

Composite presentation of

Disaster Recovery, Business Continuity Planning,

IT Security and Compliance

Services provided by Tom Bronack

Thomas Bronack
Phone: (718) 591-5553
Cell: (917) 673-6992
Email: bronackt@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.
 - Sarbanes-Oxley, Gramm-Leach-Bliley,
 - HIPAA, The Patriot Act, etc.

“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.”

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.

	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)	
Existing Laws and their Consequences				
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: <ul style="list-style-type: none"> • Responsible Employee Selection, • Risk Assessment, • Information Safeguards and Controls, • Oversight of "Service Providers", • Testing and Monitoring. 	Security Safeguards: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • (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

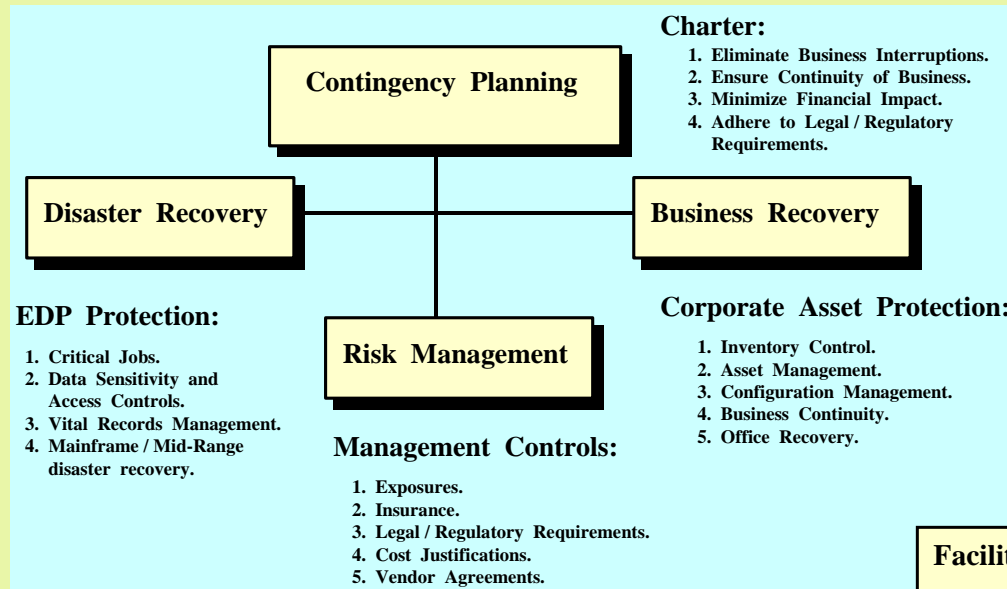
Problem definition and escalation procedures.

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.

Contingency Planning

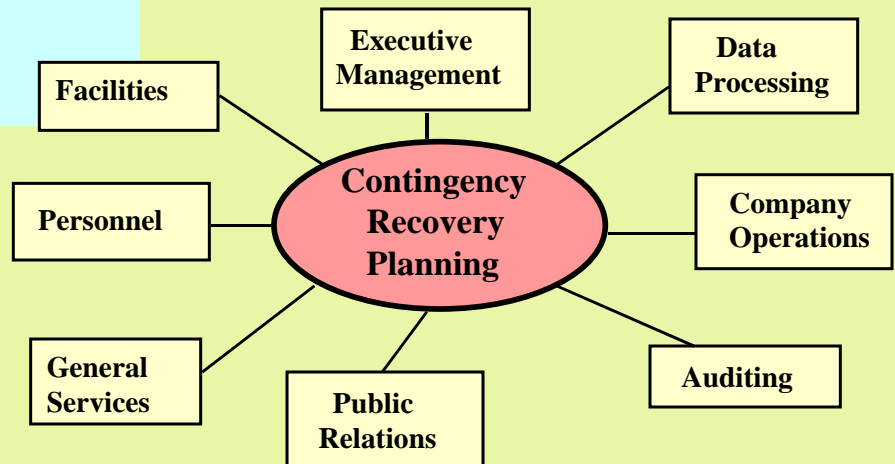
Contingency Recovery Disciplines



“These four Contingency Planning Disciplines allow for logical work separation and better controls.”

“Establishing interfaces with key departments will Allow for the inclusion of corporate-wide recovery Procedures (Security, Salvage, and Restoration, etc.) In department specific Recovery Plans.”

Contingency Recovery Interfaces



“Contingency Planning affects every part of the organization and is separated into logical work areas along lines of responsibility.”

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.**
 - Compliance, Industry, and Business Regulatory Requirements.
- **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.**

COSO Risk Assessment



Committee Of Sponsoring Organizations (COSO) was formed to develop **Risk Management and Mitigation Guidelines** throughout the industry.

Designed to **protect Stakeholders** from uncertainty and associated risk that could erode value.

A **Risk Assessment** in accordance with the COSO Enterprise Risk Management Framework, consists of (see www.erm.coso.org for details):

- **Internal Environment Review,**
- **Objective Setting,**
- **Event Identification,**
- **Risk Assessment,**
- **Risk Response,**
- **Control Activities,**
- **Information and Communication,**
- **Monitoring and Reporting.**

Creation of **Organizational Structure**, Personnel Job Descriptions and Functional Responsibilities, Workflows, Personnel Evaluation and Career Path Definition, Human Resource Management.

Implementation of **Standards and Procedures** guidelines associated with Risk Assessment to guaranty compliance to laws and regulations.

Employee awareness training, support, and maintenance going forward.

Performing a Risk Assessment or Needs Analysis

I. PERFORMING A RISK ASSESSMENT:

A. Define Laws and Regulatory Requirements.

1. Gramm-Leach-Bliley,
2. Sarbanes-Oxley,
3. HIPAA,
4. Patriot Act,
5. EPA and Superfund,
6. Industry Specific Regulators.

B. General Recovery Parameters:

1. Data Sources and their Protection,
2. Business Continuity Planning,
3. Library / Vital Records Management,
4. Disaster Recovery Planning,
5. Documentation, Training, and Support.

C. Define Business / Disaster Recovery Needs:

1. Define Business Continuity Needs,
2. Implement IT & Physical Security,
3. Implement Vital Records and Library Management,

4. Develop Disaster Recovery Planning,
5. Implement Recovery Operations,
6. Support and Maintain Recovery Plans,
7. Insure Protection of Business Assets,
8. Assure Regulatory Compliance,
9. Assure Insurance requirements are met.
10. Assure Vendor Contracts and Reciprocal
11. Agreements are in place and maintained.

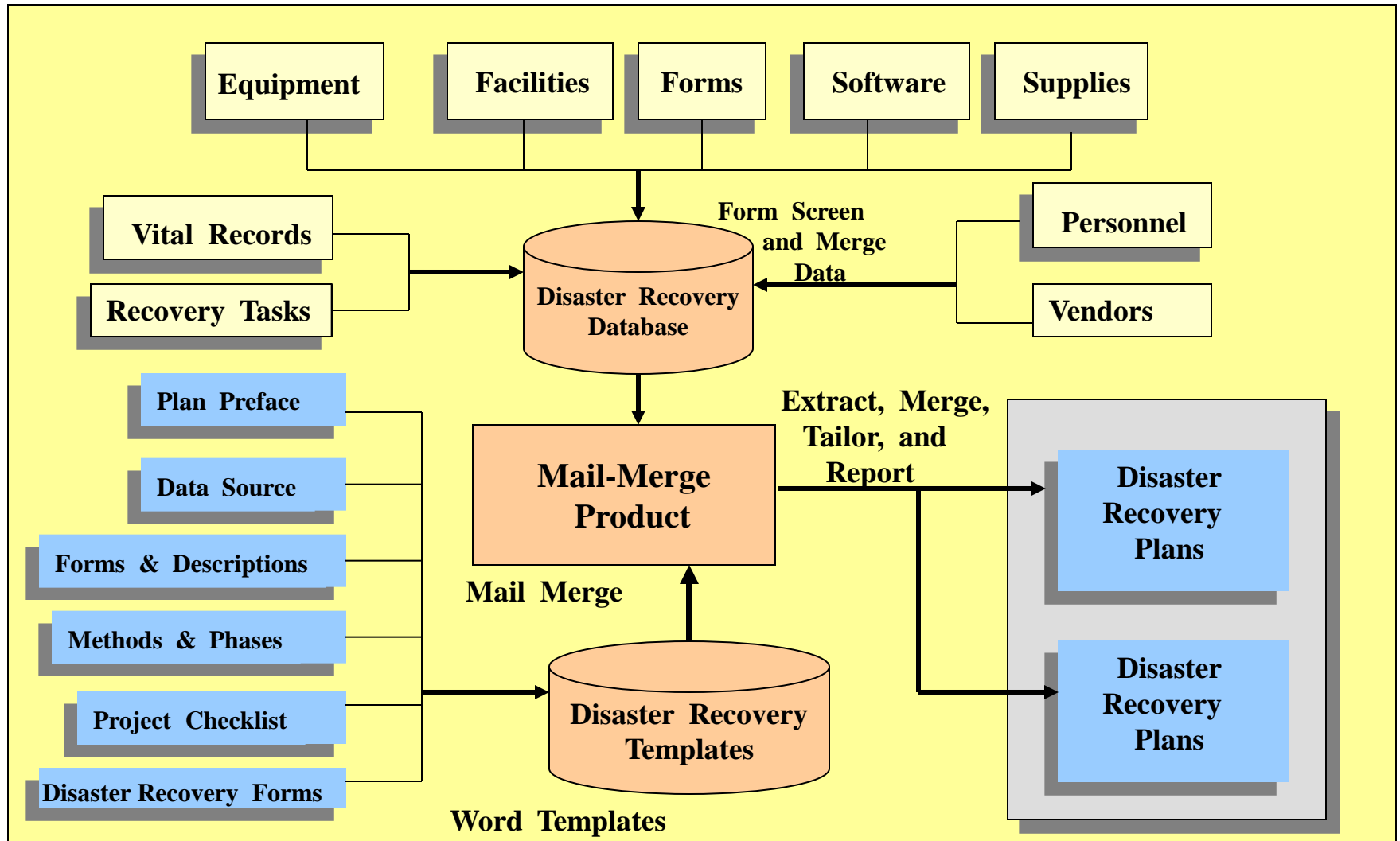
D. Develop Recovery Plan(s), as per existing Standards and Procedures.

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

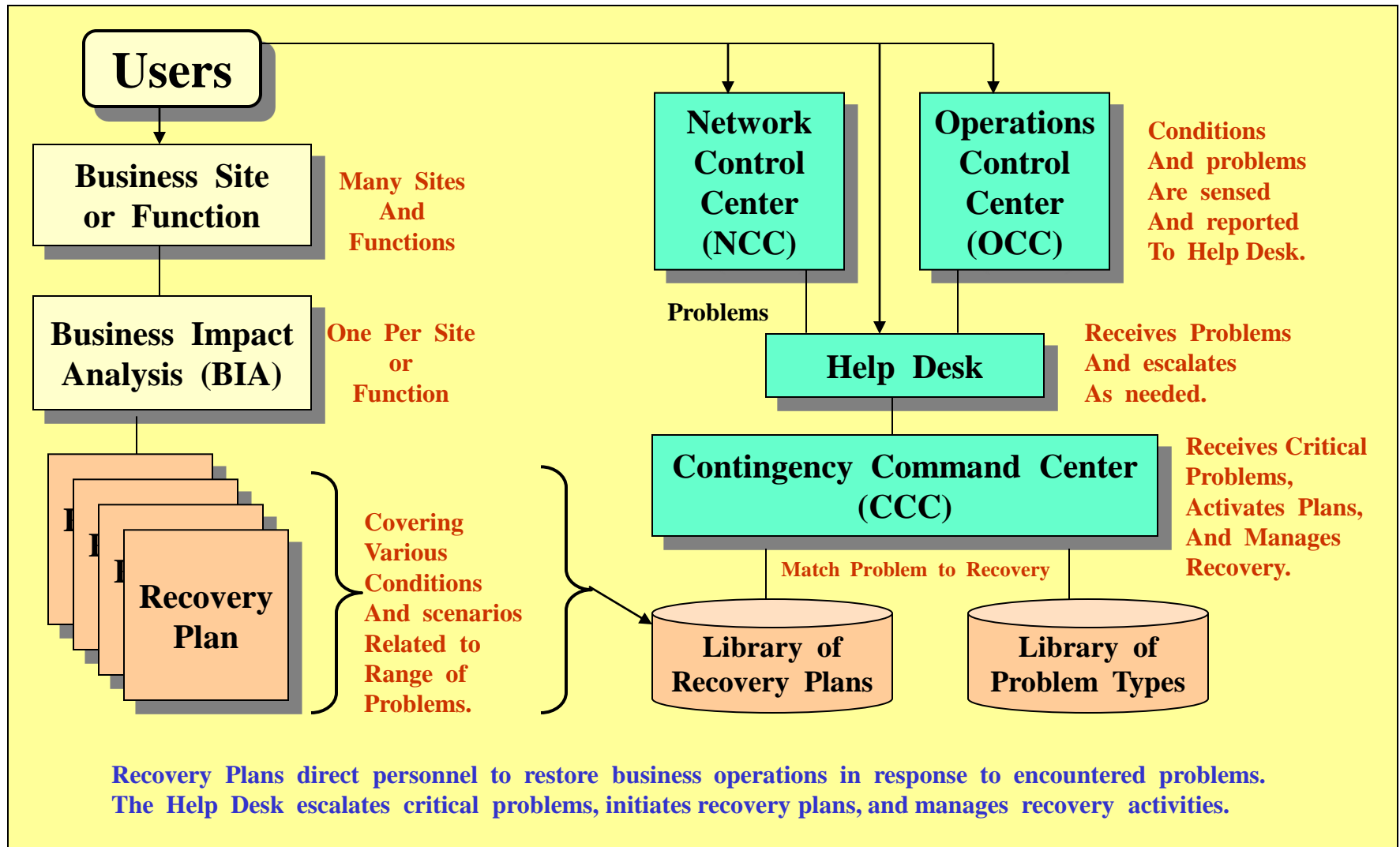
F. Review Recovery Plan Support and Maintenance Standards and Procedures.

G. Review Problem and Crisis Management Standards and Procedures.

Disaster Recovery Plan Data Sources and Output Generation



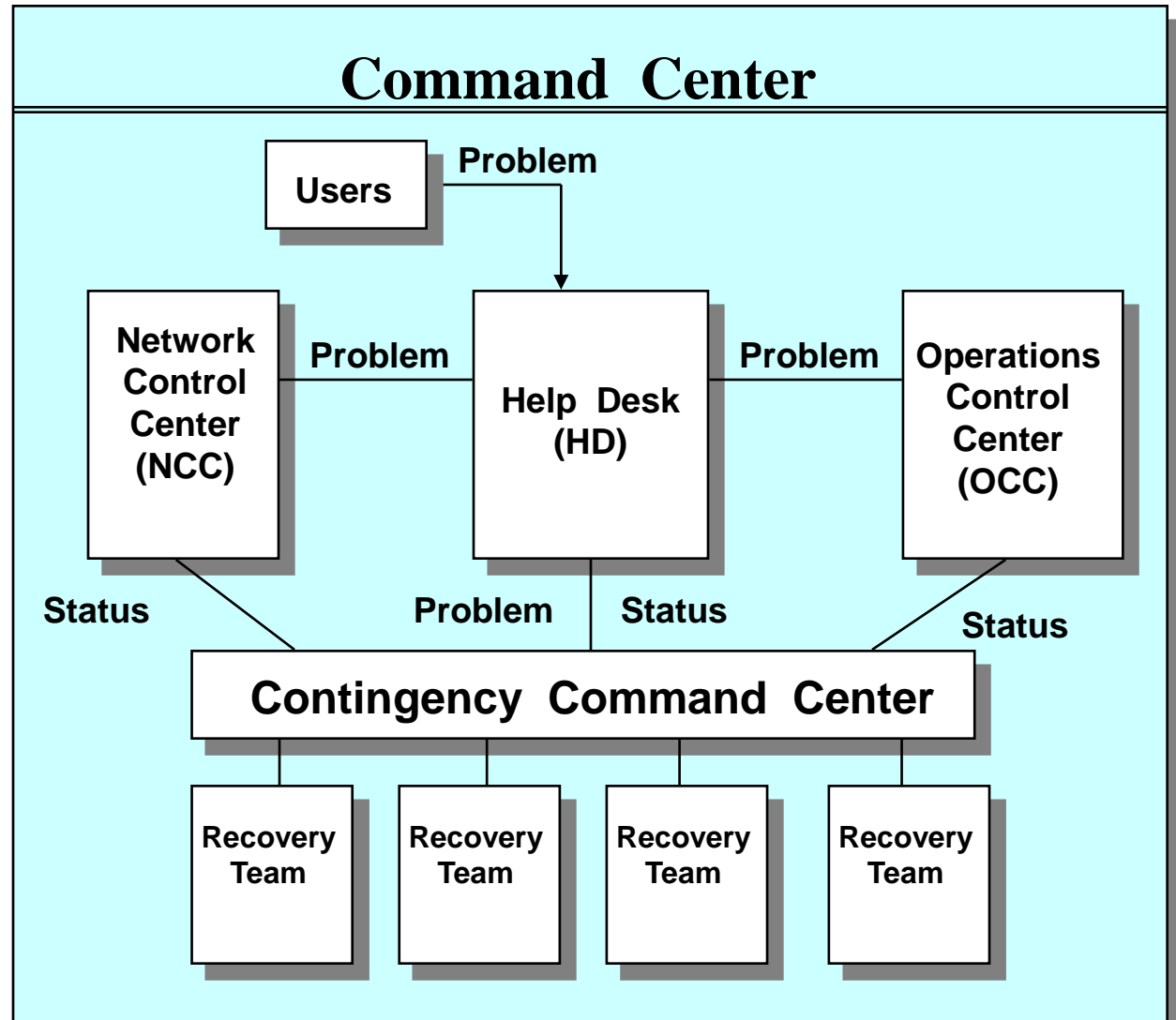
Overview of Business Continuity Planning and BIA's



Contingency Command Center

Contingency Command Center:

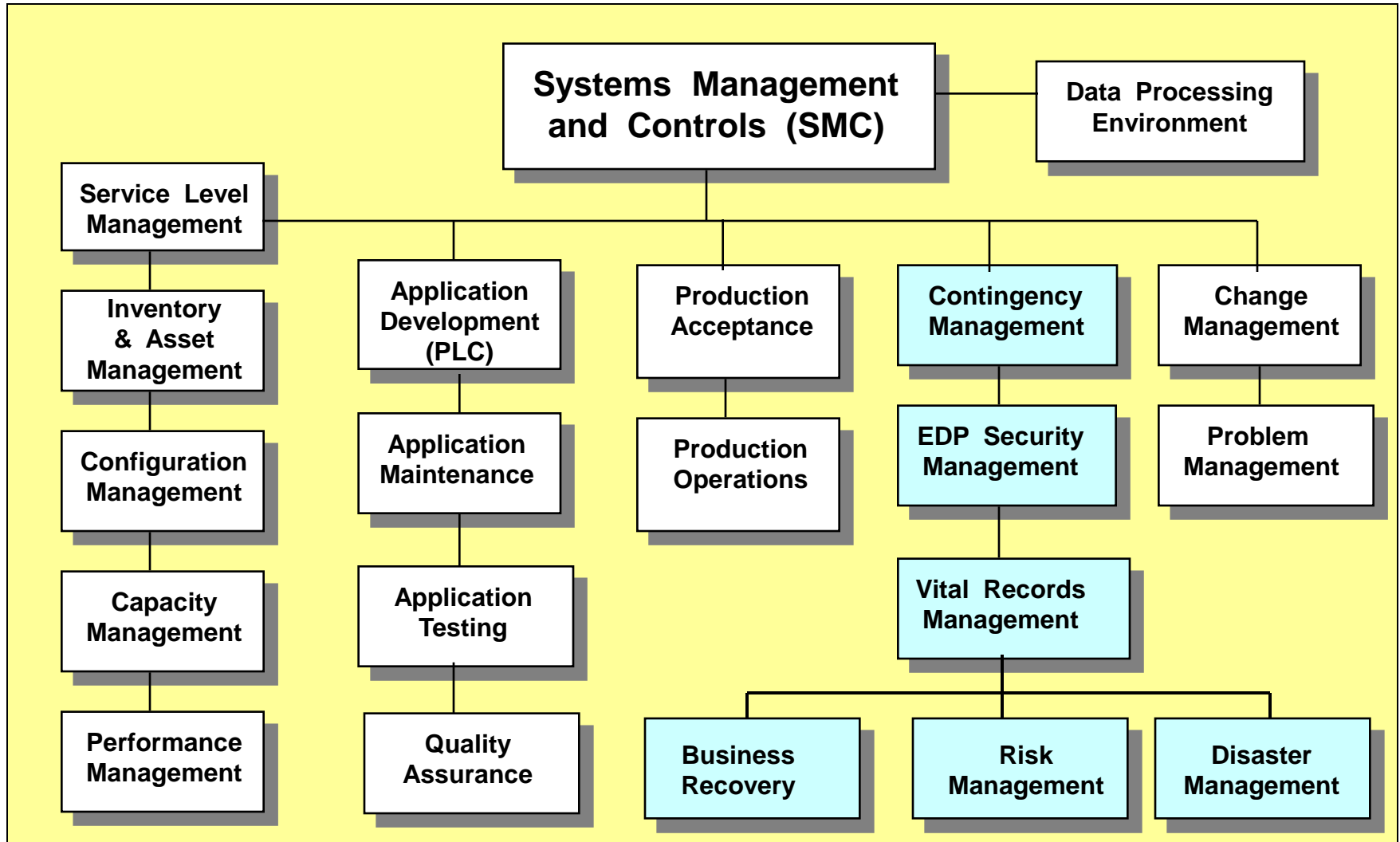
- Housed within Command Center,
- Activated during Emergencies,
- Relates problems to Recovery Plan,
- Activates appropriate Recovery Team(s),
- Coordinates Recovery Actions,
- Maintains status on disaster and crisis situations,
- Communicates with;
 - Network Control Center,
 - Operations Control Center,
 - Help Desk,
 - Technical Staff, and
 - Management.
- Will escalate recovery actions, if necessary.



Strategies for Eliminating Audit Exceptions

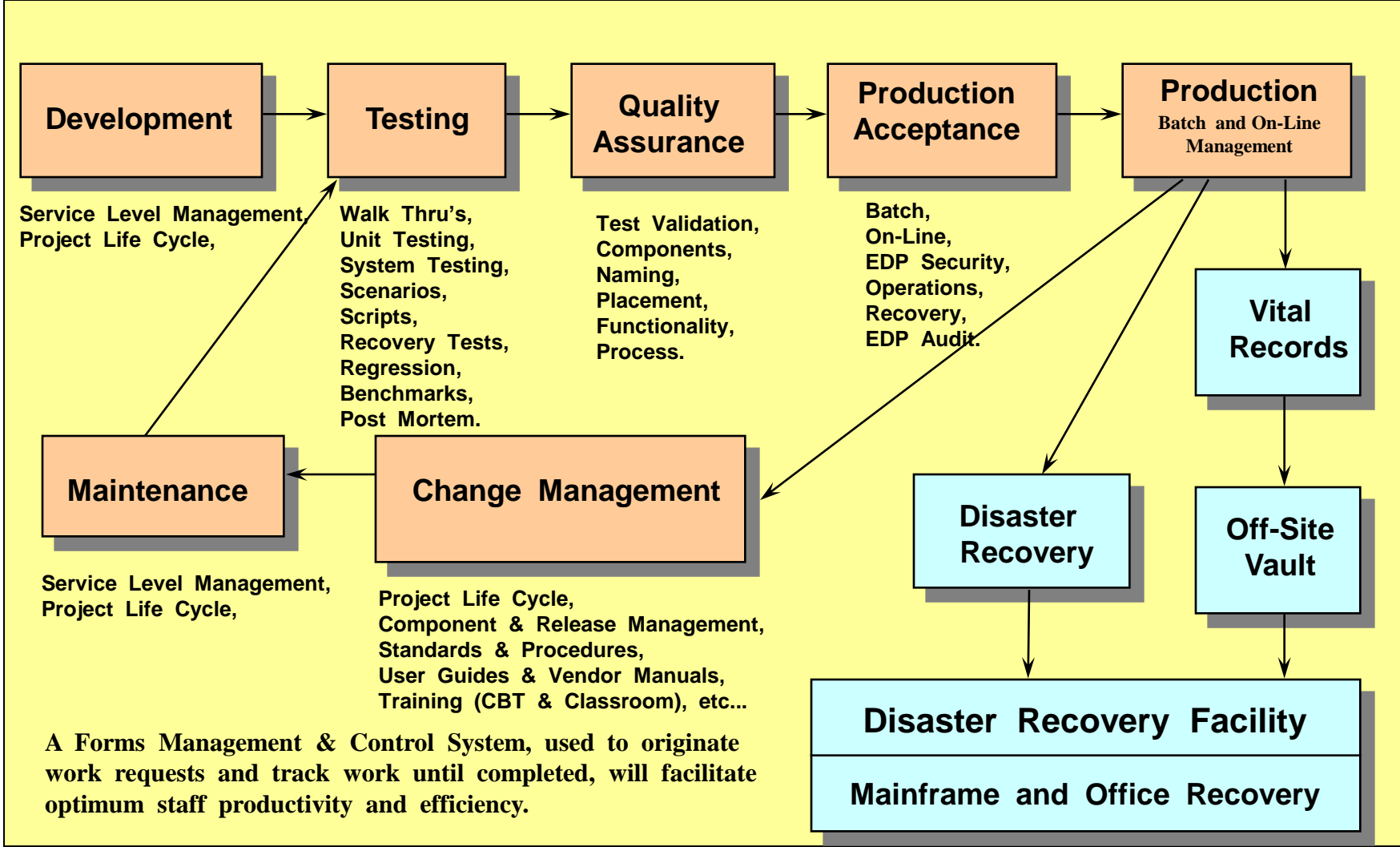
- **Review of Compliance Requirements (Business and Industry)**
- **Data Sensitivity, EDP Security and Vital Records Management,**
- **Production Acceptance, Quality Control and Project Life Cycle,**
- **Utilizing Automated Tools,**
- **Elimination of Single-Point-Of-Failure concerns,**
- **Inventory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

Systems Management Organization



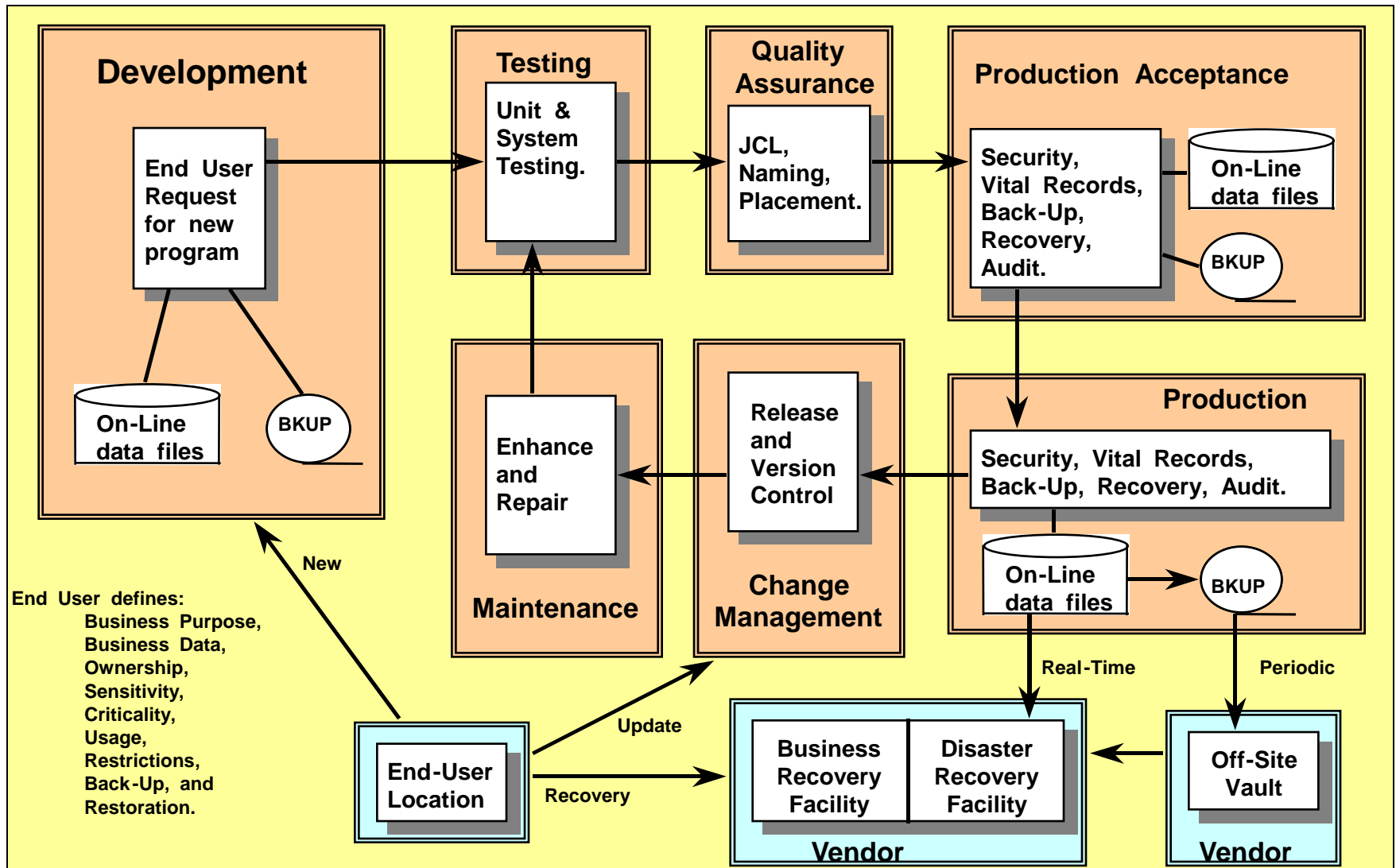
Systems Management Controls and Workflow

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



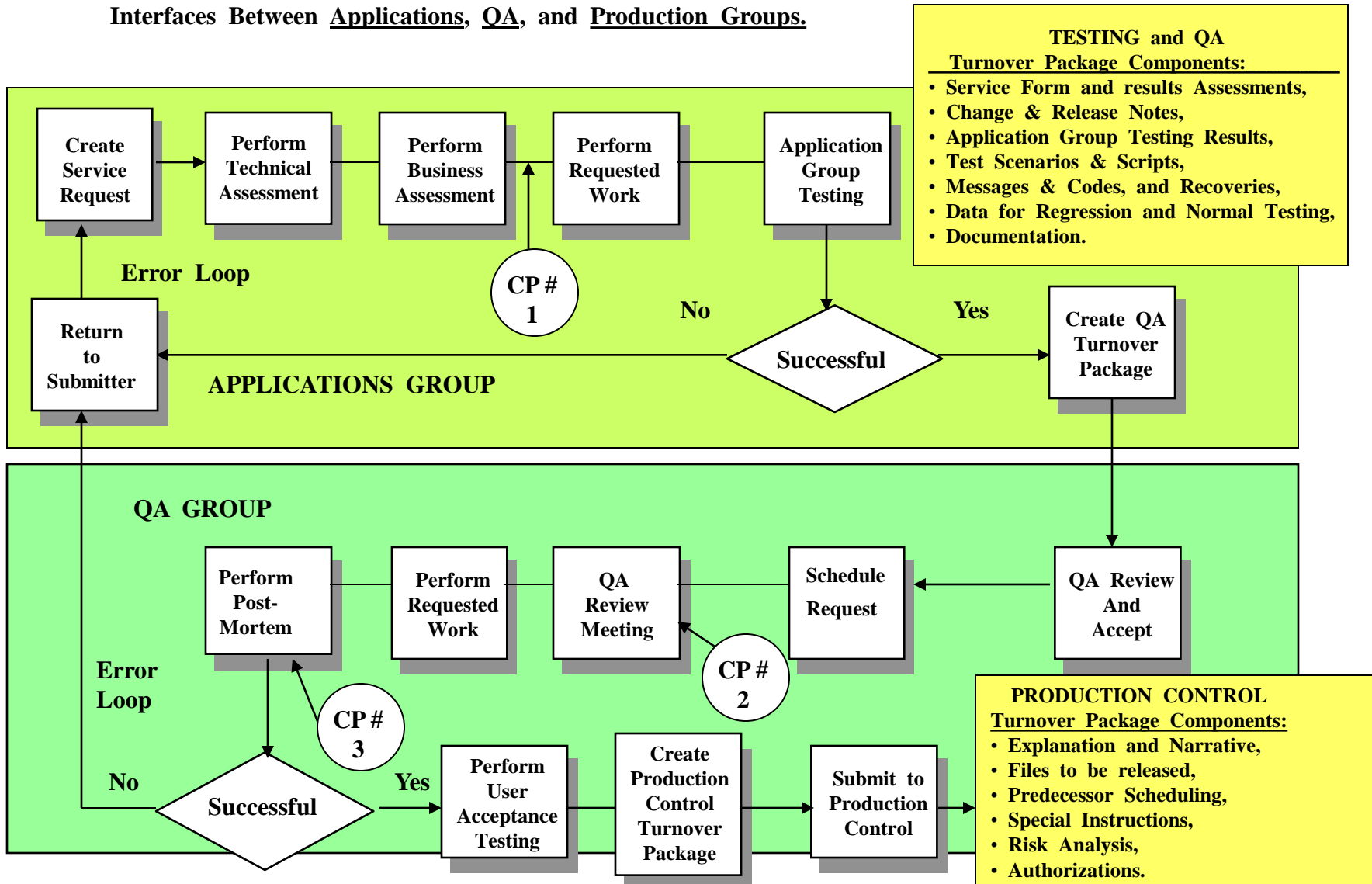
Application Life Cycles and Business Recovery Planning

(Development through Change Management and Maintenance)

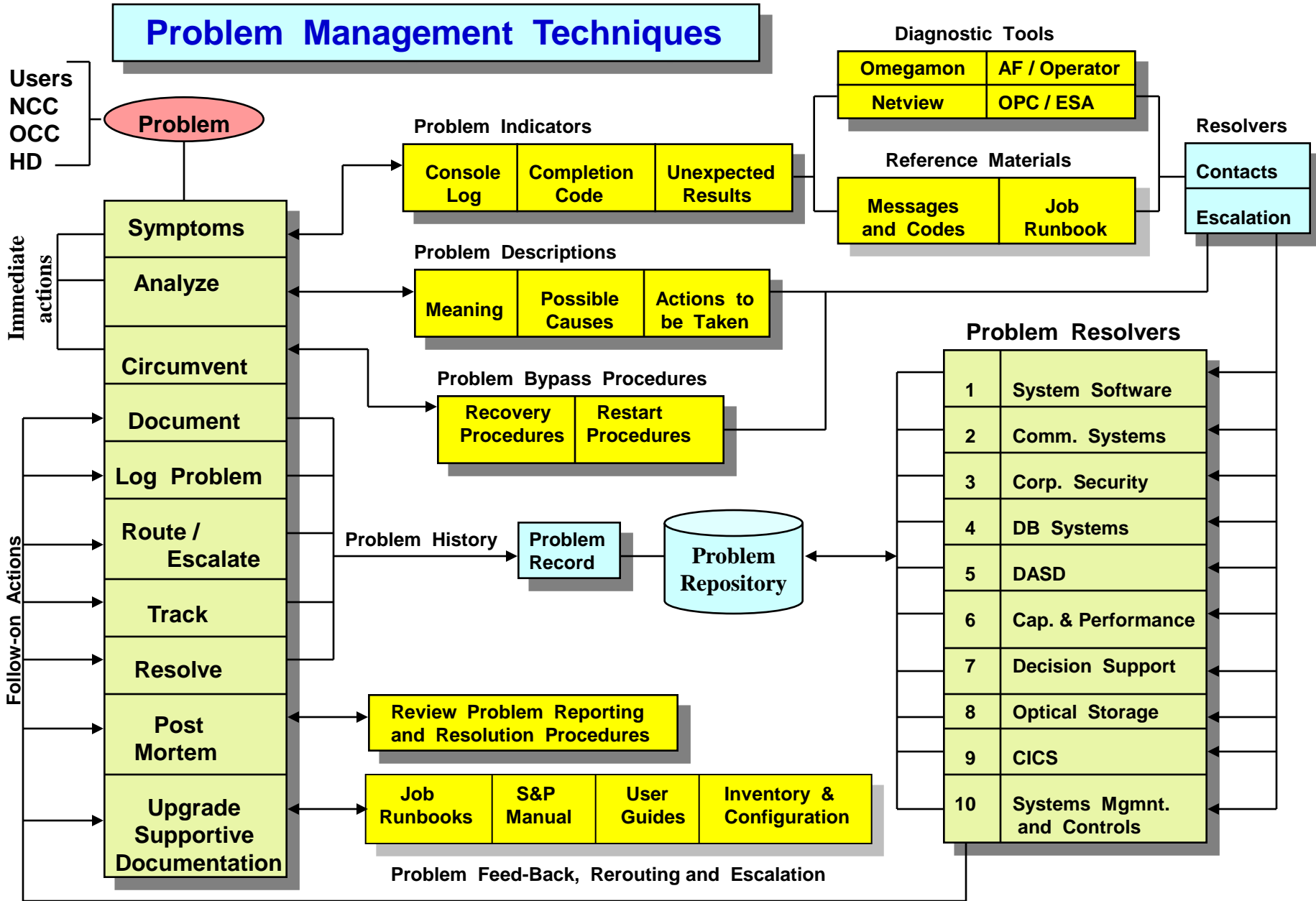


Quality Assurance and PLC Checkpoints

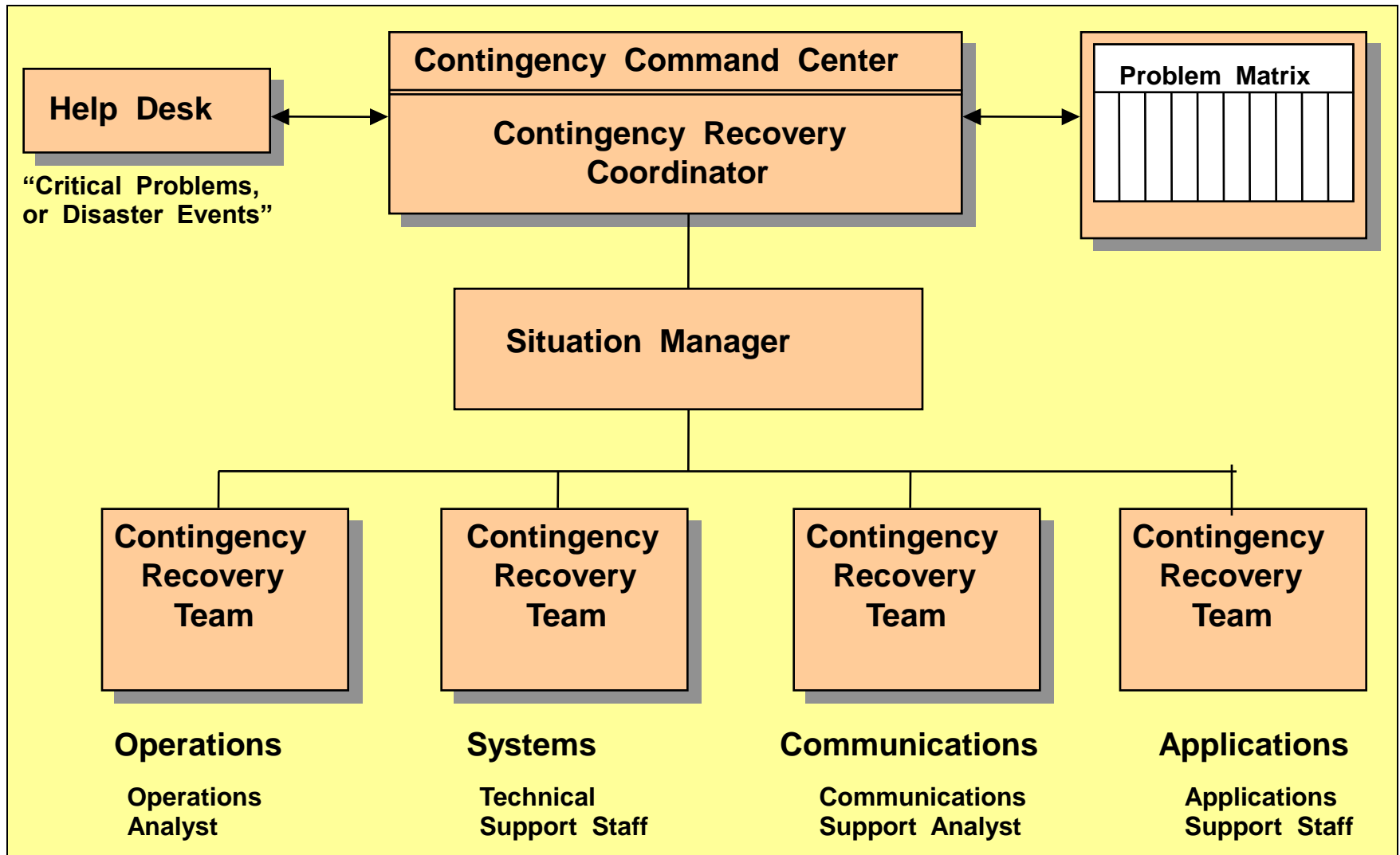
Interfaces Between Applications, QA, and Production Groups.



Problem Management Techniques



Contingency Organization in Action



Contingency Recovery Operations

Contingency Recovery Coordinator

Responds to problems classified as “Potential Crisis Situations” by:

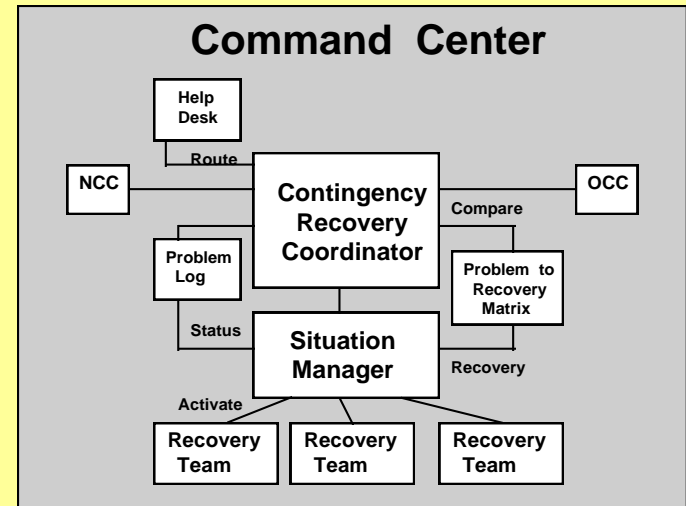
- Logging the problem within the Problem Log;
- Comparing the problem to the Recovery Matrix;
- Selecting the appropriate Recovery Plan;
- Activating the Recovery Team identified within the Recovery Plan; and,
- Monitoring recovery operations and reporting on their status to Management.

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.



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.**

Overview of our Services

(Part 1 of 3)



We provide Consulting and Personnel Placement Services, along with providing Compliance Services to assist clients adhere to the regulatory requirements of the laws listed below. These services make our firm unique.

Services

Consulting

Compliance

Placement

Project Management

Risk Assessments

Security (Physical / IT)

Business Continuity

Productivity Optimization

- Project Definition & Scope
- Goals and Objectives
- Team identification
- Team Assignment
- Team Training
- Project Plan Creation
- Project Management & Status Reporting
- Analysis Phase
- Conclusions
- Recommendations
- Management Report
- Management Presentation

- COSO Format, including:
 - Internal Environment,
 - Objective Setting,
 - Event Identification,
 - Risk Assessment,
 - Risk Responses,
 - Control Activities,
 - Information and Communications
 - Monitoring and Reporting.
- Management Report
- Management Presentation

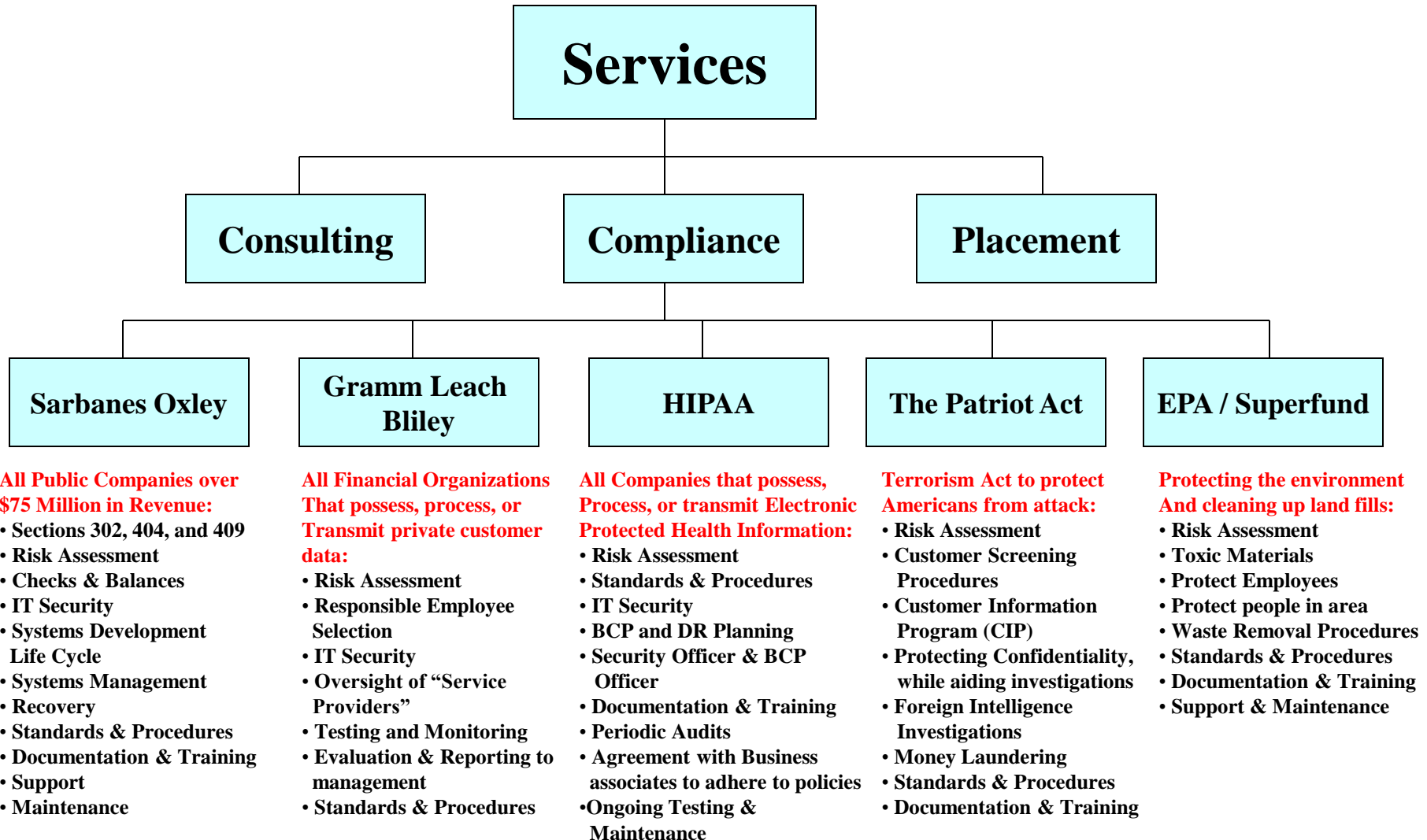
- Physical Security, including:
 - Perimeter,
 - Access Controls,
 - Surveillance & Reporting,
 - Fire Safety Protection.
- IT Security, including:
 - Data Sensitivity,
 - Access Controls,
 - Vital Records,
 - Backup & Restoration.
 - Data Management Tools.

- Disaster Recovery,
- Emergency Management,
- Business Impact Analysis,
- Contingency Command Center,
- Documentation,
- Team Selection,
- Team Training,
- Support,
- Maintenance.

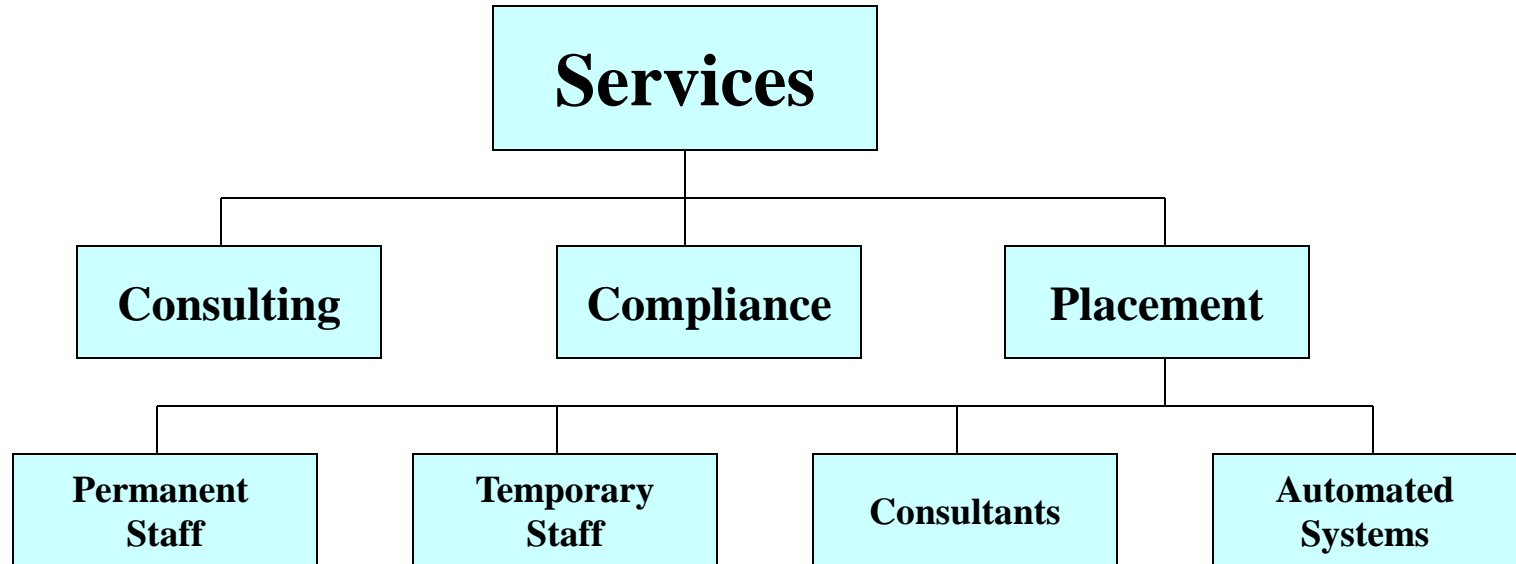
- Organizational Structure,
- Systems Management,
- Job Descriptions,
- Functional Responsibilities,
- Forms Management,
- SLA / SLR,
- Standards & Procedures,
- Personnel Training.

Overview of our Compliance Services

(Part 2 of 3)



Overview of our Services (Part 3 of 3)



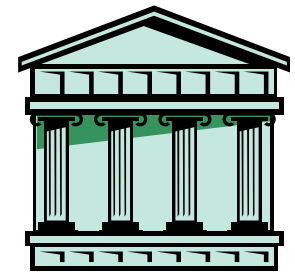
- Personnel Productivity,
- Automated Personnel,
- Workflow Management,
- Automated Training.

Sarbanes-Oxley Act



- Requires companies to perform quarterly **self-assessments** of risks to business processes that affect **financial reporting** and to attest to findings on an annual basis (CFO and CEO, possibly CIO too). Section 302 requires “**Signing Officer**” to design reports for compliance submission.
- Section 404 requires that technology personnel develop and implement means for **protecting critical financial data** (data security, back-up and recovery, business continuity planning, and disaster recovery), because loss of data is not acceptable.
- Section 409 will require “**Real-Time Reporting**” of financial data, thus creating the need for new Standards and Procedures and perhaps re-engineering of functions to better comply with the Law.
- Companies must devise “**Checks and Balances**” to guaranty that those people creating functions (like programmers) are not the person responsible for validating the functions operation (rather a separate checker must validate function).
- Checks and Balances prohibit big 4 accounting firms from performing Risk Assessment because they are the ones performing audit (**Conflict of Interest**).
- **Penalties** can include fines as high as \$5 million and imprisonment can be for as long as 20 years for deliberate violation.

Gramm-Leach-Bliley



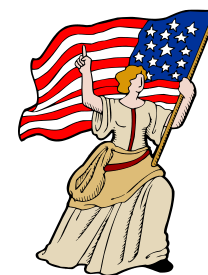
- Covers **Financial Organizations** (as defined in the Bank Holding Act) that possess, process, or transmit private customer information.
- Its purpose is to **protect Customer Information** from unauthorized disclosure or use.
- An **Information Security Program** must be in place to comply and the following operating mechanisms must be established:
 - Responsible employee as **Security Officer**.
 - **Risk Assessment** to uncover and correct exposures.
 - **Information Safeguards and Controls** must be established.
 - Oversight of “**Service Providers and Vendors**” to guaranty compliance.
 - **Testing and Monitoring** in an on-going fashion.
 - **Evaluation and Reporting** to management.
- **Compliance** date of May, 2003. Law provides for fines and imprisonment of up to 5 years for intentional violations.

HIPAA



- **Covers** organizations that possess, transmit, or process electronic protected health information (EPHI).
- Responsible for **protecting EPHI data** from unauthorized disclosure or use.
- **Required Security Safeguards include:**
 - **Risk Assessment** to uncover and resolve exposures.
 - **Policies and Procedures** to control access and track usage.
 - **Physical and IT Security Measures.**
 - **Contingency Plan and Disaster Recovery Plan.**
 - **Appointment of Security Officer and Business Continuity Officer.**
 - **Training** and communications to improve awareness.
 - **Periodic Audits** and maintenance of Audit Trail.
 - **Agreement with “Business Associates”** to comply to requirements.
 - **On-going Testing** and Evaluation of plan and deliverables.
- **Comply** by April 2005, with fines to \$250,000 and imprisonment for up to 10 years.

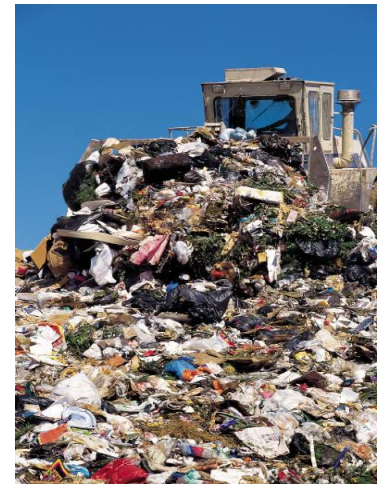
Patriots Act



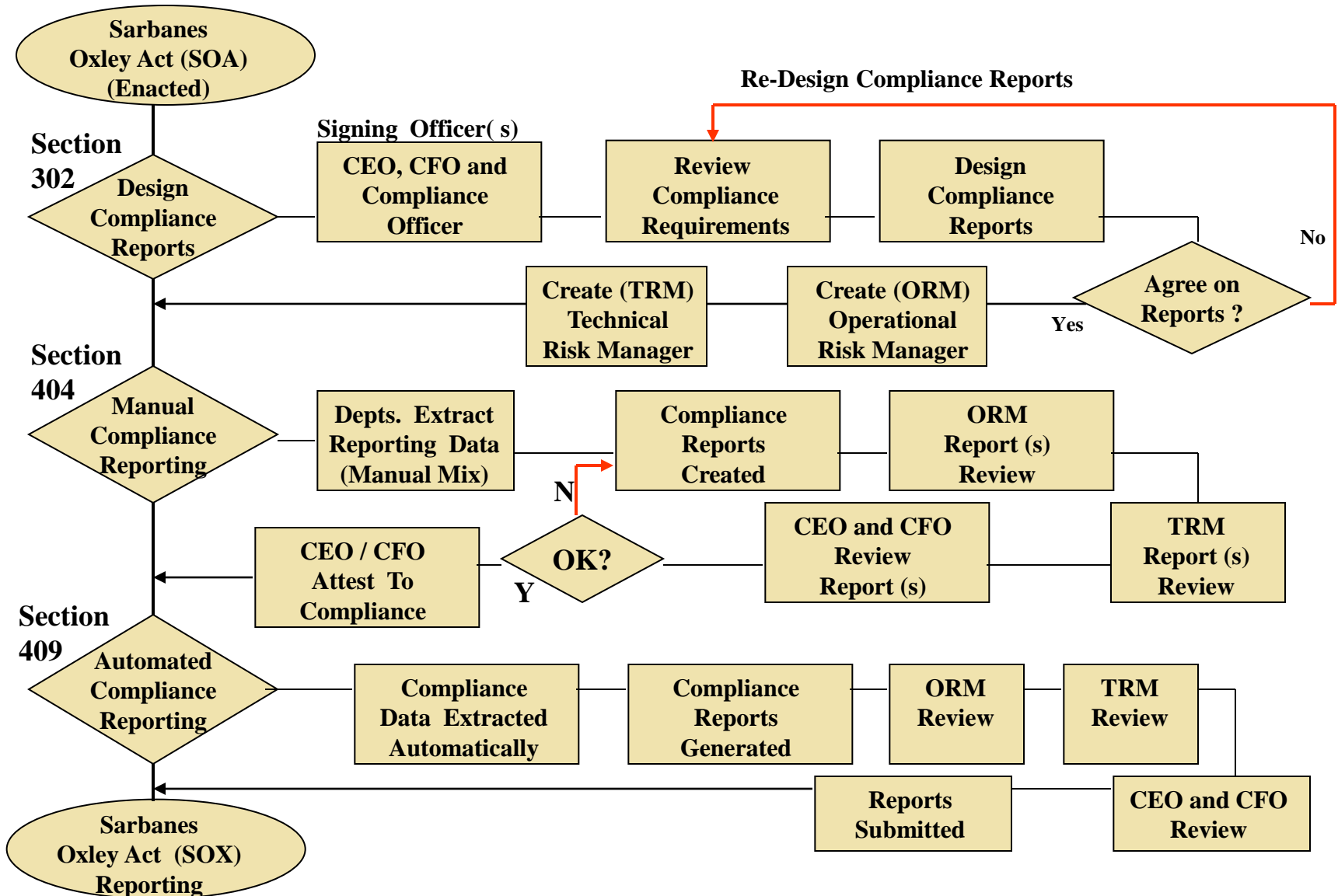
- **New Requirements — Severe Penalties** (Official Title is “**Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism”**).
- **USA PATRIOT Act Section 326** imposes new requirements on how organizations screen existing customers and process new customer information.
- **By October 1, 2003**, all financial services organizations must have in place procedures for:
 - **1. Customer Screening** — On a regular basis, customers and transactions must be matched against government-provided lists of suspected terrorists, drug traffickers, money launderers and other criminals.
 - **2. Customer Information Program (CIP)** — On all new customers, basic identification information must be obtained to verify the customer's identity. Failure to comply can result in penalties of up to \$1 million, and/or imprisonment.
- Used to **protect the confidentiality** of telephone, face-to-face, and computer communications, **while enabling authorities to identify and intercept during criminal investigations** with warrant.
- Improves ability to obtain data during **Foreign Intelligence Investigations** and increases a companies need to safeguard voice, face-to-face, and computer based data.
- Enhances financial organizations ability to track suspected **Money Laundering** activities and requires reporting of activity when uncovered, thus fostering the need to obtain, store, and safeguard data used to report on suspected Money Laundering activities.

EPA and Superfund

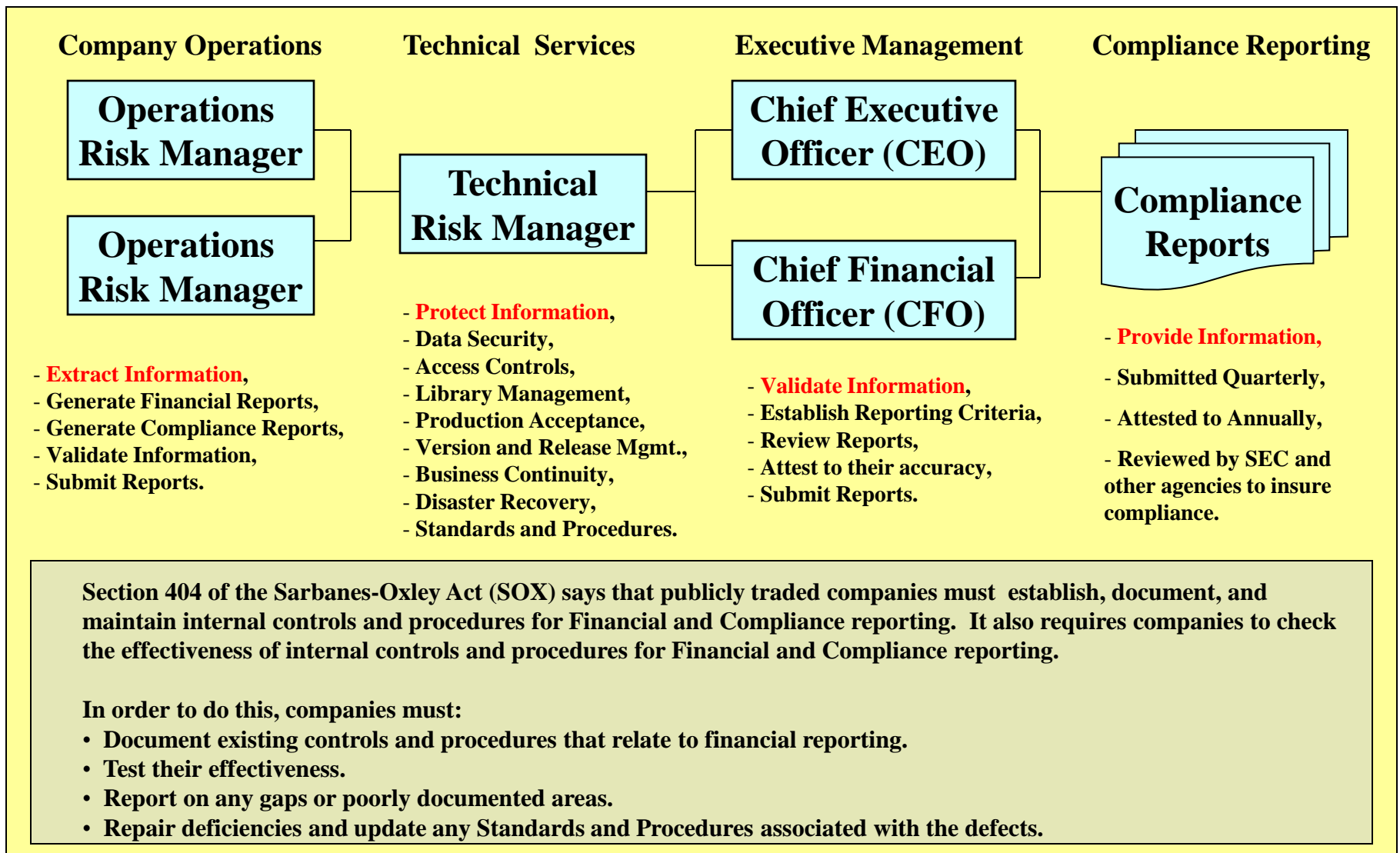
- Designed to **protect the environment** from Toxic Materials that could lead to death or illness.
- **Regulated** by the Environmental Protection Agency.
- **Fines and imprisonment** can be imposed when violation is intentional, or through a third party acting in your behalf.
- **Safeguards** should be imposed to:
 - **Identify** toxic materials,
 - Take appropriate steps to **protect** employees and community personnel,
 - Insure that proper and authorized **Waste Removal procedures** are implemented,
 - Provide personnel awareness programs and **Standards and Procedures**,
 - **Support and maintain** program going forward.



Creating Compliance Reports



How reporting is accomplished



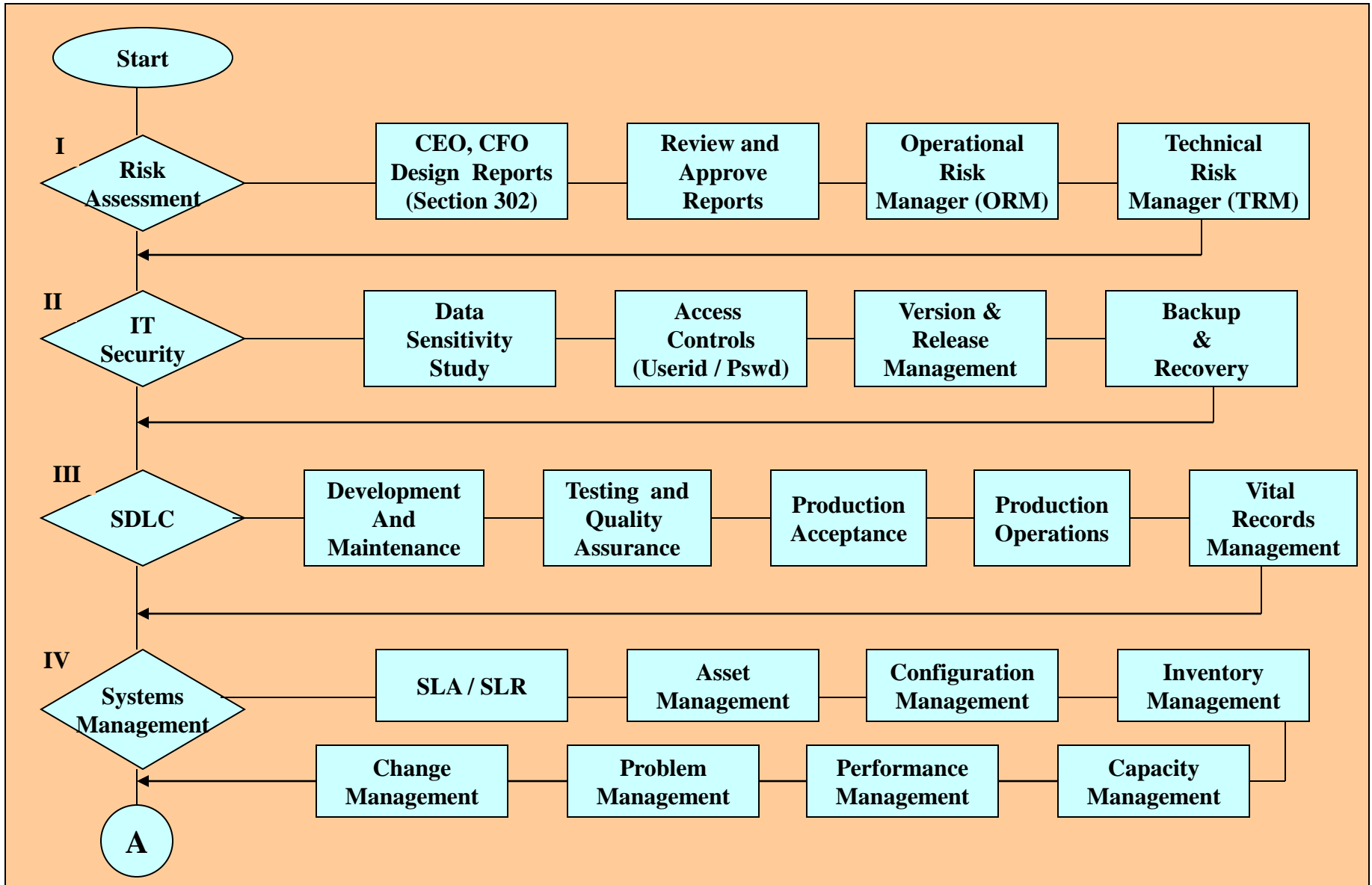
How do we comply?

Laws and Regulations concentrate on the **VALIDITY of PROVIDED DATA**, so we start with a review of how sensitive data is created, protected, and used, including:

- Identify the **lifecycle of data** used in financial reporting and compliance.
 - Where does it come from?
 - What form is it in (Excel, Database, manual, fax, email, etc.)
 - Who has access to it and how can they impact data (create, edit, use, convert, etc.)
- Review current **Data Sensitivity** and **IT Security** procedures.
- Examine **Library Management, Backup, Recovery, and Vaulting** procedures associated with sensitive data.
- Review **Business Continuity Planning** and **Disaster Recovery** procedures used to protect and safeguard critical data and facilities.
- Utilize existing **Standards and Procedures** to duplicate process and identify errors.
- Examine the available **Employee Awareness and Education** programs.

As a result of this study, it will be possible to identify weaknesses and develop procedures to overcome the weaknesses, thereby improving efficiency and productivity.

DCAG Project Phases (part 1 of 2)



DCAG Project Phases (part 2 of 2)

