Release Date: March 21, 2012

File Name: IFSA presentation

Identifying and Protecting Compliance Information Through Current Business Continuation Practices

Produced by:

Thomas Bronack
15180 20th Avenue
Whitestone, NY 11357
Email: bronackt@dcag.com

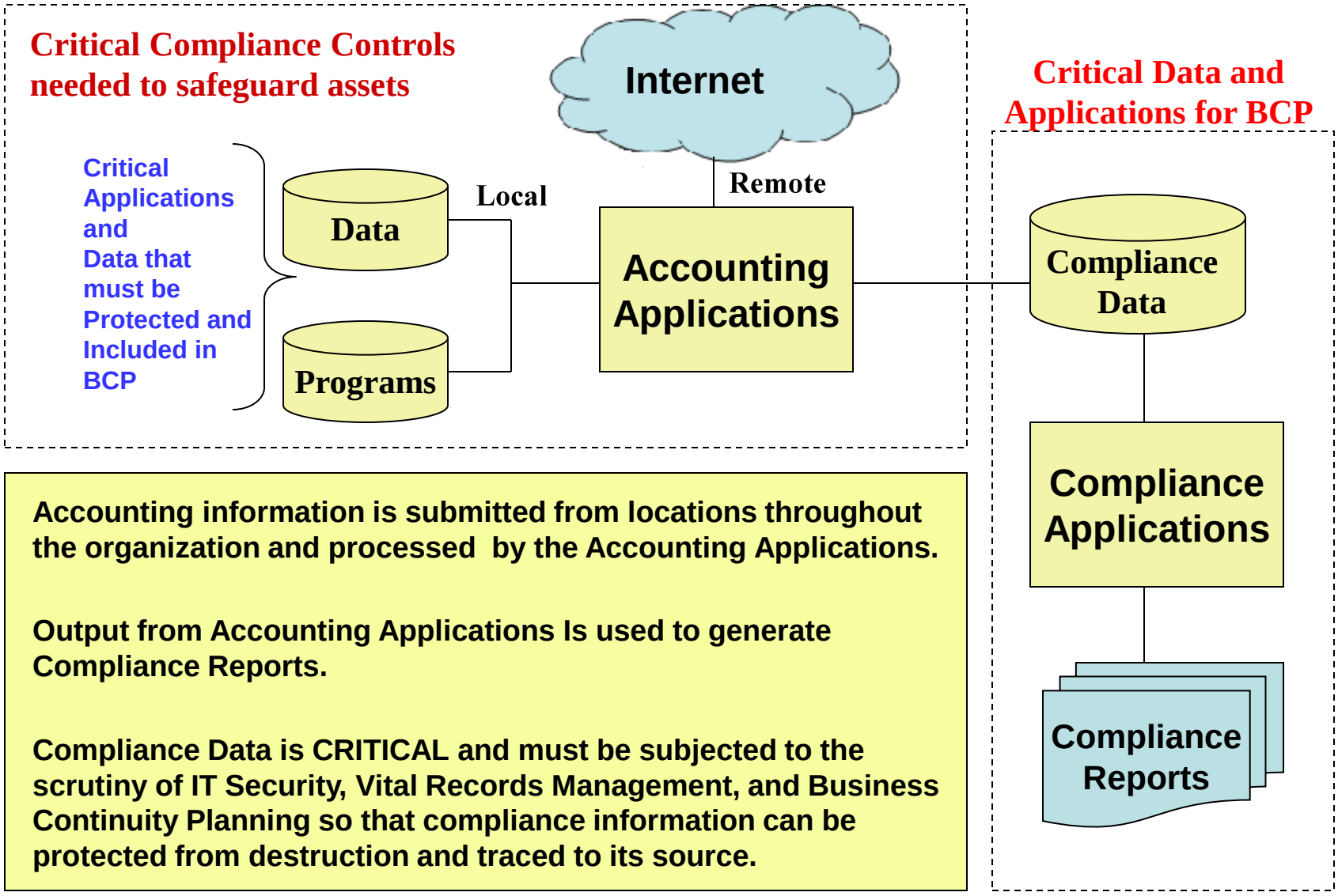
Phone: (718) 591-5553
Cell: (917) 673-6992

Overview of Presentation – A Roadmap to Protection.

Safeguarding Financial and Compliance Information:

- **Audit Applications to Identify Critical Information and any Gaps or Exceptions associated with the critical files.**
- **Utilize Technical Risk Management Services to correct Gaps and Exposures associated with protecting critical data:**
  - **IT Security (both Physical and Data);**
  - **Vital Records Management;**
  - **Version and Release Management;**
  - **Disaster Recovery and Business Continuity Planning; and**
  - **Process Improvements and Re-Engineering Work Flow.**
- **Integrate Safeguards within normal Work Flow & Operations.**
- **Update Standards and Procedures Manual for Work Flow.**
- **Provide Documentation and Training to Personnel.**
- **Prepare for the Future through Monitoring and Adjustment.**

Auditing Accounting and Compliance Applications

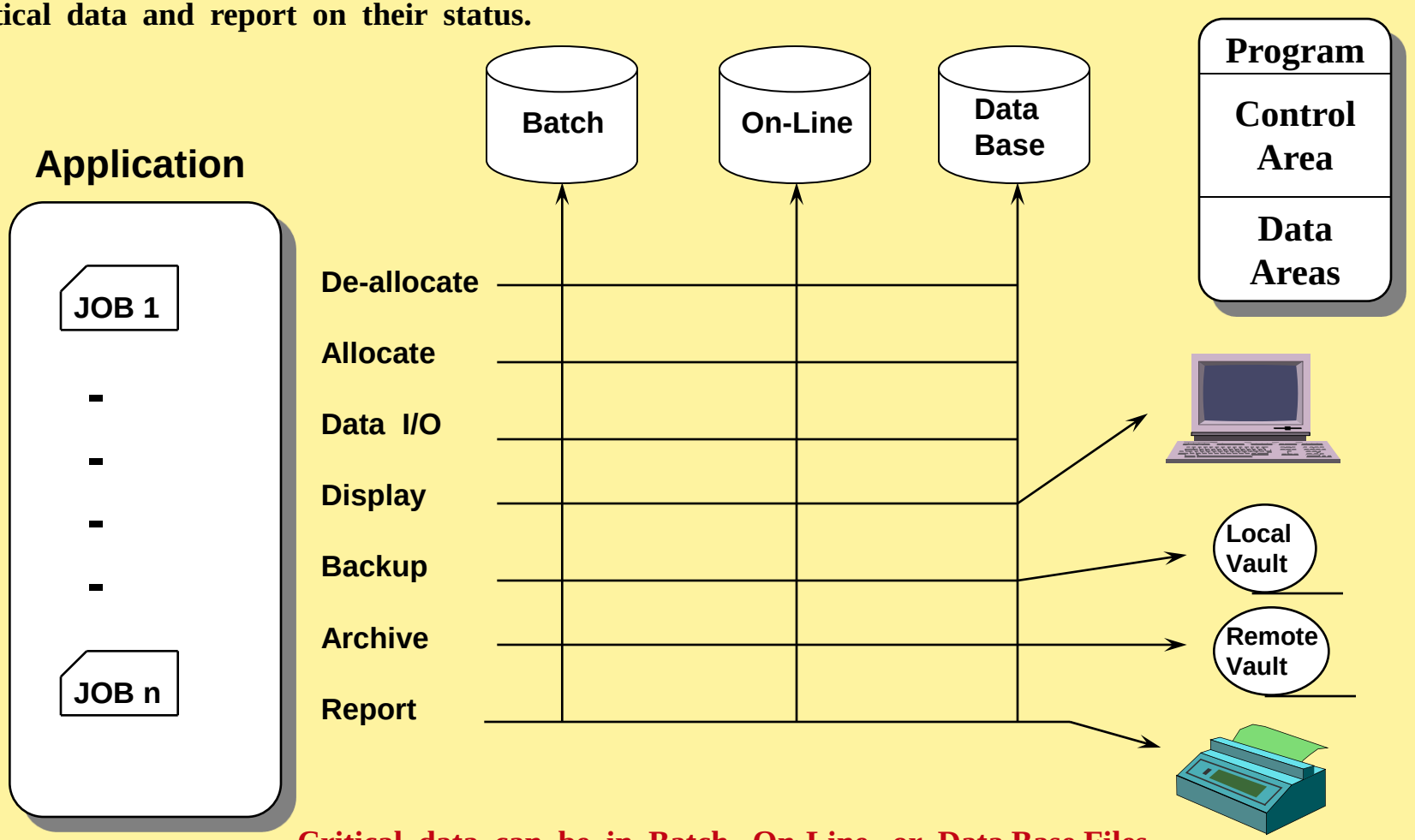


Existing Laws and their Consequences

	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 "busines 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.

Application and Program Profile

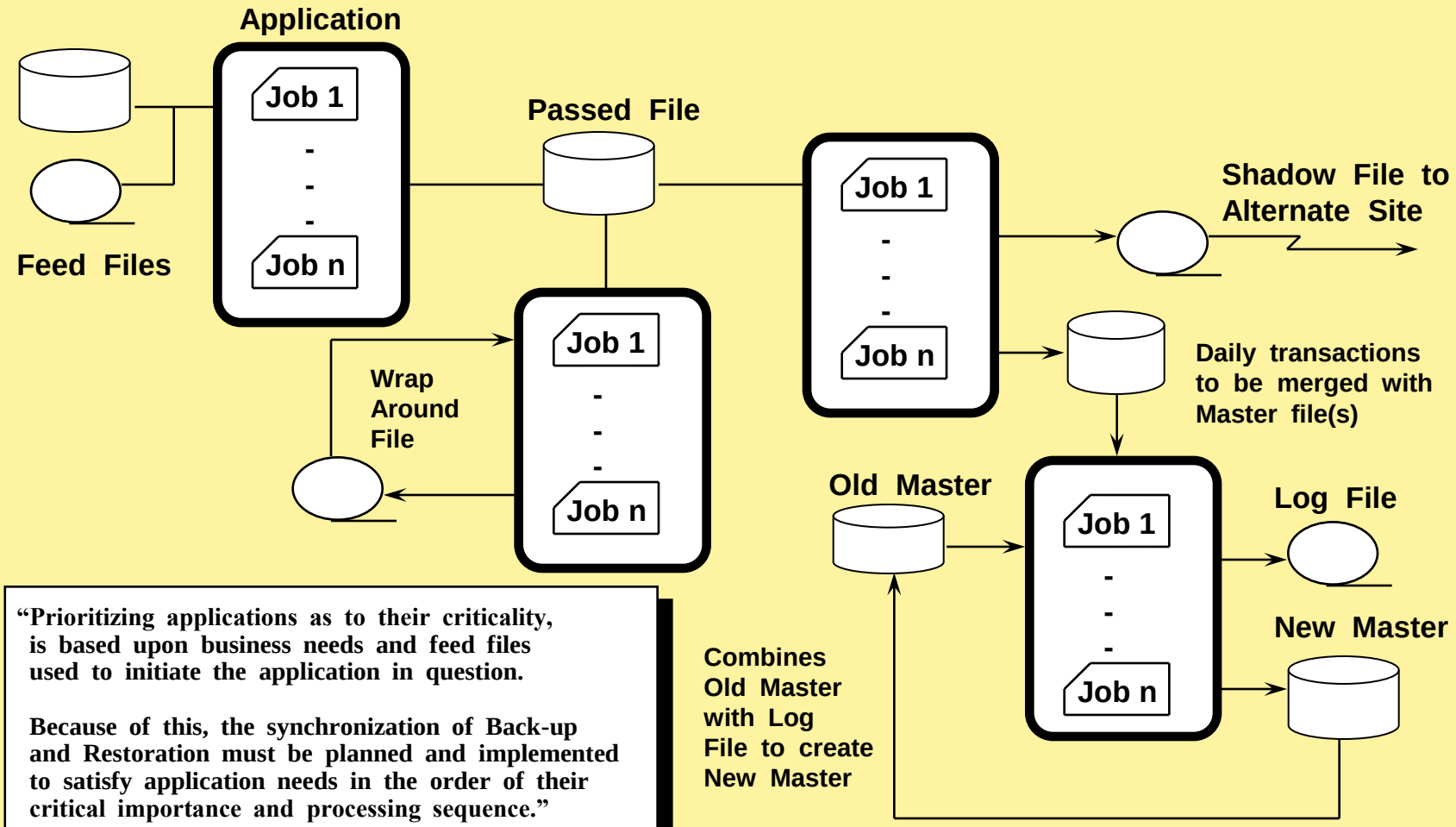
Applications de-allocate / allocate files for input / work / output operations. Then they process data for display and report generation. Finally backup and archive operations are performed to protect critical data and report on their status.



Critical data can be in Batch, On-Line, or Data Base Files.

Application Interconnections and Data Usage

The various methods for introducing data to an application, and maintaining it going forward, are shown below.

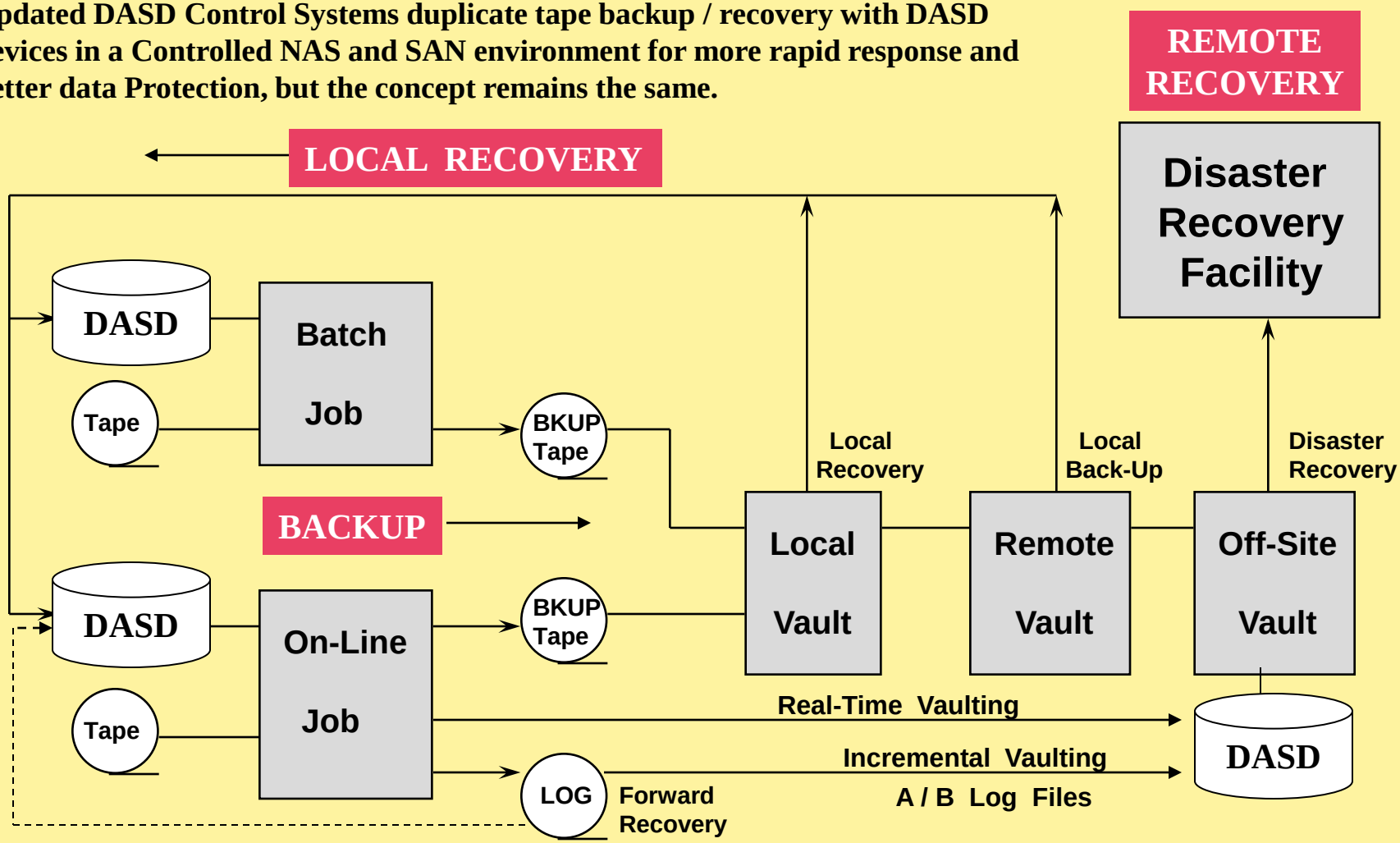


"Prioritizing applications as to their criticality, is based upon business needs and feed files used to initiate the application in question.

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."

Vital Records Management Techniques

Updated DASD Control Systems duplicate tape backup / recovery with DASD devices in a Controlled NAS and SAN environment for more rapid response and better data Protection, but the concept remains the same.



Why you need a Recovery Plan

Rapid increase in Regulations after 9-11-01

* 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, EPA Superfund, etc.

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

* Penalties.

- Three Times the Cost of the Outage, or more,
- Jail Time is possible and becoming more probable.

> "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.".

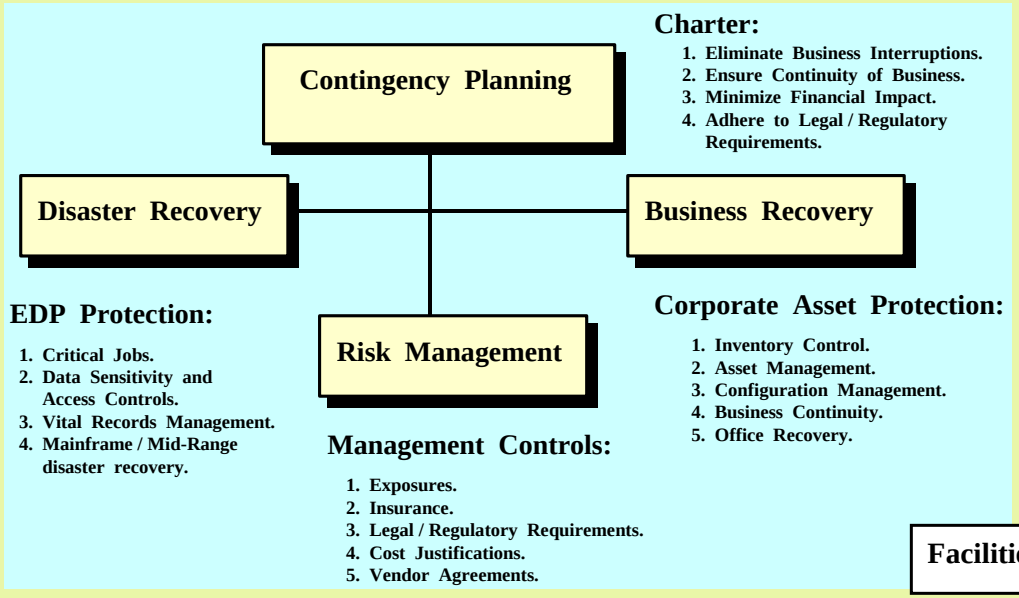
* Insurance.

- 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."

Contingency Planning

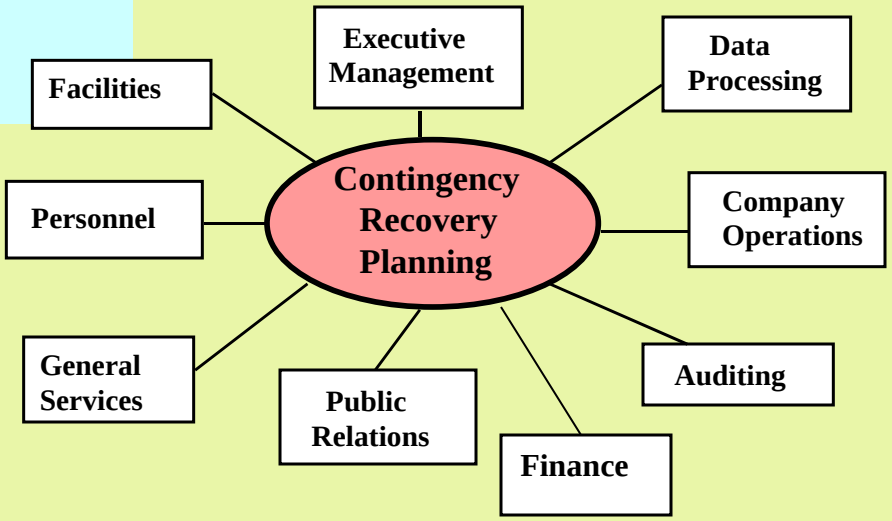
Contingency Recovery Disciplines



"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."

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 (Recovery Point Objective, Recovery Time Objective),**
- **Event Identification (Range of Disaster Event types),**
- **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.

Information Technology Risk Assessment (ITRA) Final Report Layout and Baseline Controls Matrices

(289 IT Risk Analysis Audit Controls are reviewed within the 13 areas listed below)

ITRA Deliverable Format:

- Cover Page
- Table of Contents
- Executive Summary
  - Introduction
  - Background
  - Summary of Findings
  - Recommendations
  - Conclusions
- Supporting Charts — Appendix I
- Overview — Appendix II
- IT Audit Schedule — Appendix III
- Definition of Risk Matrix Terms — Appendix IV
- Baseline Control Matrices — Appendix V
- Detailed Findings — Appendix VI
- Detailed Work Program — Appendix VII
- Technology Acronyms — Appendix VIII

Circled areas are condensed into one of the eight Baseline Control Matrices

Areas Covered within IT Risk Assessment

13 Areas broken down into 8 Baseline Controls

1. Organization and Management Policies.
2. Segregation of Duties.
3. Logical Access Controls.
4. Physical Access Controls.
5. Systems Development Life Cycle (SDLC) and Change Management Controls.
6. Incident Response (Problem Management, Help Desk, Problem Escalation, Crisis Management, etc.).
7. Business Continuity.
8. Data Center Computer Operations.
9. Network Communications.
10. Operating Systems Software.
11. Database Systems.
12. Application Systems.
13. End-User Computing.

Detailed Findings document

Finding:	Implication:	Priority:	Recommendation:
Critical Financial Files are not protected.	Security Flaw	High	Implement IT Security over files

The Detailed Findings document is used to list the top findings of the ITRA in Priority Sequence (High, Medium, Low). The Implication associated with the finding and supportive references to the Detailed Work Program are listed to further define the Findings and Implications associated with Gaps or Exceptions. Recommendations for mitigating any Findings are provided with the Finding and Implication for a Gap or Exception.

From this information, the customer can launch projects to correct any Findings and Implement our Recommendations for the identified areas. We can also provide the customer with the technical assistance needed to accomplish project goals and objectives. This is where TRM can be introduced to the customer as the technical arm of the organization.

Strategies for Eliminating Audit Exceptions ($$)

- Adhere to Compliance Requirements (Business and Industry) by implementing Business Continuity Planning disciplines;
- Implement Data Protection Techniques like Data Sensitivity, IT Security and Vital Records Management;
- Document SDLC, including: Development, Testing, Quality Assurance, Production Acceptance, Version Management, and Production Operations;
- Utilize Automated Tools;
- Eliminate "Single-Point-Of-Failure" concerns;
- Integrate Asset / Inventory / Configuration Management practices;
- Create Problem and Crisis Management practices and procedures;
- Optimize Work-Flow through Re-Engineering and Automation;
- Provide Documentation, Training, and Awareness programs.

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.

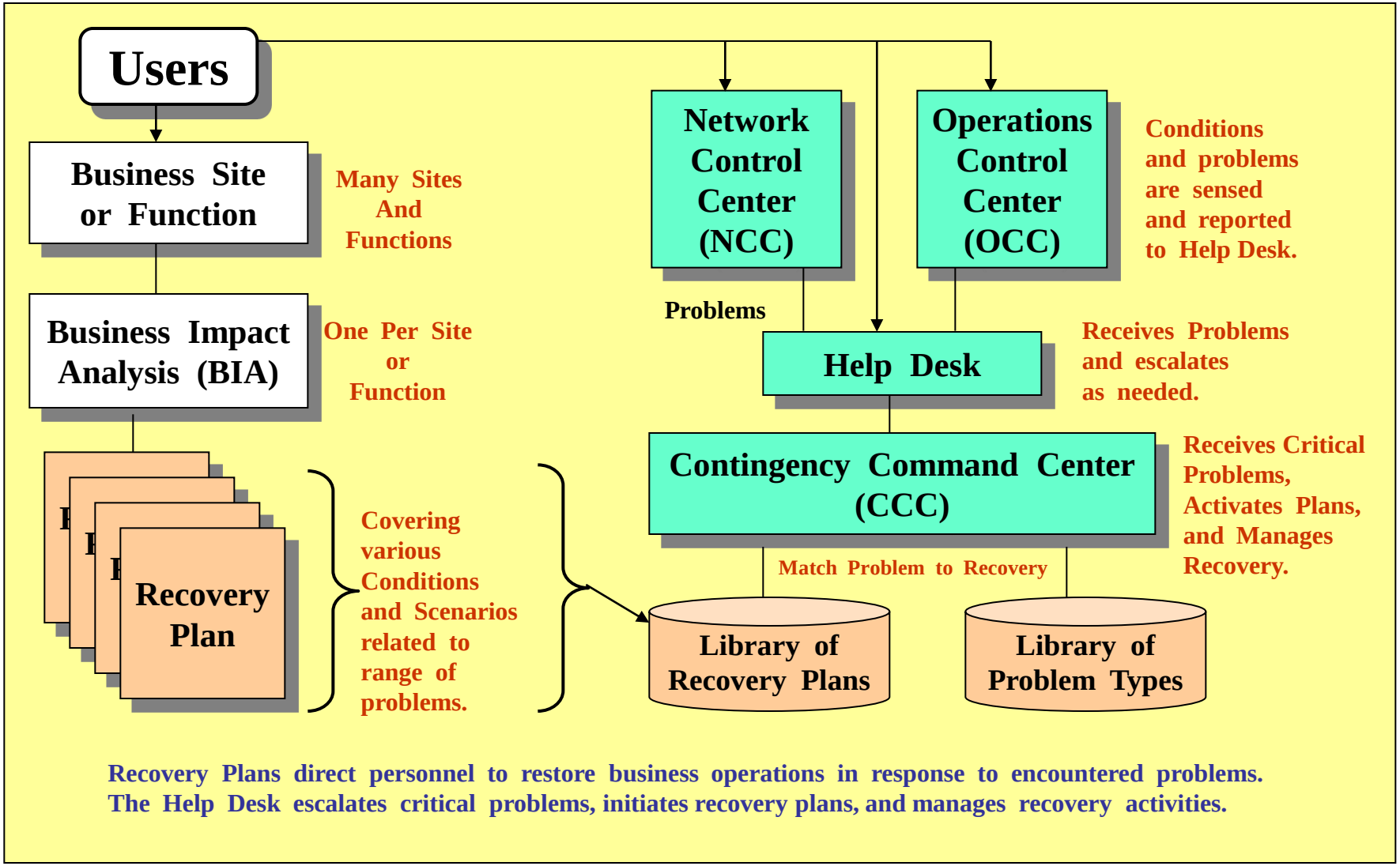
HAZARD SPECIFIC INFORMATION:

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

APPENDICES:

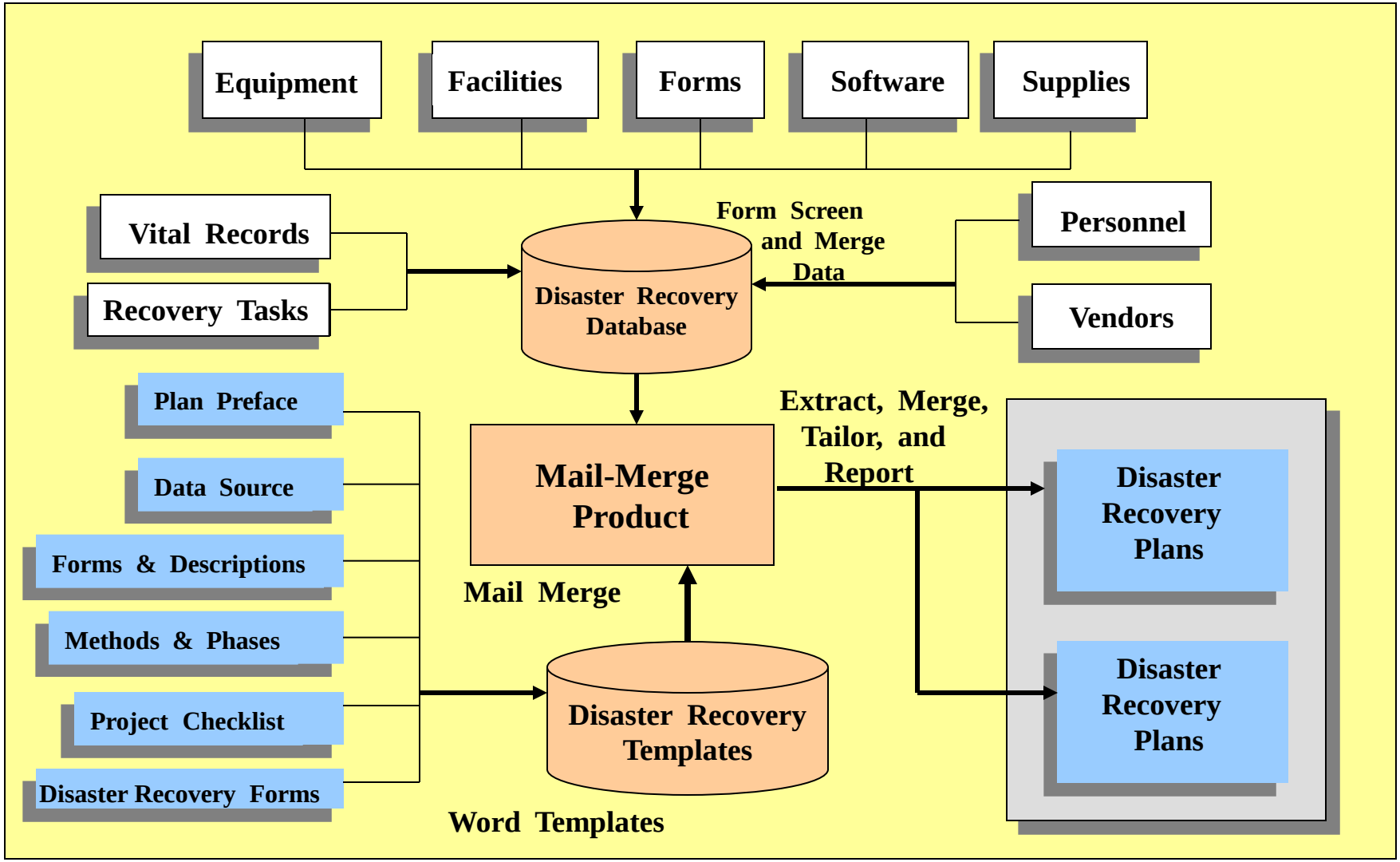
1. Vulnerability Analysis Chart.
2. Training Drills and Exercises Chart.
3. Information Sources (where to turn For additional information).

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.

Disaster Recovery Plan Data Sources and Output Generation



IT Security Management

1. IT Security Organizational Structure and assigned Personnel Positions.

2. IT Security Personnel and their Functional Responsibilities:
   a. Data Owner definition.
   b. Data Sensitivity.
   c. Data Usage guidelines.
   d. Data Access Controls.
   e. Violation Capturing.
   f. Violation Reporting.
   g. Required Forms.
   h. Procedures for completing forms.
   i. Forms submission and processing.

3. Existing Documentation and Training.

4. Standards and Procedures manual sections.

<NOTE>: The IT Security Management discipline will be included as needed in the SMC processes documented within the S&P Manual.

Vital Records Management

1. Define Vital Records Management Organizational Structure.

2. Define Vital Records Management personnel and their functional responsibilities.

3. Vital Records Management Standards:
   a. Vital Records definition;
   b. Library Management and Naming Conventions for Vital Records,
   c. Backup requirements;
   d. Vaulting requirements; and,
   e. Recovery requirements.

3. Vital Records Management procedures:
   a. Identification;
   b. Classification;
   c. Back-up procedures;
   d. Local Vaulting;
   e. Remote Vaulting, Retention, and Archiving;
   f. Restoration, Re-Use, and/or Destruction procedures;
   g. Interface with Tape Management System; and
      - Vault Management,
      - Encryption.

4. Vital Records Management Standards and Procedures Manual sections, including process descriptions.

Vaulting Backup Tape Life Cycle

8 Encryption?

1 Critical File

Local, NAS, or SAN

Local Vault

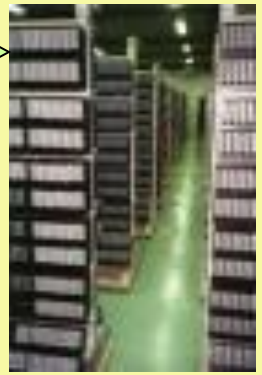
2

Tapes Transported To/From Customer Site

Backup Tape

Vaulting Cycle

3 Remote Tape Vault



4

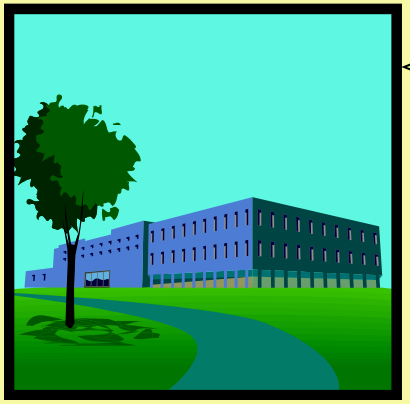
5

Backup Tape

6

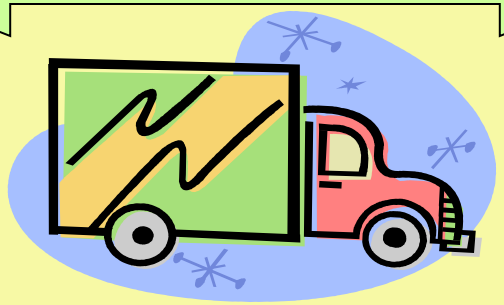
Return Cycle

7



Customer Site

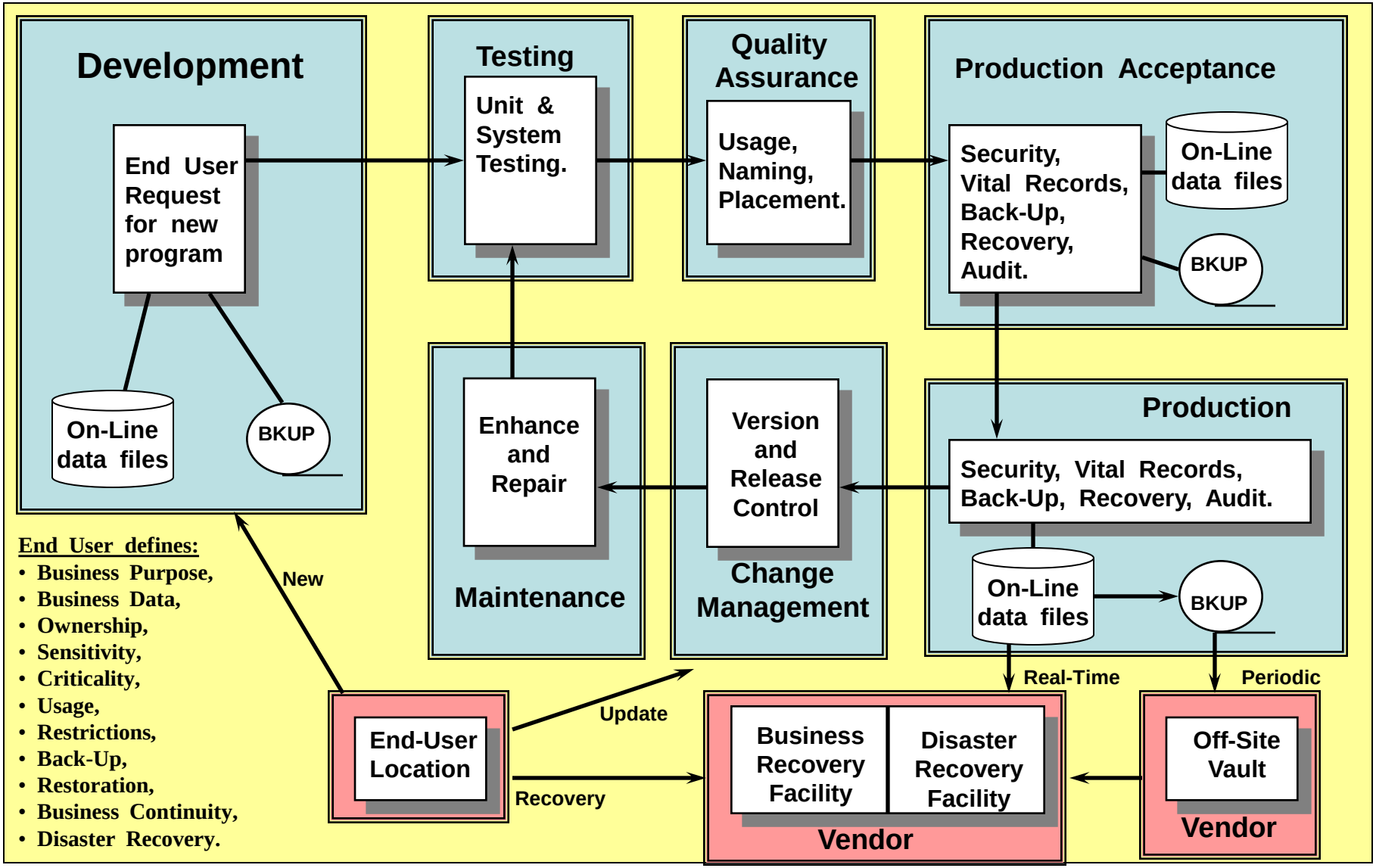
Transport To / From by Truck



Vital Records Transport

Remote Vault

Systems Development Life Cycle, INITIATING a development request



New Application Development Request Form Life Cycle

Development Request Form	Date:
User Information	_____
Business Justification	_____
Technical Justification	_____
Build or Buy?	_____
Development (Build/Modify)	_____
Test (Unit, System, Regression)	_____
Quality Assurance	_____
Production Acceptance	_____
Production	_____
Support (Problem / Change)	_____
Maintenance (Fix, Enhance)	_____
Documentation	_____
Recovery	_____

Link to Documentation

Documentation

- Business Need
- Application Overview
- Audience
- Business / Technical Review
- Cost Justification
- Build or Buy decision
- Request Approval

Documentation

- Sensitive Data
- IT Security
- Vital Records Management
- Tape Vaulting / Encryption
- Disaster Recovery
- Business Recovery

Documentation

- Support Programmer
- End User Coordinator
- Vendor Contacts
- Recovery Supervisor

Documentation

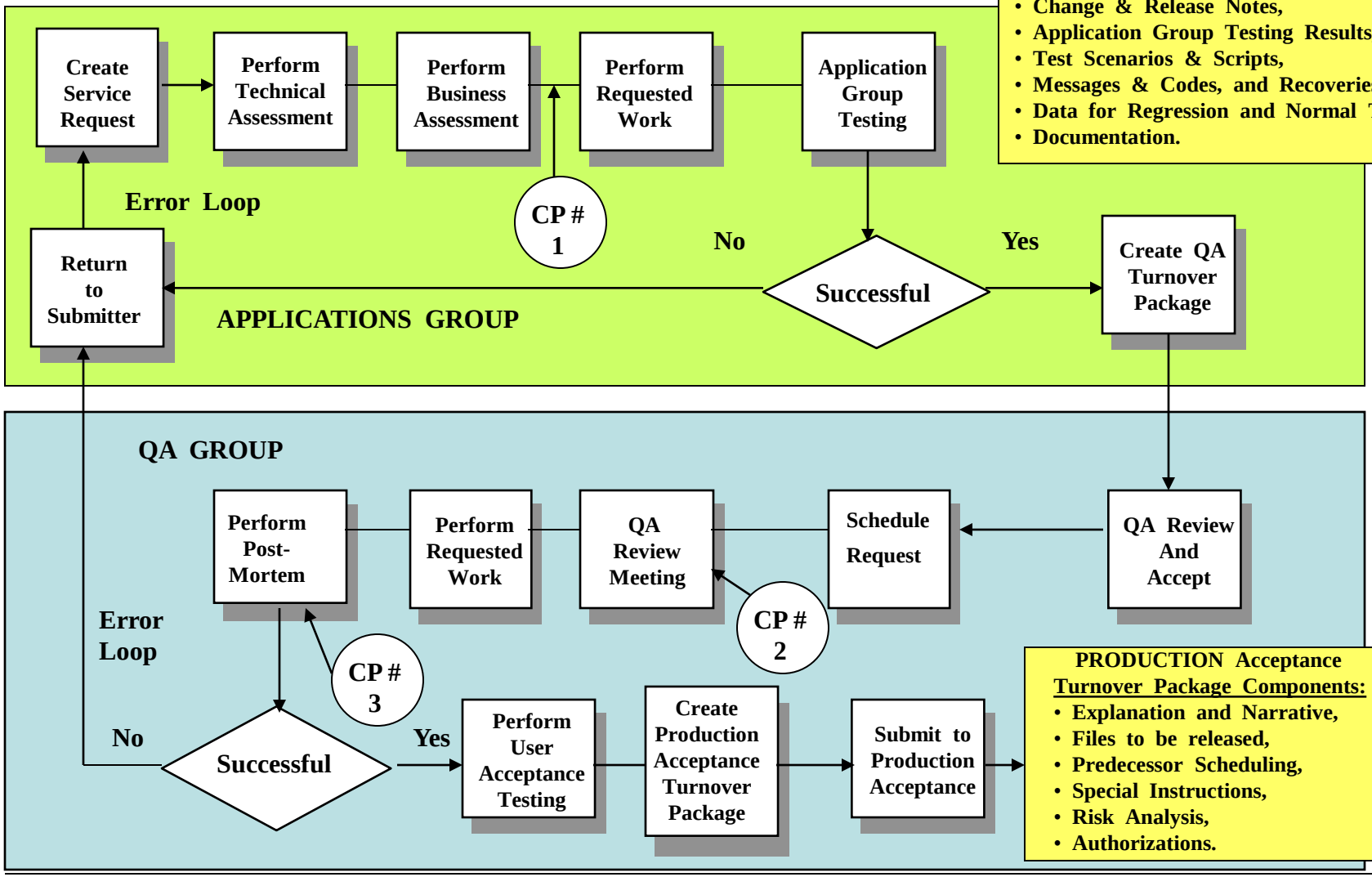
- Application Overview
- Application Setup
- Input / Process / Output
- Messages and Codes

Recovery Procedures

Dates are used to show application development status and as links to documentation

Quality Assurance and SDLC Checkpoints

Interfaces Between Applications, QA, and Production Groups.



TESTING and QA Turnover Package Components:

- Service Form and results from Assessments,
- Change & Release Notes,
- Application Group Testing Results,
- Test Scenarios & Scripts,
- Messages & Codes, and Recoveries,
- Data for Regression and Normal Testing,
- Documentation.

PRODUCTION Acceptance Turnover Package Components:

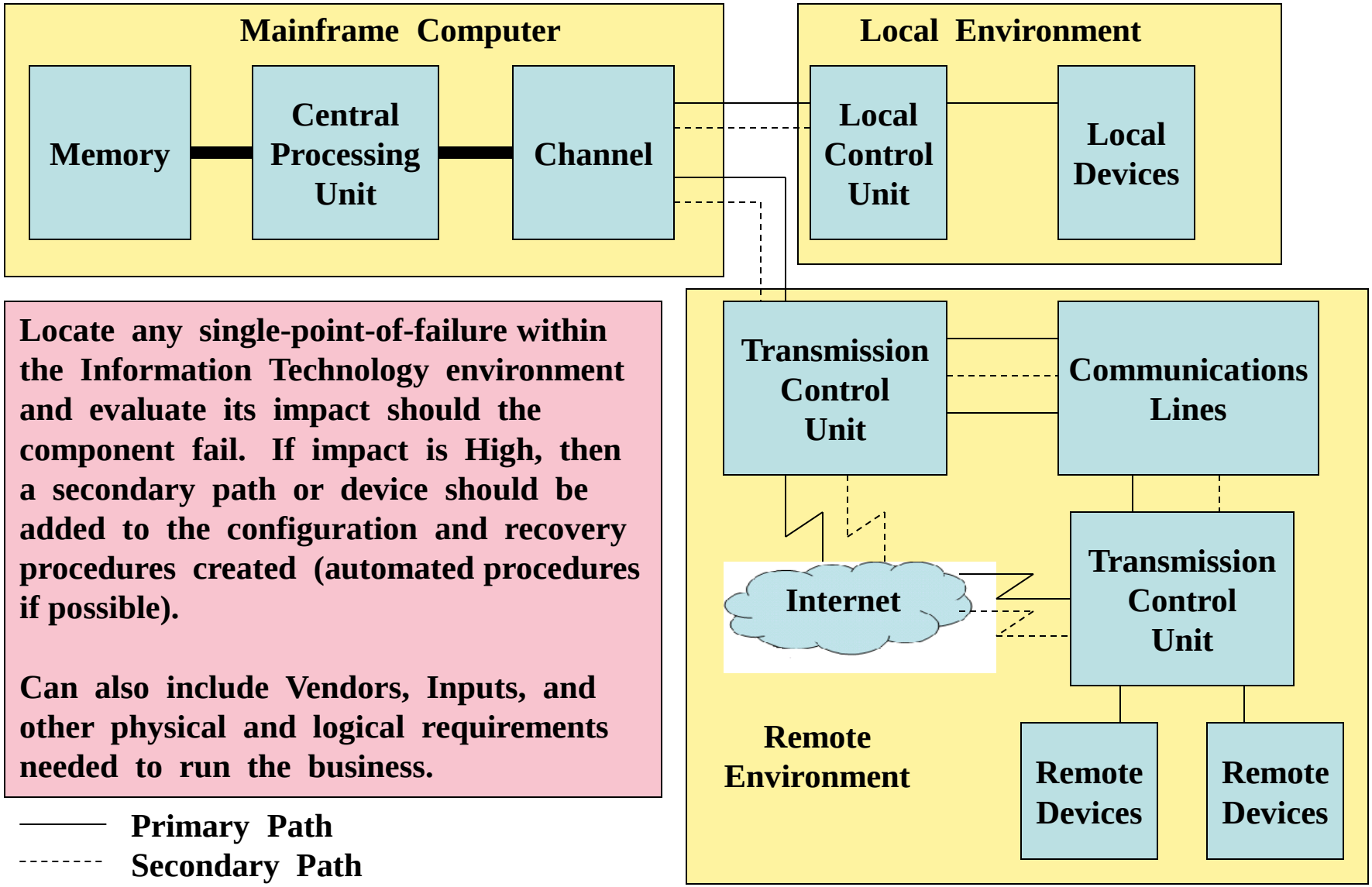
- Explanation and Narrative,
- Files to be released,
- Predecessor Scheduling,
- Special Instructions,
- Risk Analysis,
- Authorizations.

Utilizing Automated Tools

Whenever possible, automated tools should be utilized to:

- **Gather inventory information;**
- **Gather Business Impact Analysis (BIA) information;**
- **Merge BIA information into Business Continuity Plans.**
- **Scan paper documents through Optical Character Recognition (OCR) readers.**
- **Utilize Job Scheduler Information on job sequence and resource requirements.**
- **Utilize Job Scanners to validate sequence and resources.**
- **Utilize automated job turnover products like Endevor and PVCS to enforce standards, naming conventions, and placement requirements.**
- **Utilize communications analyzers like Netview to capture problems, initiate recoveries and circumventions, and to report problems to the help desk.**
- **Utilize Problem Management Systems and integrate them within the Help Desk environment.**
- **Assist Application Development and Maintenance.**
- **Supplement Systems Management Disciplines (Problem, Change, Capacity, Performance, etc.)**

Eliminating Single-Point-Of-Failure



Locate any single-point-of-failure within the Information Technology environment and evaluate its impact should the component fail. If impact is High, then a secondary path or device should be added to the configuration and recovery procedures created (automated procedures if possible).

Can also include Vendors, Inputs, and other physical and logical requirements needed to run the business.

——— Primary Path

- - - - - - - - Secondary Path

Identifying and Controlling Assets and Equipment

Asset Management (Financial and Legal)

- **Acquisition (Interface with Finance for costs and Legal for Vendor Agreement).**
- **Re-Deployment (Interface with Facilities Management for install and removal).**
- **Termination (Surplus Equipment Disposal).**
- **Financials (Total Cost of Ownership).**

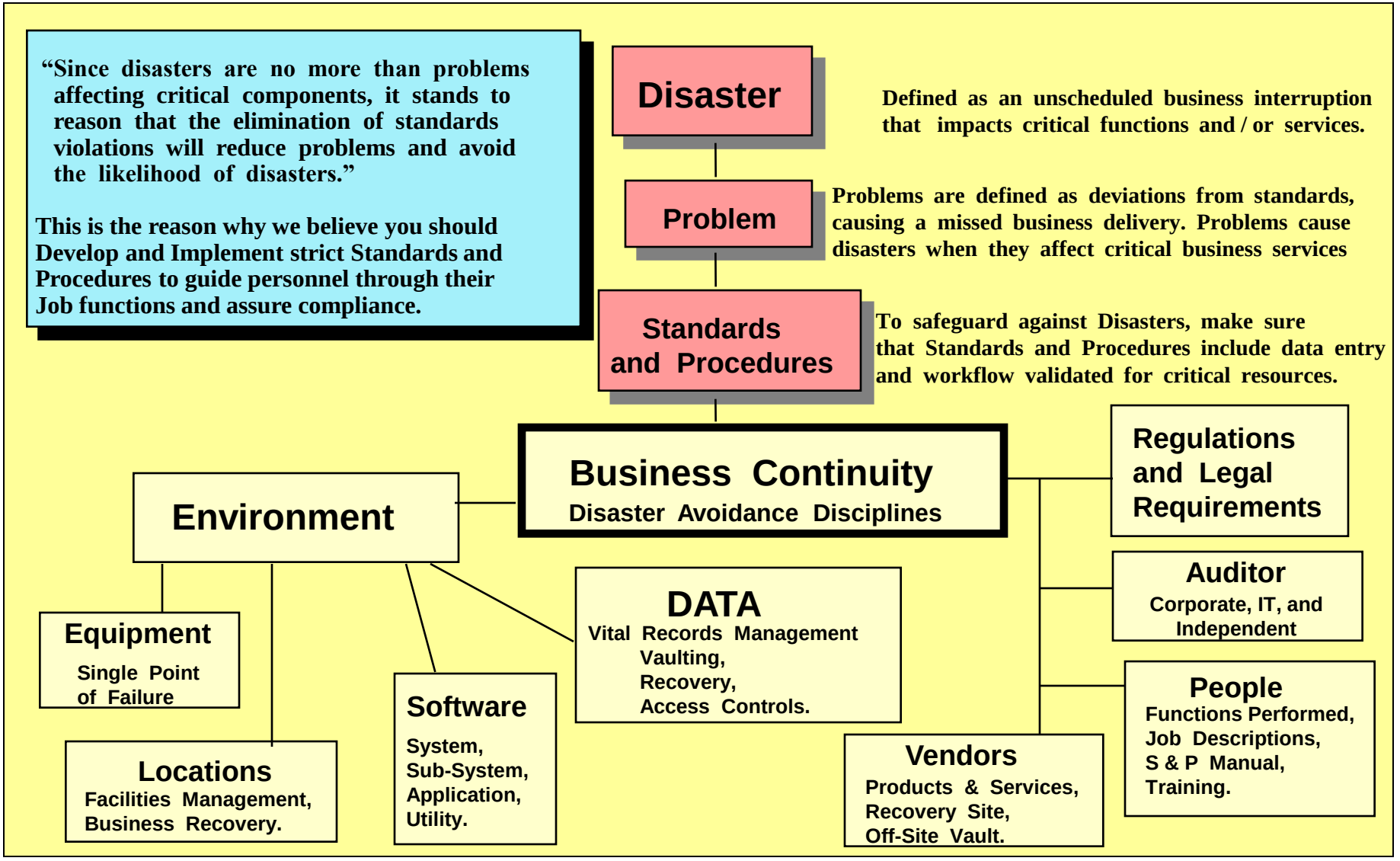
Inventory Management (Asset Location and Criticality)

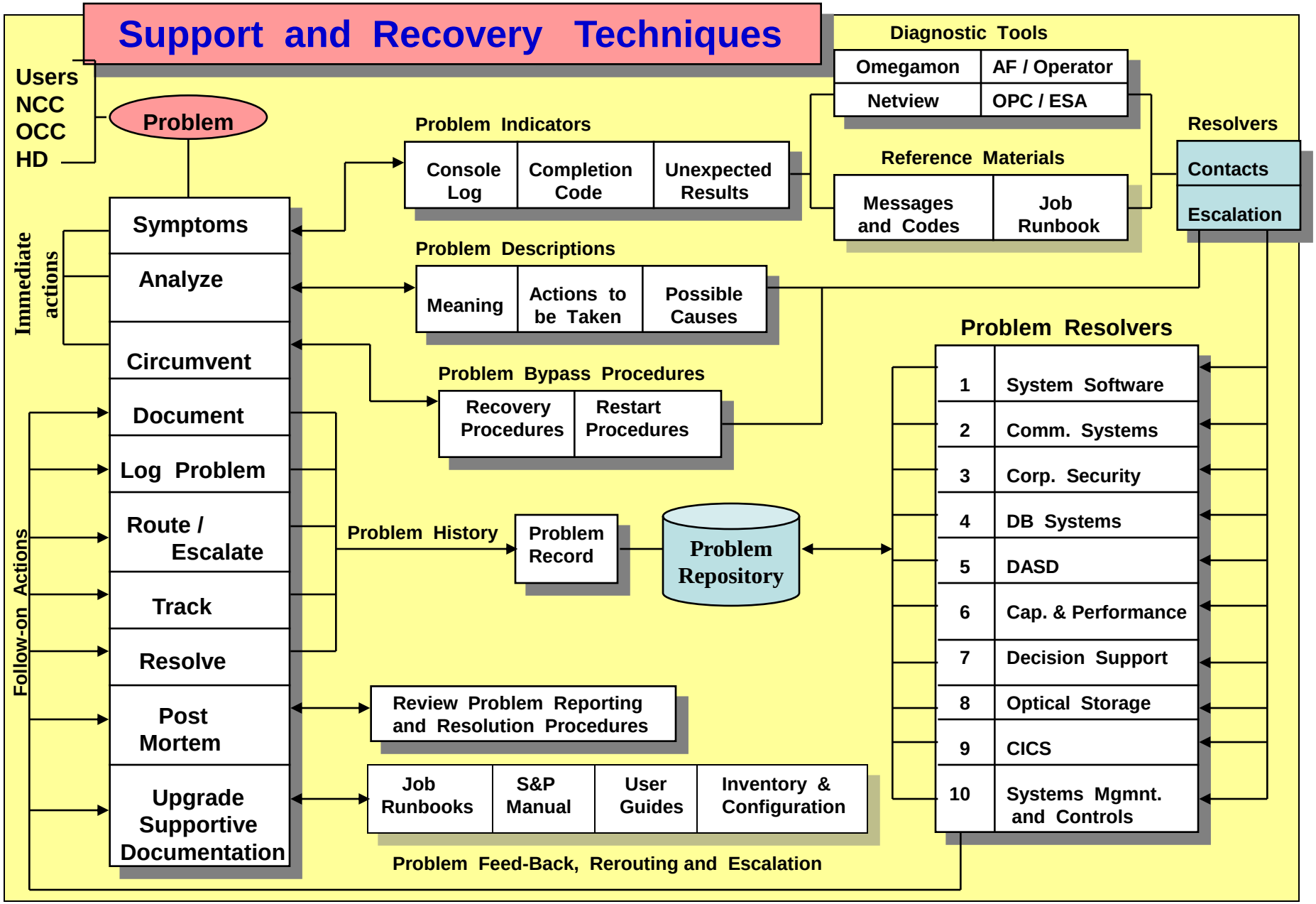
- **Resource Identification (Vendor Make and Model Information).**
- **Usage contract conditions.**
- **Location.**

Configuration Management (System and User)

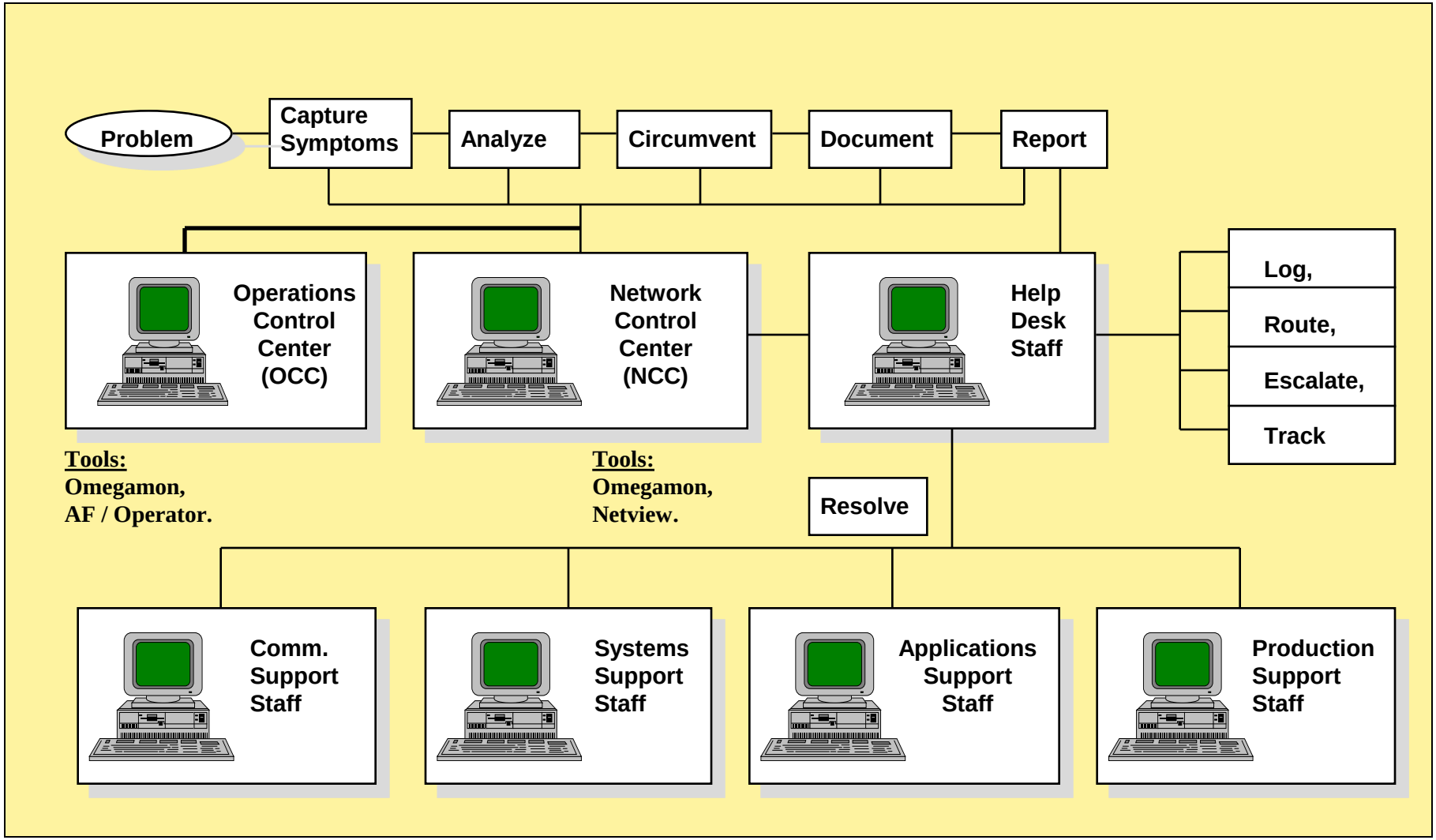
- **Component and Release Management.**
- **Systems Generation.**
- **Deployment, Installation, and Removal.**
- **Support (Problem and Crisis Management).**
- **Maintenance (Change Management)**

How disasters occur, and avoiding them....



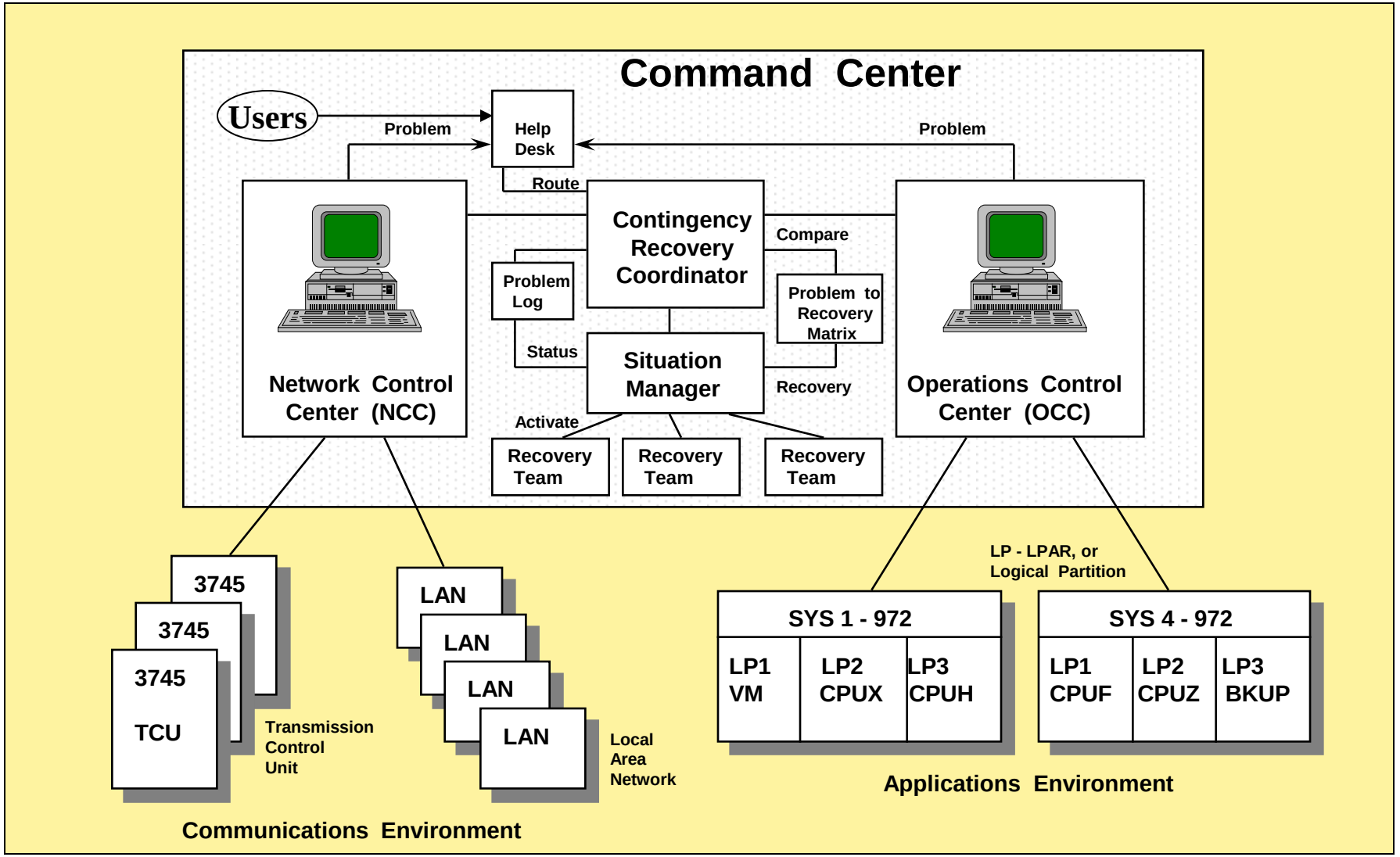

Support and Recovery Techniques
Users
NCC
OCC
HD
Problem
Diagnostic Tools
Omegamon
AF / Operator
Netview
OPC / ESA
Problem Indicators
Console Log
Completion Code
Unexpected Results
Reference Materials
Messages and Codes
Job Runbook
Resolvers
Contacts
Escalation
Immediate actions
Symptoms
Analyze
Circumvent
Problem Descriptions
Meaning
Actions to be Taken
Possible Causes
Problem Bypass Procedures
Recovery Procedures
Restart Procedures
Problem Resolvers
1 System Software
2 Comm. Systems
3 Corp. Security
4 DB Systems
5 DASD
6 Cap. & Performance
7 Decision Support
8 Optical Storage
9 CICS
10 Systems Mgmnt. and Controls
Follow-on Actions
Document
Log Problem
Route / Escalate
Track
Resolve
Post Mortem
Upgrade Supportive Documentation
Problem History
Problem Record
Problem Repository
Review Problem Reporting and Resolution Procedures
Job Runbooks
S&P Manual
User Guides
Inventory & Configuration
Problem Feed-Back, Rerouting and Escalation

Recovery Techniques and Personnel Involvement



Command Center Interactions

"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."

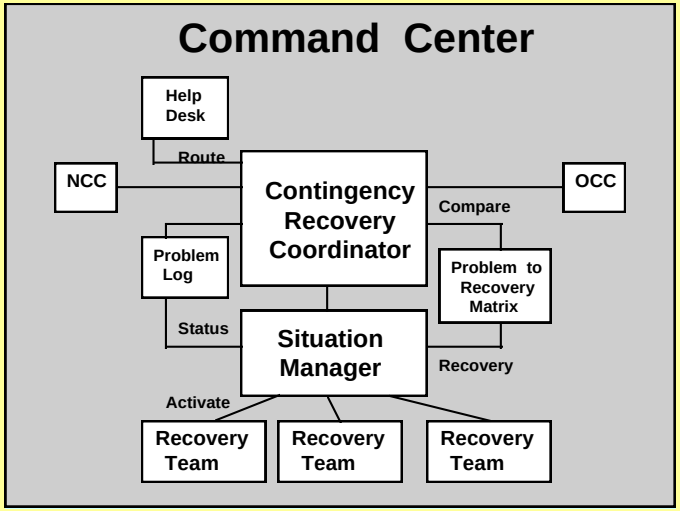


Contingency Recovery Operations

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

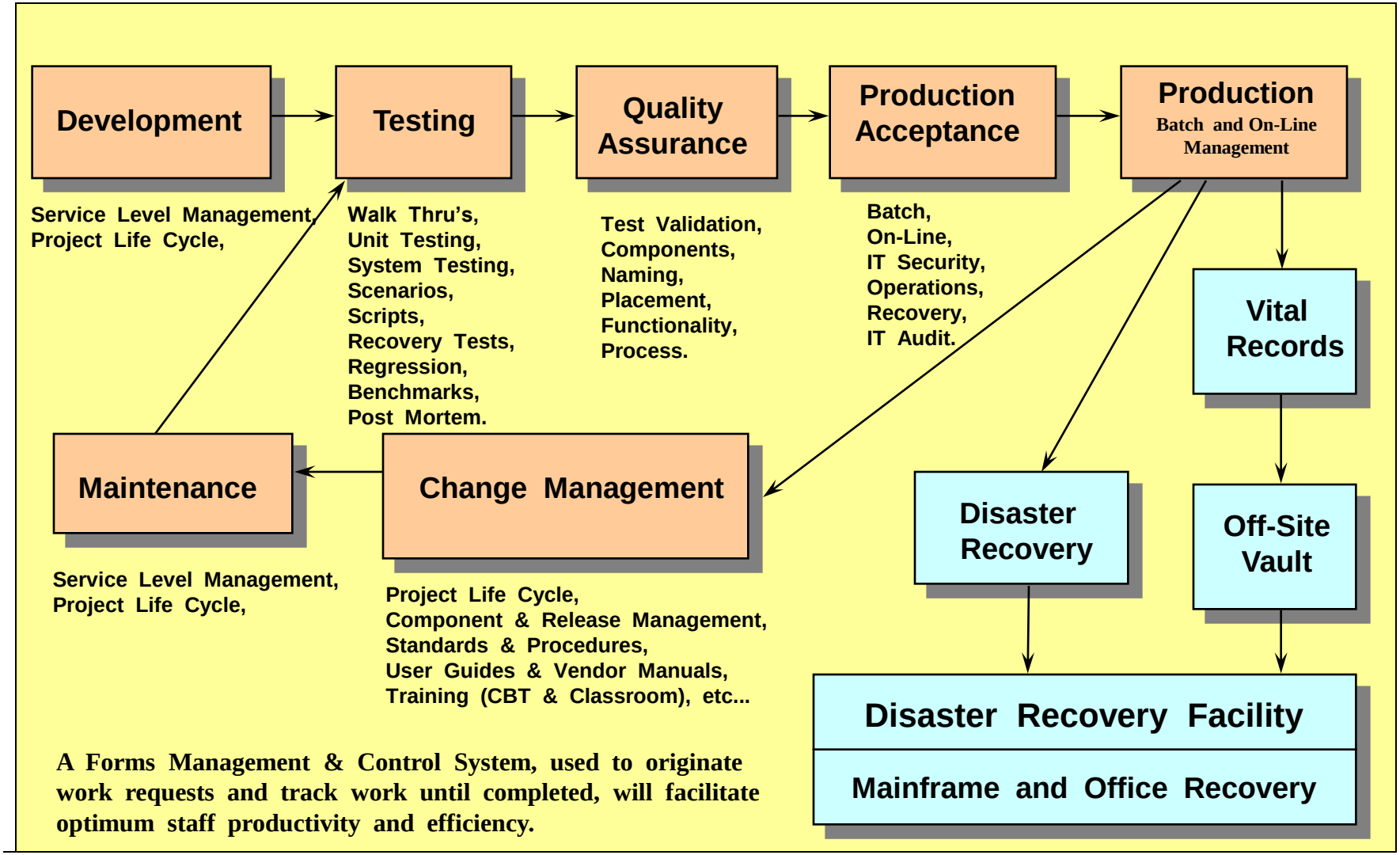
Reporting to the Contingency Recovery Coordinator and responsible for monitoring Recovery Team operations and providing assistance through any mechanism at their disposal. When situations become overly complex and a potential crisis can occur, the Situation Manager will take appropriate escalation actions 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.

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.

Standards and Procedures Manual - Structure

i. Table of Contents
ii. Benefits from S&P Manual.
iii, Company Overview.
iv. Division and Department Overview.
v. Compliance Requirements.
vi. Company Organization.
vii. Department Organization.
viii. Job Functions and Descriptions.
ix. Forms Library.
x. Workflow Analysis.
xi. Tools Analysis.
xii. Available Training.

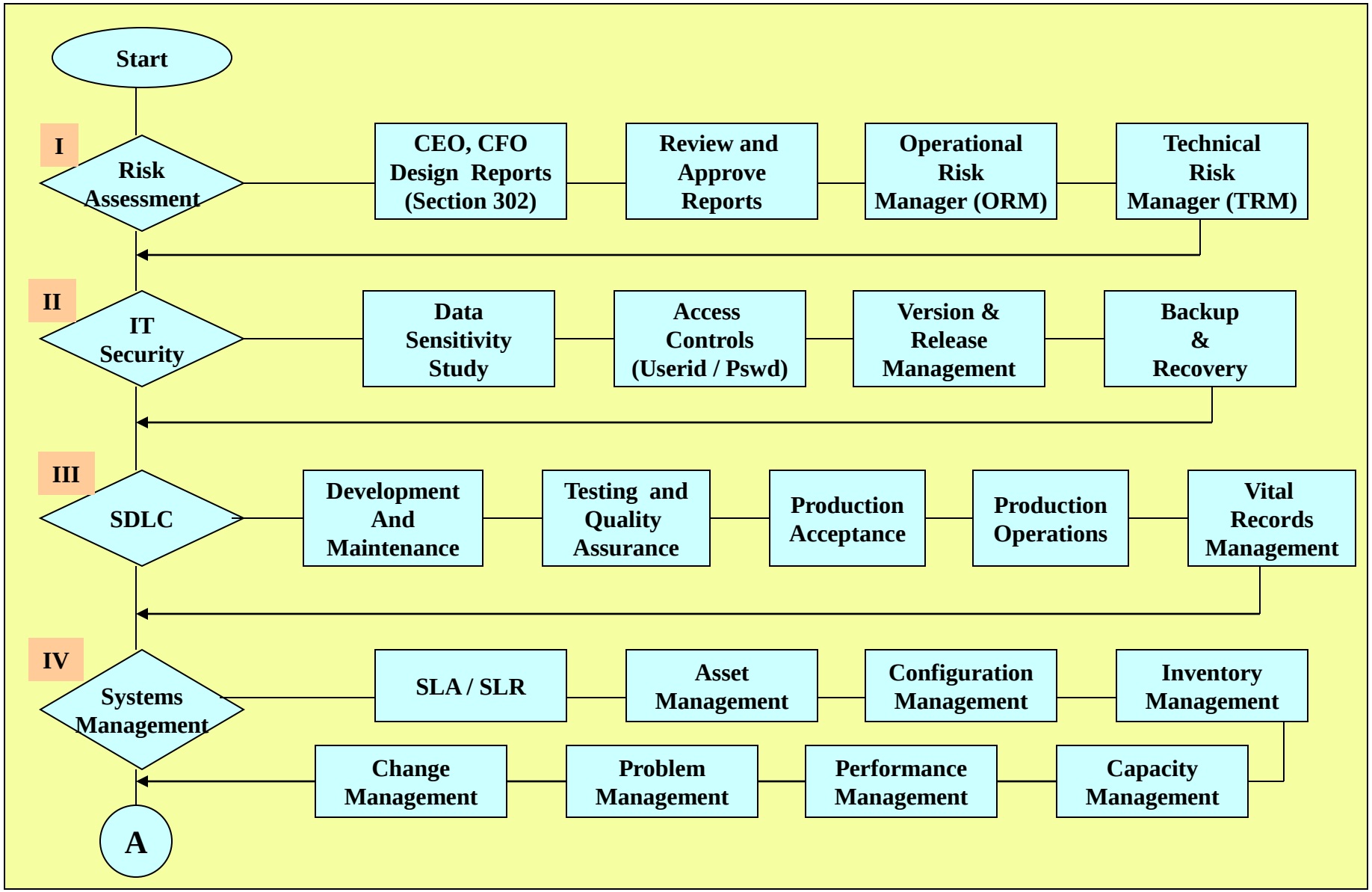
1. Service Level Management
2. Inventory Management
3. Configuration Management
4. Capacity Management
5. Performance Management
6. Application Development
7. Application Maintenance.
8. Application Testing.
9. Quality Assurance.
10. Production Acceptance
11. Production Operations
12. Recovery Management
13. IT Security Management
14. Vital Records Management
15. Change Management
16. Problem Management:
    a. Operations Control Center,
    b. Network Control Center,
    c. Help Desk,
    d. Crisis Management,
    e. Activating Contingencies,
    f. Contingency Command Center.
17. Data Processing Environment.

Business Recovery Services

- **Risk Assessment** to identify Continuity of Business (COB) exposures and gaps relating to newly adopted Business Recovery requirements.
- **Business Impact Analysis** requirements definition and risk analysis studies**,**
- **Data Sensitivity** studies and evaluations**,**
- **IT 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) (Evaluation through Selection),**
- **Business Recovery Training (Documentation, On-Line, and Class Room),**
- **Permanent Personnel Recruitment and Placement Services,**
- **Consulting, Outsourcing, and Temporary Personnel Services.**

Overall Project Phases (part 1 of 2)

Sarbanes Oxley IT Audit



Overall Project Phases (part 2 0f 2)