identify upgradeable resources.
3. Identify obsolete resources.
4. Establish equipment and application guidelines, company-wide.
5. Create Vendor relationships for resources and software.
1. Asset **Acquisition** procedures.
2. Asset **Redeployment** procedures.
3. Asset **Termination** procedures.
6. Vendor and Manufacturer Agreements.
7. Personnel interface to guaranty adherence to Asset Management standards and procedures.
Contingency Planning

Charter:
1. Eliminate Business Interruptions.
2. Insure Continuity of Business.
4. Legal / Regulatory Requirements.

EDP Protection:
2. Data Sensitivity and Access Controls.

Corporate Asset Protection:
1. Inventory Control.
2. Asset Management.
4. Office Recovery.

Management Controls:
1. Exposures.
2. Insurance.
3. Legal / Regulatory Requirements.
5. Vendor Agreements.
Contingency Recovery Interfaces

- Executive Management
- Data Processing
- Company Operations
- Auditing
- Public Relations
- General Services
- Personnel
- Facilities
1. Critical Path Applications and Jobs.
3. Isolation of Performance Flaws, or inadequate Capacity.
4. Strategies to resolve Performance Flaws and obtain additional Capacity.
5. Report to management on findings and recommendations.
6. Utilize Asset Management System to acquire, redeploy, or terminate resources.
Inventory Management

- Identify inventory records,
- Validate inventory and financial records,
- Identify resources by; owner, type, location and vendor,
- Establish current resource configurations,
- Identify inefficiencies in resource configurations,
- Formulate resource configurations that are best suited to support present and future business needs,
- Determine best vendor(s) to support present and future business needs,
- Determine end-user cost allocations and charge-back,
- Negotiate Volume Purchase Agreements with vendors to optimize financial considerations for resources.
Resource Performance Profile

- Identify application mix and define Critical Path,
- Implement Capacity and Performance reporting,
- Analyze reported information to isolate poorly performing applications and areas for improvement,
- Formulate strategies to implement Performance improvements,
- Present findings to management and gain approval,
- Review standards and Procedures to uncover areas for improvement,
- Optimize applications and the Critical Path,
- Update the Standards and Procedures to reflect performance and optimization methodologies.
Resource Financial Profile

- Categorize resources by financial type (i.e., rented, leased, owned, surplus, etc.),
- Compare present resource mix against standardized configurations,
- Identify resource migration candidates and resources to be discontinued or upgraded,
- Formulate Resource Migration Plan to create standard configurations in adherence to management goals,
- Formulate vendor contractual agreements in support of resource configurations,
- Integrate resource configuration guidelines within the facility and resource procurement areas.
Asset Management System

- Establish Asset Management charter and mission,
- Formulate Asset Management objectives,
- Identify interfaces to Asset Management System,
- Calculate data exchanges between functional areas and the Asset Management system,
- Upgrade supportive literature and develop training,
- Develop Asset Management Implementation Plan,
- Develop Asset Management Roll-Out Plan,
- Implement Asset Management Implementation and Roll-Out Plans,
- Monitor results and upgrade plans, if necessary,
- Provide training to required personnel.
Business Recovery Planning

• **Contingency Planning Principals:**
  - The need for a Recovery Plan,
  - Establishing Contingency Planning,
  - Contingency Planning functions and responsibilities,
  - Vendor contracts and reciprocal agreements.

• The ideal environment,
• Testing and maintaining the Contingency Plan,
• Documentation and materials requirements,
• Personnel training,
Overview of Business Continuity Planning and BIA’s

Recovery Plans direct personnel to restore business operations in response to encountered problems. The Help Desk escalates critical problems, initiates recovery plans, and manages recovery activities.
Business Impact Analysis (BIA)

Used to identify business operations that may need recovery plans and to then rate them as to risk exposure and their need for a recovery plan. As a result of this analysis, a report and presentation is provided to management defining exposures and the difficulty associated with creating recovery plans to protect operations and adhere to regulations.

Disaster Recovery Plan (D/R), or Business Continuity Plan (BCP)

D/R Plans are used to direct recovery procedures for specific functional areas (i.e., Data Center, Business Office, Vendor, Office Space, etc.) or conditions (i.e., Building/Floor closure, Hurricane, Flood, Loss of Power, etc.). The can cover small groups of people, or the entire organization. Recovery Plans are activated by the Contingency Command Center as a result of an encountered problem and are used to direct the actions of team members.

Contingency Command Center connection

Ties Recovery Plans to specific problem conditions, so that when problems are reported the appropriate Recovery Plan can be identified and activated. Pre-defined recovery actions and ad-hoc recovery teams can be directed via the Contingency Command Center staff.
Performance Optimization

- Identification of Applications on the Critical Path,
- Job Scheduling weaknesses,
- Resource usage weaknesses,
- System level performance improvements,
- Program level performance improvements,
- Manual interventions,
- Standards and Procedures weaknesses,
- Personnel training and skills inventory,
- Project Plan creation,
- Management report and presentation of findings,
- Project Plan implementation,
- Standards and Procedures upgrade and personnel training.
Project Management

- Project Management System,
- Management Checkpoints and Status Reporting,
- Inventory Management Project,
- Asset Management Project,
- Global Standards and Procedures Project,
- Disaster Avoidance and Business Recovery Planning Project,
- Application Performance and Software Re-Engineering Project,
- Systems Management Disciplines Project,
- Documentation and Training.
Benefits

• Inventory of all Assets within a Repository,

• Asset Management System to optimize resource costs,

• Disaster Avoidance and Contingency Planning,

• Systems Management Disciplines,

• Optimized Applications and Personnel,

• Reduced costs and improved efficiencies,

• Prepared for current and future workloads.
Tasks to be performed

- Formulation of Asset Management committee,
- Define scope and deliverable schedule,
- Identify project personnel,
- Formulate requirements definition,
- Develop and implement Pilot Project,
- Review results and implement Production Project Plan,
- Develop and implement Roll-Out Plan,
- Integrate Asset Management System with personnel responsible for resource acquisition and control,
- Upgrade Standards and Procedures,
- Provide training to designated personnel,
- Monitor system operation to insure optimization.
Services provided by DCAG

* Risk Assessment and Requirements Definition,

* Contingency Plan Creation and Maintenance,

* EDP Security and Access Controls,

* Vital Records and Library Management,

* New technologies and Strategies,

* Training and periodic audits of the Contingency Plan,

* DCAG can even perform all, or part, of the Contingency Planning function for its clients.