DCAG
Data Center Assistance Group, Inc.

Date: 3/21/2012

Composite presentation of

Disaster Recovery / Business Continuity Planning

Services provided by DCAG

And Tom Bronack

Thomas Bronack
15180 20th Avenue
Whitestone, NY 11357
Phone: (718) 591-5553
Cell: (917) 673-6992
Email: bronack@dcag.com
Web Site: www.dcag.com

Mission Statement and Scope

Mission Statement:

To develop and implement Continuity of Business (COB) Plans throughout the Organization for both Business Locations (Business Continuity Planning – BCP) and Data Processing Sites (Disaster Recovery Planning - DRP).

Scope:

- **Define Regulatory and Business Requirements associated with DR / BCP Plans.**
- **Perform a Risk Assessment to define the present state of Continuity of Business Planning.**
- **Identify gaps and exposures in existing BCP / DR Plans.**
- **Formulate methods for correcting exposures and eliminating gaps in Recovery Plans.**
- **Recommend a plan to implement a common BCP / DR process throughout the Company.**
- **Identify Internal and External personnel needed to support DR / BCP Implementation Plan.**
- **Establish Recovery teams and meet to define direction, objectives, needs, and timeframe.**
- **Create a DR / BCP project plan and gain management approval.**
- **Provide training to all team personnel so that everybody is aware of direction and they have an opportunity to raise concerns associated with the plan.**
- **Commence work on project plan and conduct periodic status meetings to ensure adherence to plan and timeframe.**

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.

> "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."

* **Laws and Regulators.**
  - Controller of the Currency (OCC).
    - OCC-177 Contingency Recovery Plan.
    - OCC-187 Identifying Financial Records.
    - OCC-229 Access Controls.
    - OCC-226 End-User computing.

> "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".

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

> "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.".

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

> "Once you have defined your exposures, construct an insurance portfolio that protects the business from sudden damages that could result from a disaster event."

- **Sarbanes–Oxley, HIPAA, and Graham-Leach-Bliley Acts.**

Business Continuity Planning Laws and Regulations

Federal Trade Commission (FTC):

- **GLB Privacy Rule – requires a written information security program and protection over customer data.**

Department of Health and Human Services (DHHS):

- **Final Security Regulations under HIPAA ("Security Rule" - comply by 4/2005) covering Electronic Protected Health Information. Responsible for: ensuring the integrity, confidentiality and availability of EPHI; protect EPHI against reasonably anticipated threats or hazards to its security or integrity and unauthorized use or disclosure.**
- **HIPAA (effective 4/2003) regulates all types of health information, including paper records.**

Securities and Exchange Commission (SEC):

- **Final rules for Section 404 of the Sarbanes-Oxley Act of 2002 to be effective 6/2004 for all SEC reporting companies. The 404 Rules require CEOs and CFOs to provide written report on state of data security and ability to recover from disaster event.**

Non-Compliance:

- **Can result in criminal and/or civil damages; liability and criminal prosecution for responsible companies and individuals.**
- **Although the rules stress the protection, preservation and retention of records and data, their principal purpose is the establishment of a control environment that will govern how transactions are to be carried out, recorded and reported in accordance with management's authorization and applicable policies and procedures.**
- **Additional losses include; reputation, trust, and general enterprise value.**
- **Go to www.erm.coso.org for details relating to Committee of Sponsoring Organizations (COSO) industry standards relating to Enterprise Risk Management (ERM). Documents can be downloaded.**

Existing Laws and their Consequences

	Graham-Leach-Bliley Safeguard Rule	HIPAA Security Rule	Sarbanes-Oxley 404 Rules	California SB 1386
Effective Date:	**May 23, 2002**	**April 21, 2003**	**June 5, 2003**	**July 1, 2003**
Compliance Deadline	**May 23, 2003**	**April 21, 2005**	**June 15, 2004** (for public companies with market cap. of $75 million or more) **June 15, 2005** (for other SEC reporting companies)	
Covered Entities	Financial Institutions as defined in the Bank Holding Company Act that possess, process, or transmit private customer information.	Organizations that possess, transmit, or process electronic protected health information (EPHI).	Publicly owned companies that file periodic reports with the SEC.	Any public or private entity that has unencrypted electronic personal information of California residents.
Purpose	Protect Customer Information from unauthorized disclosure or use.	Protect EPHI from unauthorized disclosure or use.	Provide senior management assessment of effectiveness of company's "internal controls for financial reporting" and attestation by independent auditors.	Protect California residents from Identity Theft.
Operative Mechanisms	**Information Security Program:** • Responsible Employee Selection, • Risk Assessment, • Information Safeguards and Controls, • Oversight of "Service Providers", • Testing and Monitoring.	**Security Safeguards:** • Risk Assessment, • Policies and Procedures to control access, • Physical Security Measures, • Contingency Plan, •Appointment of Security Officer, • Training and communication to increase awareness, • Audits and maintenance of Audit Trails, • Agreements with "business associates", • Testing and Evaluation.	Internal Control Framework: (Coso Framework or Equivalent) • Control environments – Compliance and Ethics, • Risk Assessment and Analysis, • Control Activities – policies, procedures, controls, • Information and Communications, • Monitoring or operations and control activities to determine continuing effectiveness of internal controls.	
Criminal Consequences of Noncompliance	Fines and Imprisonment for up to 5 years.	Fines to $250,000 and imprisonment for up to 10 years.	Fines up to $5 million and prison sentences for up to 20 years for deliberate violations.	Civil liability to any injured California resident.

Corporate and Departmental 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.

The "Ten Step" Process

Recommended by the Business Continuity Institute for BCP (see: www.thebci.org)

1. **Project Initiation and Management.**
2. **Risk Evaluation and Control.**
3. **Business Impact Analysis (BIA).**
4. **Developing Business Continuity Strategies.**
5. **Emergency Response and Operations.**
6. **Designing and Implementing Business Continuity Plans.**
7. **Awareness and Training Programs.**
8. **Maintaining and Exercising Business Continuity Plans.**
9. **Public Relations and Crisis Communications.**
10. **Coordinating with Public Authorities.**

Contingency Planning Strategy

(FEMA) EMERGENCY MANAGEMENT PREPAREDNESS – PROJECT PLAN

THE PLANNING PROCESS:

1. Establish a Planning Team.
2. Analyze Capabilities and Hazards.
3. Develop the Plan.
4. Implement the Plan.

EMERGENCY MANAGEMENT CONSIDERATIONS:

1. Direction and Control.
2. Communications.
3. Life Safety
4. Property Protection.
5. Community Outreach.
6. Recovery and Restoration.
7. Administration and Logistics.

HAZARD SPECIFIC INFORMATION:

1. Fire.
2. Hazardous Materials Incidents.
3. Floods and Flash Floods.
4. Tornadoes.
5. Severe Winter Storms.
6. Earthquakes.
7. Technology Emergencies.

APPENDICES:

1. Vulnerability Analysis Chart.
2. Training Drills and Exercises Chart.
3. Information Sources (where to turn For additional information).

Getting Started

- **Strong Management Backing and Commitment.**
- **Contingency Planning Organization:**
  - **Contingency Recovery Interfaces.**
  - **Systems Management Disciplines.**
  - **Component and Release Management.**
  - **Problem Management Overview.**
  - **Project Management, Goals, and Deliverables.**
  - **Business Recovery Planning.**
  - **Vital Records Management Personnel Functions.**
  - **Integrating DR and BCP Plans within Command Center.**
  - **Informational Requirements and Workflow Process Integration.**
  - **Standards and Procedures.**
  - **Awareness and Educational Training.**
- **Risk Assessment and Business Impact Analysis (BIA).**
- **Contingency Plan Creation, Testing and Implementation.**
- **Contingency Planning Support and Maintenance.**

Performing a Risk Assessment or Needs Analysis

A. Review General Recovery Parameters:

1. Contingency Operations;
2. Business Restoration;
3. Lead Times;
4. Responsibility for Disaster Recovery;
5. Standards and Procedures Manual.

B. Disaster Recovery Needs Analysis:

1. Assure adherence to Regulatory requirements;
2. Insure protection of business assets through Asset Management, Inventory Control and EDP Security;
3. Enhance Project Life Cycle and Systems Management for BCP;
4. Assure Insurance requirements are met;
5. Assure Vendor Contracts and Reciprocal Agreements are in place and maintained;
6. Review Recovery Plan Development;
7. Review Recovery Plan Testing;
8. Review Recovery Operations;
9. Review Recovery Plan Support and Maintenance procedures.

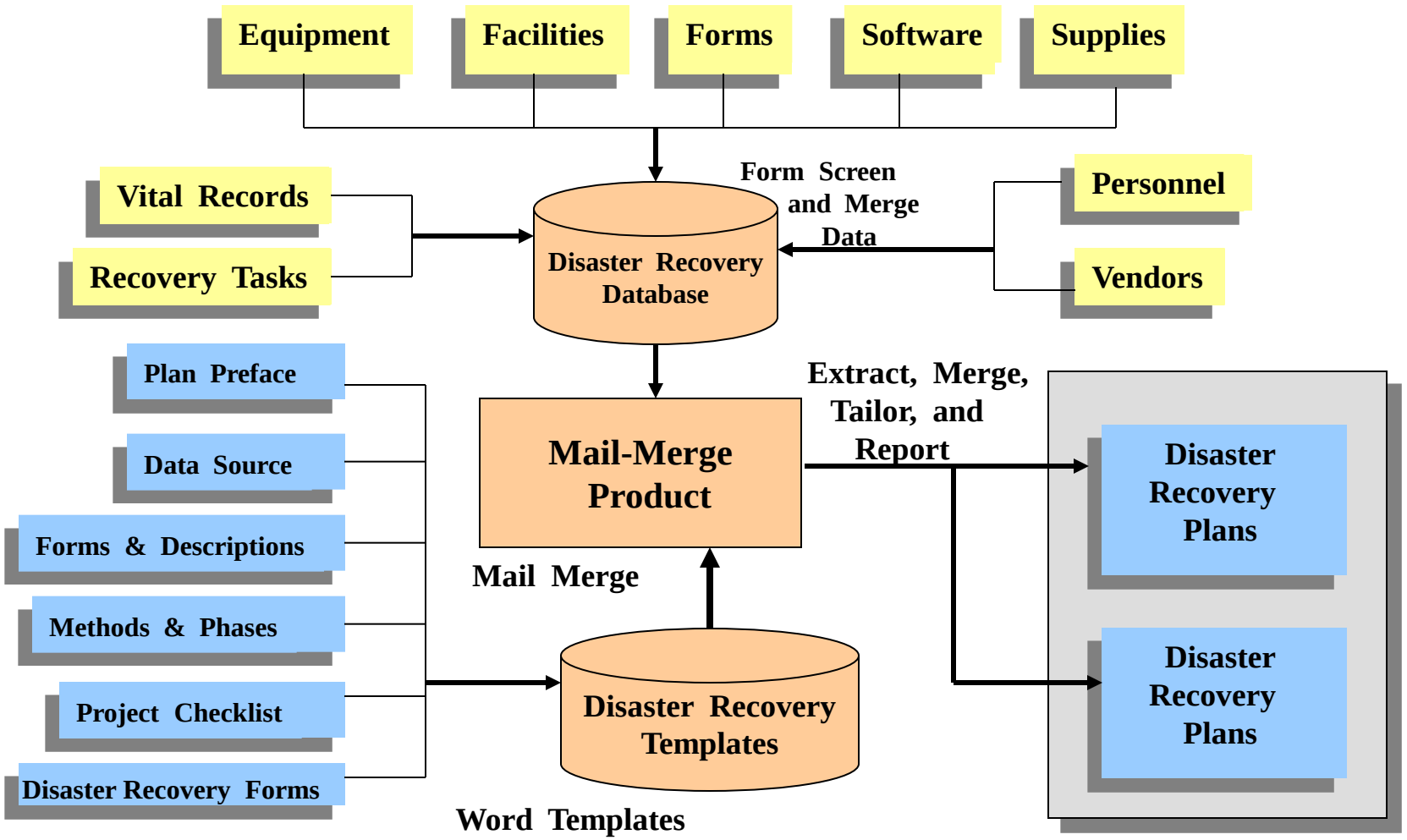
C. Developing Recovery Plan(s), as per existing Standards and Procedures.

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

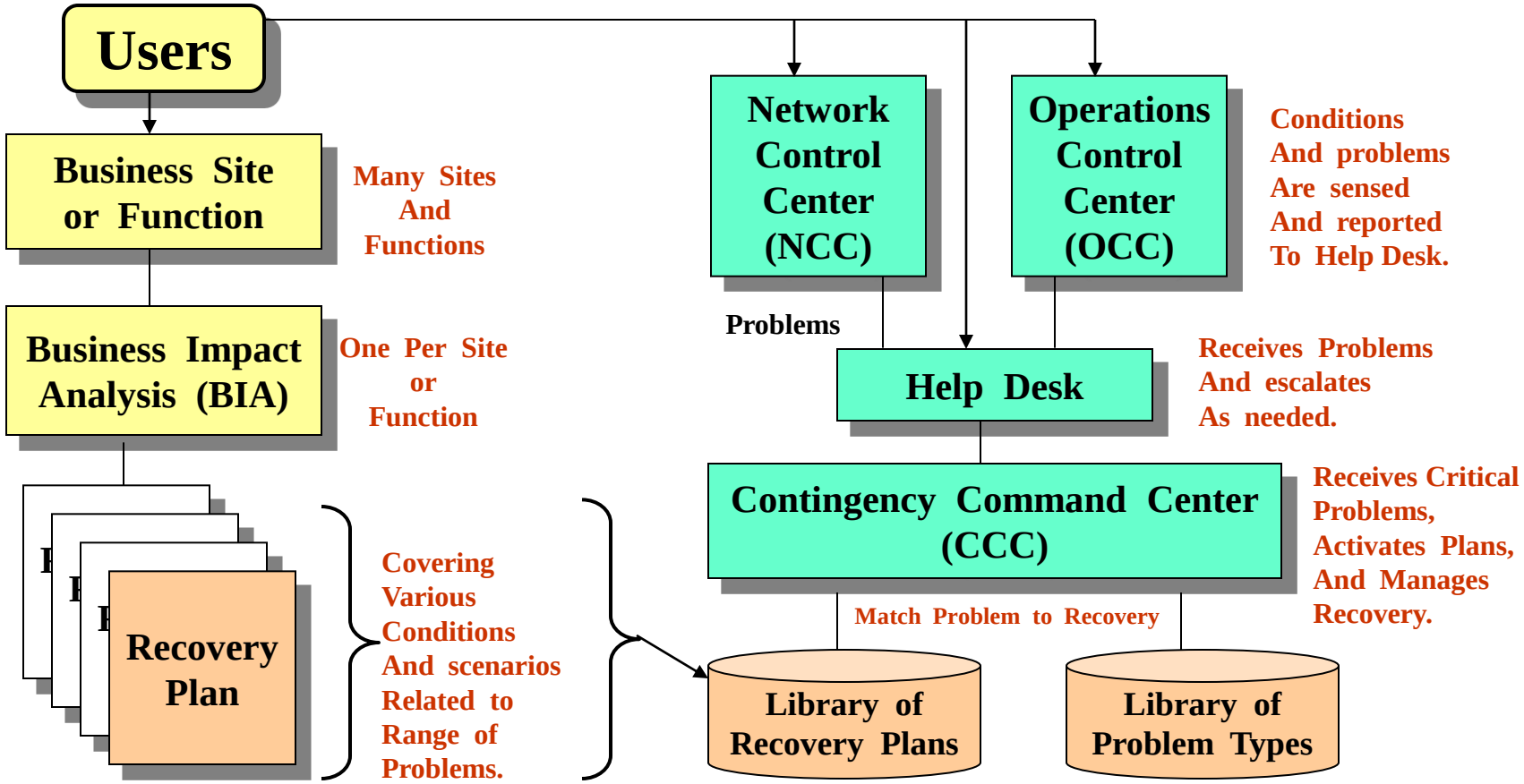
E. Reviewing Recovery Plan Maintenance Standards and Procedures.

F. Review of Standards and Procedures for Problem and Crisis Management.

Disaster Recovery Plan Data Sources and Output Generation



Overview of Business Continuity Planning and BIA's

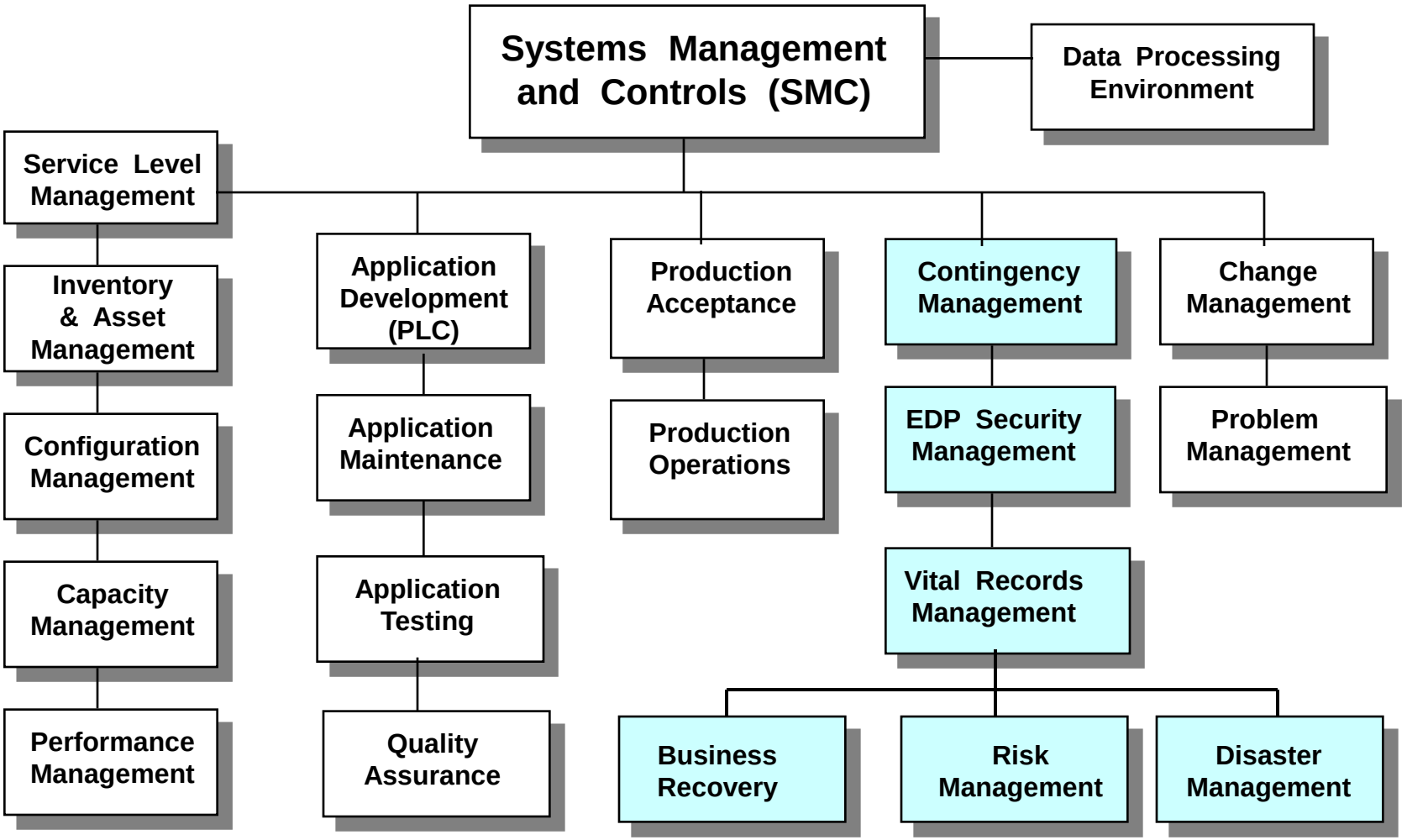


Recovery Plans direct personnel to restore business operations in response to encountered problems. The Help Desk escalates critical problems, initiates recovery plans, and manages recovery activities.

Strategies for Eliminating Audit Exceptions

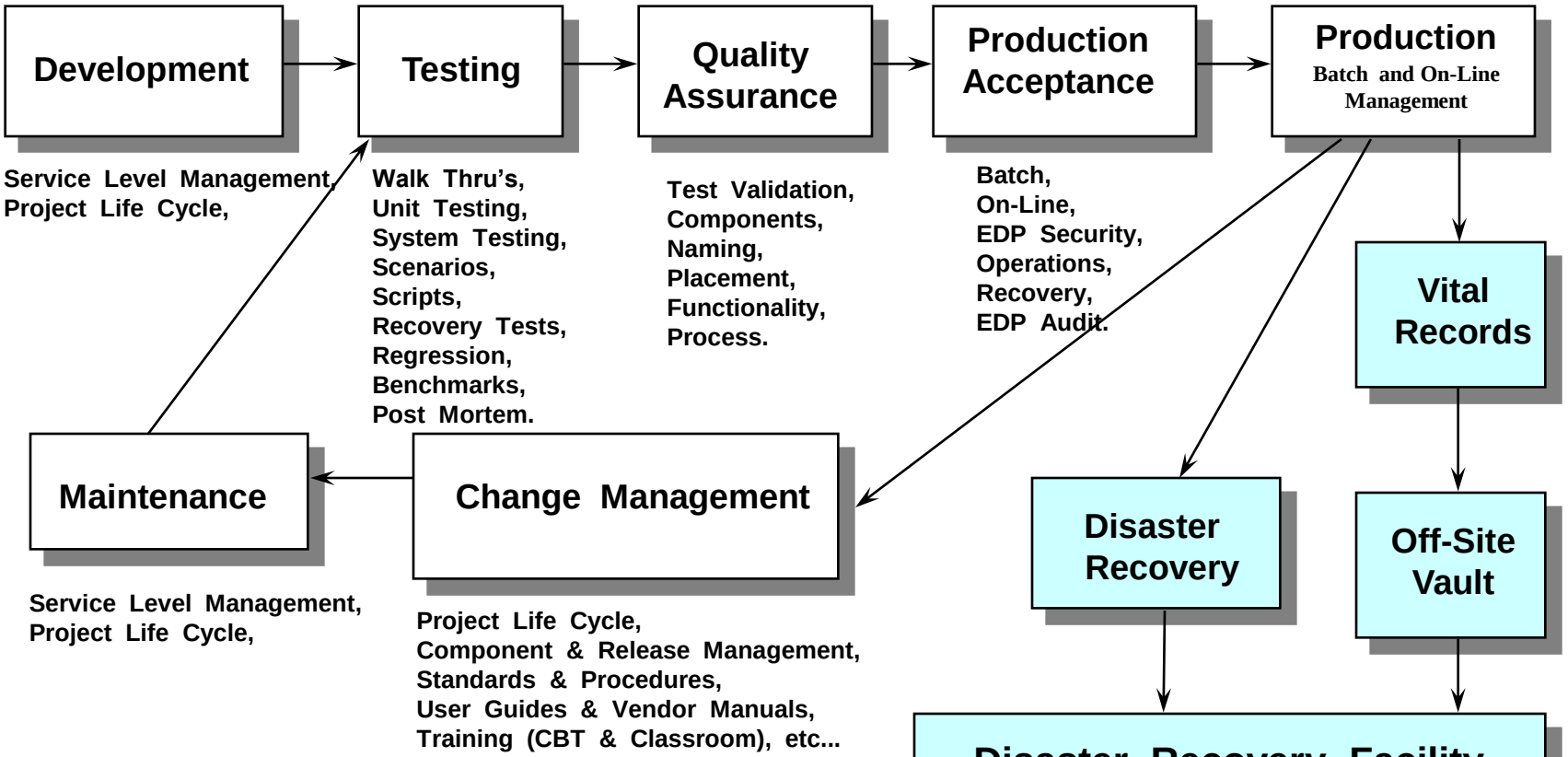
- **Review of Compliance Requirements (Business and Industry)**
- **Data Sensitivity, EDP Security and Vital Records Management,**
- **Production Acceptance, Quality Control and Project Life Cycle,**
- **Utilizing Automated Tools,**
- **Elimination of Single-Point-Of-Failure concerns,**
- **Inventory / Asset Management,**
- **Problem and Crisis Management,**
- **Work-Flow automation through Re-Engineering processes,**
- **Training and Awareness programs.**

Systems Management Organization



Systems Management Controls and Workflow

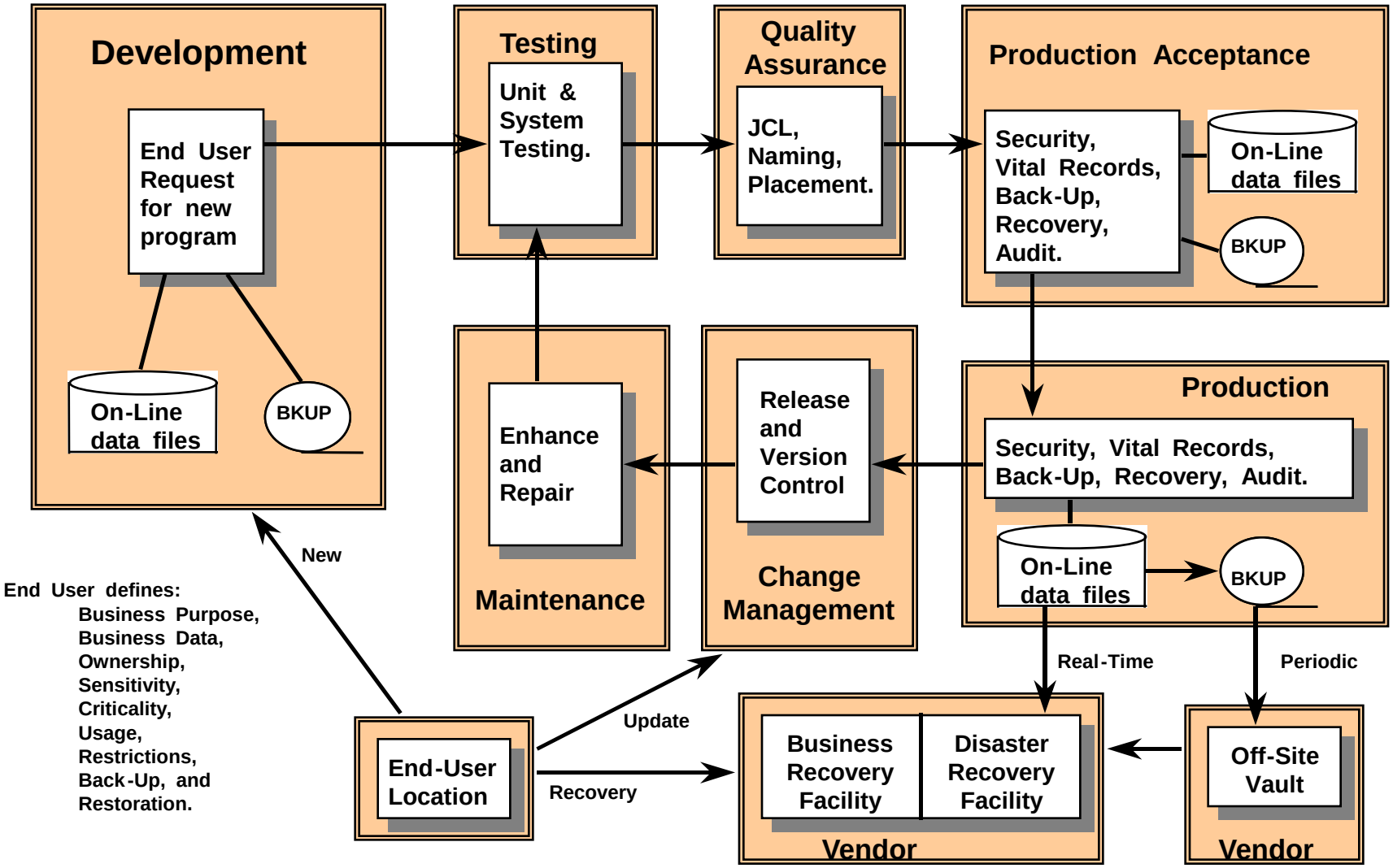
Service Level Reporting, Capacity Management, Performance Management, Problem Management, Inventory Management, Configuration Management.



A Forms Management & Control System, used to originate work requests and track work until completed, will facilitate optimum staff productivity and efficiency.

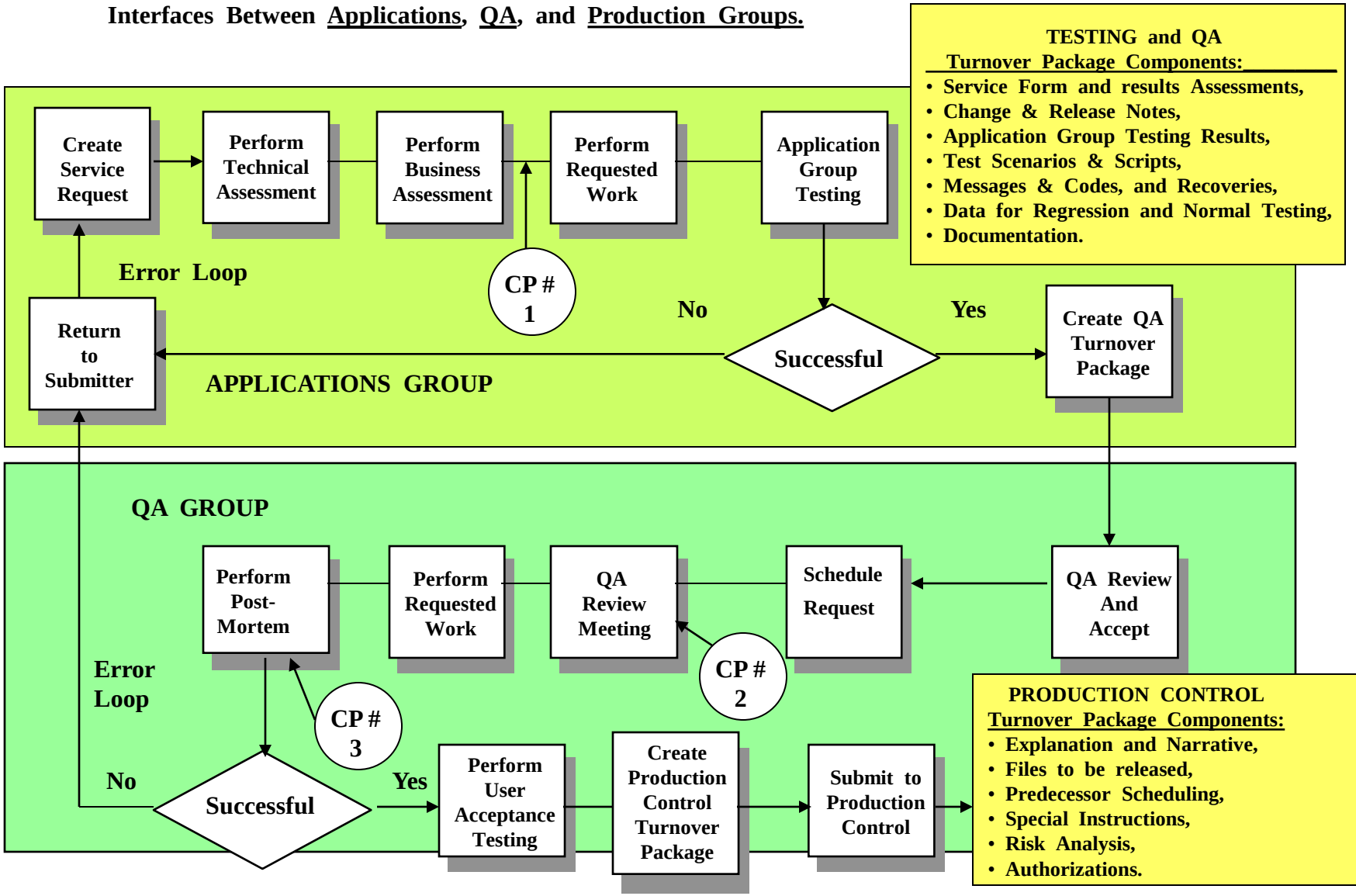
Application Life Cycles and Business Recovery Planning

(Development through Change Management and Maintenance)

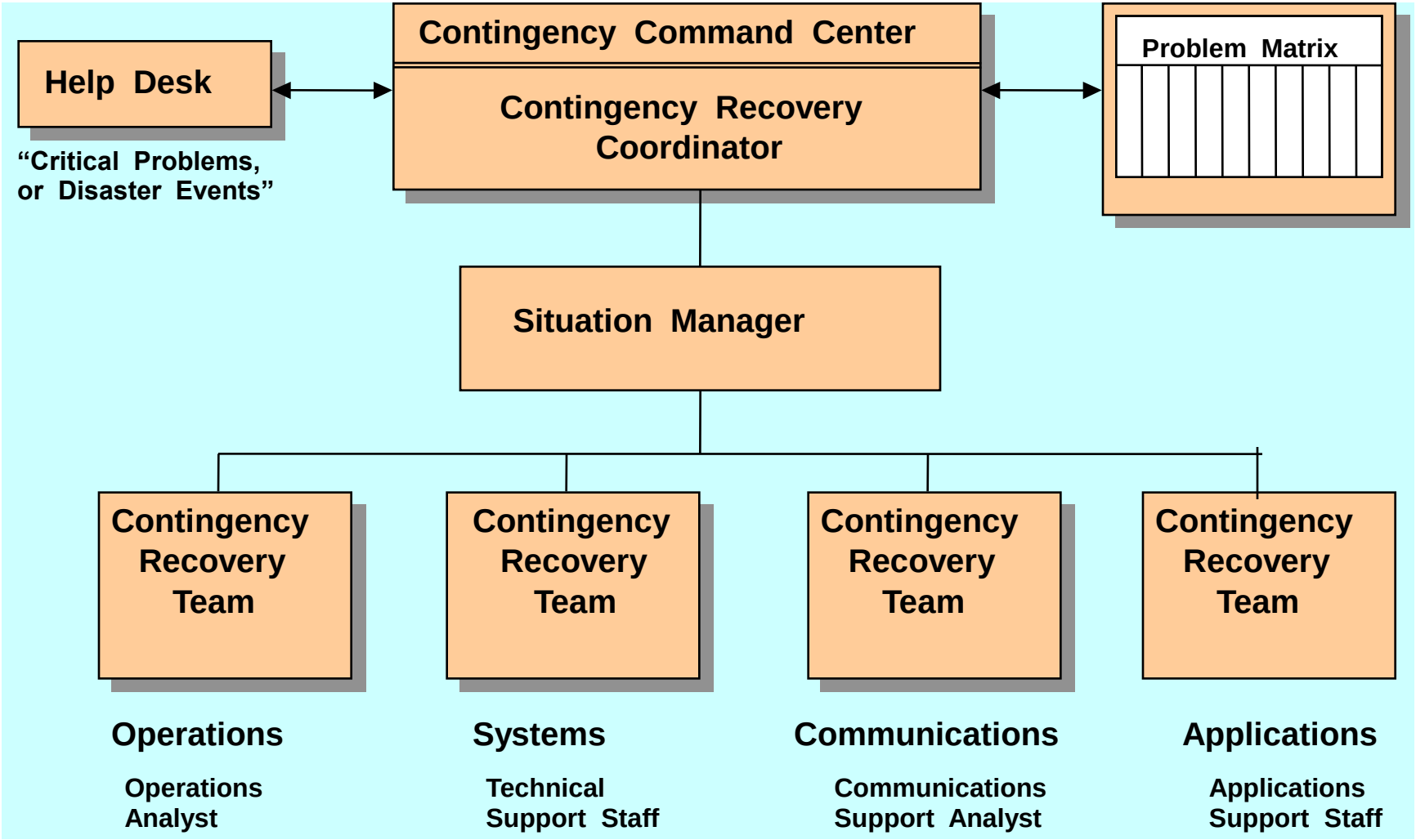


Quality Assurance and PLC Checkpoints

Interfaces Between Applications, QA, and Production Groups.



Contingency Organization in Action

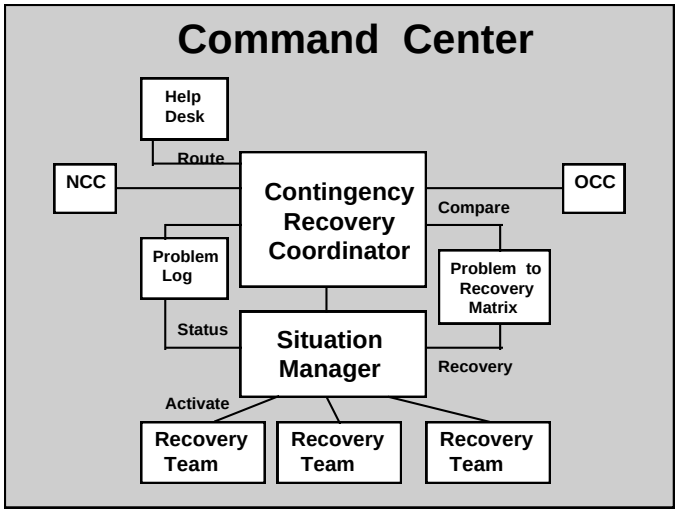


Contingency Recovery Operations

Contingency Recovery Coordinator

Responds to problems classified as "Potential Crisis Situations" by:

- **Logging the problem within the Problem Log;**
- **Comparing the problem to the Recovery Matrix;**
- **Selecting the appropriate Recovery Plan;**
- **Activating the Recovery Team identified within the Recovery Plan; and,**
- **Monitoring recovery operations and reporting on their status to Management.**



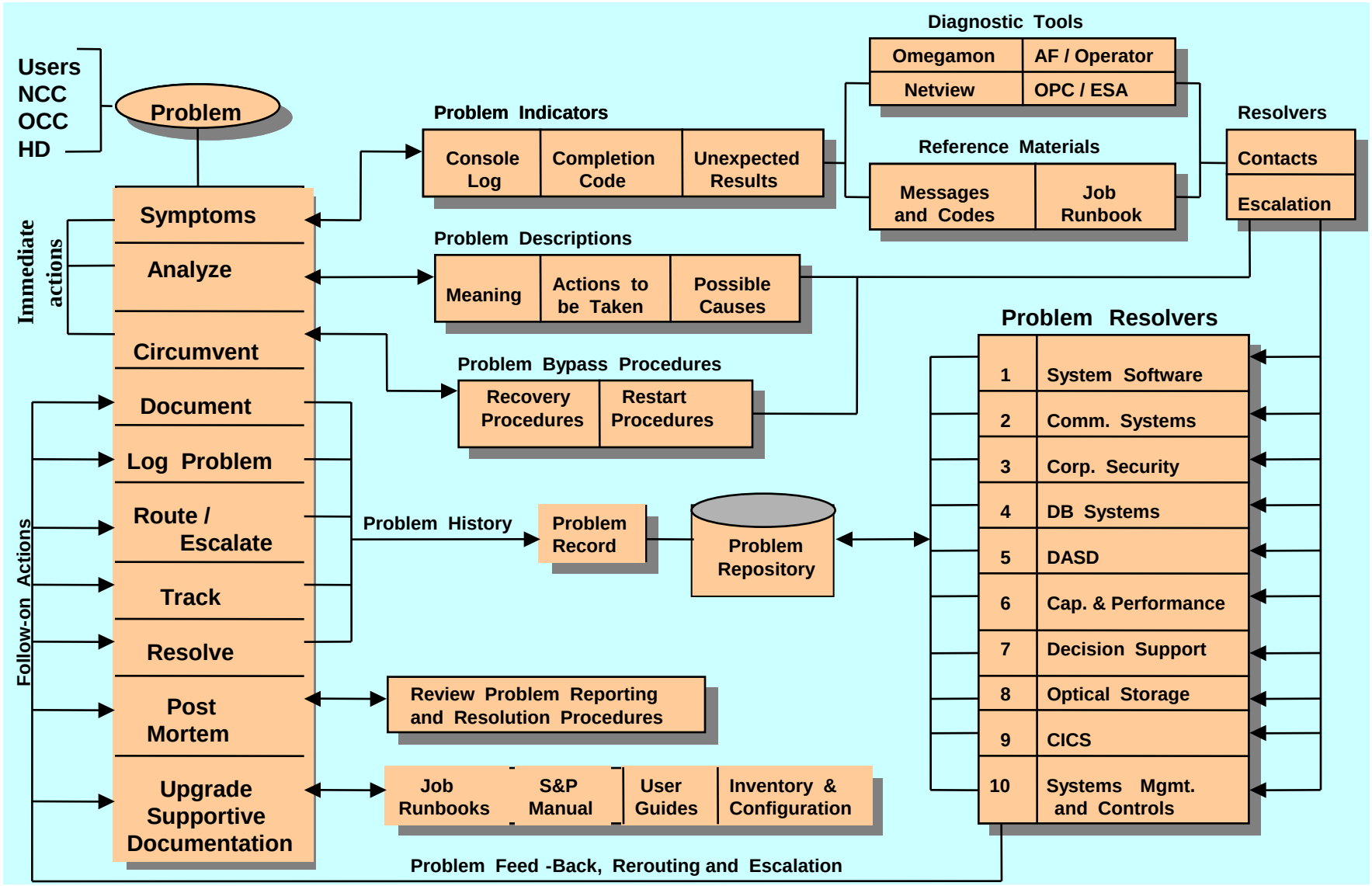
Situation Manager

Reporting to the Contingency Recovery Coordinator and responsible for monitoring Recovery Team operations and providing assistance through any mechanism at their disposal. When situations become overly complex and a potential crisis can occur, the Situation Manager will take appropriate escalation procedures needed to concentrate more resources on the resolution of the problem.

Recovery Teams

Designed to pull expertise together so that specific talents can address problems that require recovery operations, before normal processing can be resumed. Each Recovery Team consists of a Team Manager and Team Members. The organization of a Recovery Team is supplied to the Situation Manager and Contingency Recovery Coordinator. This organizational description includes functional responsibilities and alternate personnel for each of the recovery positions. Recovery Teams may require recovery tools to be utilized as an aid in performing recovery operations.

Problem Management Overview



DCAG Business Recovery Services

- **Risk Assessment** to identify Continuity of Business (COB) exposures and gaps relating to newly adopted COB requirements.
- **Business Impact Analysis** requirements definition and risk analysis studies**,**
- **Data Sensitivity** studies and evaluations**,**
- **EDP Security (Physical and Data)** studies and evaluations**,**
- **Vital Records (Vaulting Services)** and/or **Library Management,**
- **Business Recovery Documentation** evaluation and needs definition**,**
- **Business Recovery Plan (Development, and/or Implementation),**
- **Disaster Recovery Vendor(s) (Evaluations through Selection),**
- **Business Recovery Training,**
- **Permanent Personnel Recruitment and Placement Services,**
- **Consulting and Temporary Personnel Services.**