Crisis and Situation Management

SMC Disciplines

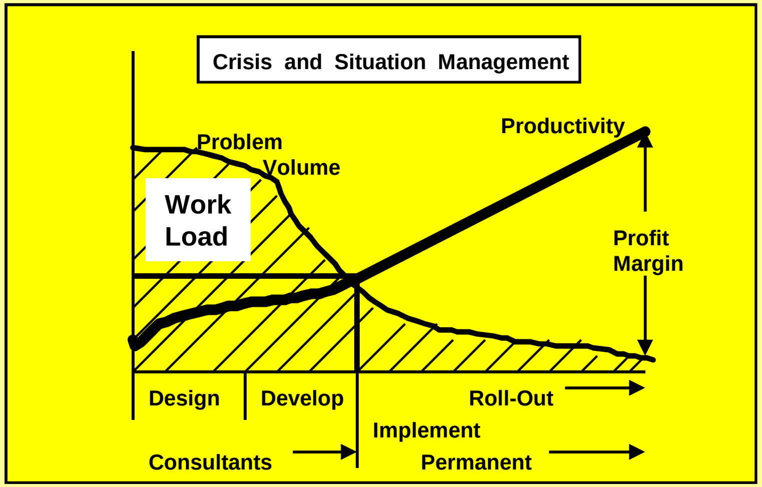
Prepared by:

Thomas Bronack, President
Data Center Assistance Group, Inc.
15180 20th Avenue
Whitestone, NY 11357

Phone: (718) 591-5553 Cell: (917) 673-6992
Email: bronackt@dcag.com

Table of Contents

Business Justification



With the increased complexity of our ever changing Information Technology environments, the opportunity for problem situations to become crisis' has increased.

To better prepare organizational responses to potential crisis situations, management has elected to implement the Crisis and Situation Management discipline -- a Systems Management and Controls (SMC) discipline.

Related to Recovery Management, Crisis and Situation Management utilizes pre-defined recovery plans to respond to encountered problems in an orderly fashion. Through these recovery plans, the impact of a problem is reduced and business operations achieve a higher degree of stability. Eventually, a reduction in problem volume and duration is accomplished. This increase in productivity lessens the demand for additional staff needed to respond to problem situations.

An increase in profit margins will be achieved by improving operational performance and reducing customer dissatisfaction caused by unscheduled outages.

These work load improvements will be achieved through the implementation of Crisis and Situation Management practices (one of the Systems Management Disciplines).

Charter

"Crisis and Situation Management is responsible for establishing Standards and Procedures that maximize operational responses to encountered problems and minimize business interruptions."

"By categorizing problems and their established recoveries within a matrix, the appropriate contingency plan can be activated that best responds to exceptional situations -- before they become a crisis."

"Much as Battle Stations are assumed within a military organization, when crisis situations occur personnel assume recovery team functions and management enacts a contingency organization to coordinate business operations."

"Through these efforts, business services are continued in a planned fashion and reactions are kept under control."

"The results obtained from this Systems Management discipline are fewer interruptions and a safeguarded environment that is capable of responding to a wide-range of disaster events"

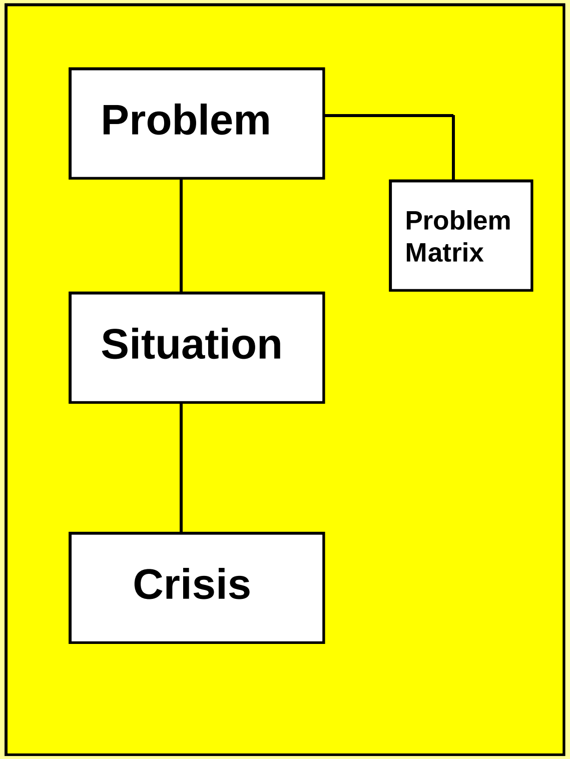
How Problems become Crisis'

When a problem arises and there are no formal procedures to direct Operations personnel in the analysis and repair of the problem, then a situation can occur that may lead to a potential crisis.

Compounding a problem by taking unnecessary actions can lead to a prolonged outage, which can affect the ability to meet deadlines. This additional scheduling problem may result in a situation which can lead to a crisis as well.

An example of this would be when a Data Check on a DASD device occurs and there are no back-up copies of the VOLSER. This problem would create a prolonged outage, because the data contents of the DASD volume would have to be recreated. Additionally, if multiple jobs are dependent upon the failed DASD Volume the effect of the problem will be even greater. This type of a crisis situation could very easily be avoided by insuring that all DASD volumes have back-up copies stored in the local tape library, so that restores can be provided.

The goal of this project is to determine which problem types can occur in the data processing environment, calculate our exposure to these types of problems, and then plan recovery procedures that will result in an orderly response to encountered problems - before they become situations and / or crisis'. The responses to encountered problems will be planned and added to a Problem Matrix, which relates problems to their planned recoveries - thereby avoiding situations that can lead to a crisis.



Problem Categories

HARDWARE:

- **EQUIPMENT CHECK**
  - **Hardware component suffered a machine failure, due to electronics or mechanics.**
    - **Only Vendor Service Representative can repair failing machine.**
  - **Recovery must be available to:**
    - **Bypass failing component,**
    - **Restore information on damaged DASD Volume.**
  - **Single-Point-of-Failure can be eliminated through multi-pathing and having a spare DASD Volume available for restoration and recovery.**

- **DATA CHECK**
  - **Data is received incorrectly:**
    - **Detected via Parity Check,**
    - **Usually related to damaged, or dirty, recording media.**
  - **Recovery procedures include:**
    - **Clean failing component,**
    - **Retransmit data,**
    - **Restore data to back-up component and retry,**
    - **Report failure to Vendor Service Representative.**
  - **Back-up copies of the data stored on critical components is essential:**
    - **Eliminate exposure to loss of data,**
    - **Allows for restore / recovery operations.**

Problem Categories continued...

SOFTWARE:

- ABEND
  - Derived from "Abnormal Ending",
  - Occurs when programs do not complete successfully,
  - Can occur when resources are missing or depleted,
  - Use Messages and Codes Manual to obtain Meaning, Actions to be Taken, and Probable Cause.
  - Use Job Runbook for application Abend explanations - format as Messages and Codes.
- MESSAGE
  - Generated to provide; Information, Instructions, or Error Indication.
  - Some require Operator Responses, before deletion from display (WTOR).
  - All messages should be listed in Messages and Codes Manual, or Job Runbooks.
  - Must explain Message, Actions to be Taken, and Probable Causes.
- WAIT
  - Wait States occur when event interrupt is not received by program, or system.
  - Can be caused by Device Not Ready, or Keyboard Lock-out types of conditions.
  - Wait State Codes explain wait condition.
  - Can be normal condition like "Out of Paper".
  - All Wait State Codes should be listed in Messages and Codes Manual, or Job Runbooks.
  - Must explain Wait State Code, Actions to be Taken, and Probable Causes.

Problem Categories continued...

LOOP

- Occurs when Conditioned Operation's ending condition is never sensed.
- Results from Unconditional Branch, or error blocks receipt of ending condition.
- Loops eat up processing cycles and elongate program run times.

- Can cause recording resources to fill, effecting system operation (i.e., JES2 Checkpoint, LOGREC, etc.).
- Stop system and take dump - record Loop addresses, if possible.
- Report problem and seek assistance.

INCORRECT RESULTS

- Output Balancing and Validation catches Incorrect Results in the I / O Control area.
- Can result from equipment (smudged output) or software (macro updated causing old macro to fail).

- Take dump at time of failure, if possible.
- Rerun job after correcting faulty device.
- Route results to Resolver and seek advice on resolution.

PERFORMANCE

- Usually detected when delivery schedules are not met, or when users complain of response times.
- Can be caused by resource contention.
- Can result from bottlenecks caused by failing paths, when multiple paths are available.
- Performance problems should be caught during Testing phase, when Benchmarks are performed.

- Capacity and Performance group can produce reports to help isolate flaws.
- Omegamon can illustrate performance bottlenecks.
- Problem resolution usually requires capacity upgrade, or elimination of points of contention.

Problem Matrix Format

Problem Matrix

Problem Type Matrix:

Problem Type:	Page:
Hardware:	
Mainframe	1
Channel	2
Control Unit	3
Device	4
DASD	5
Tape	6
Printer	7

Specific Problem Index Page

Device Problem - DASD

5.1 Problem Flow Chart.

5.2 Problem Description.

5.3 Problem Symptoms.

5.4 Actions to be Taken:

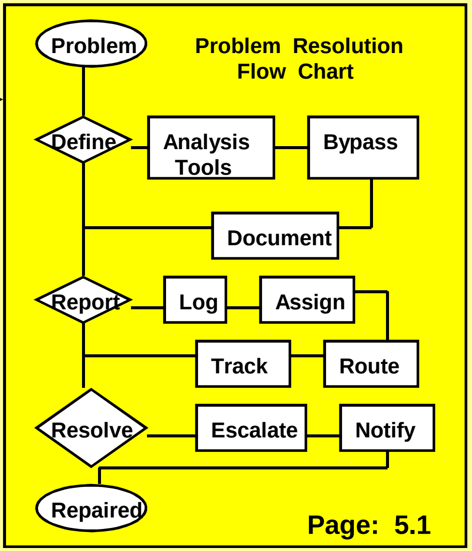
5.5 Circumventions / Bypass.

5.6 Probable Causes:

5.7 Personnel to Notify:

Page: 5

Problem Resolution Flow Chart



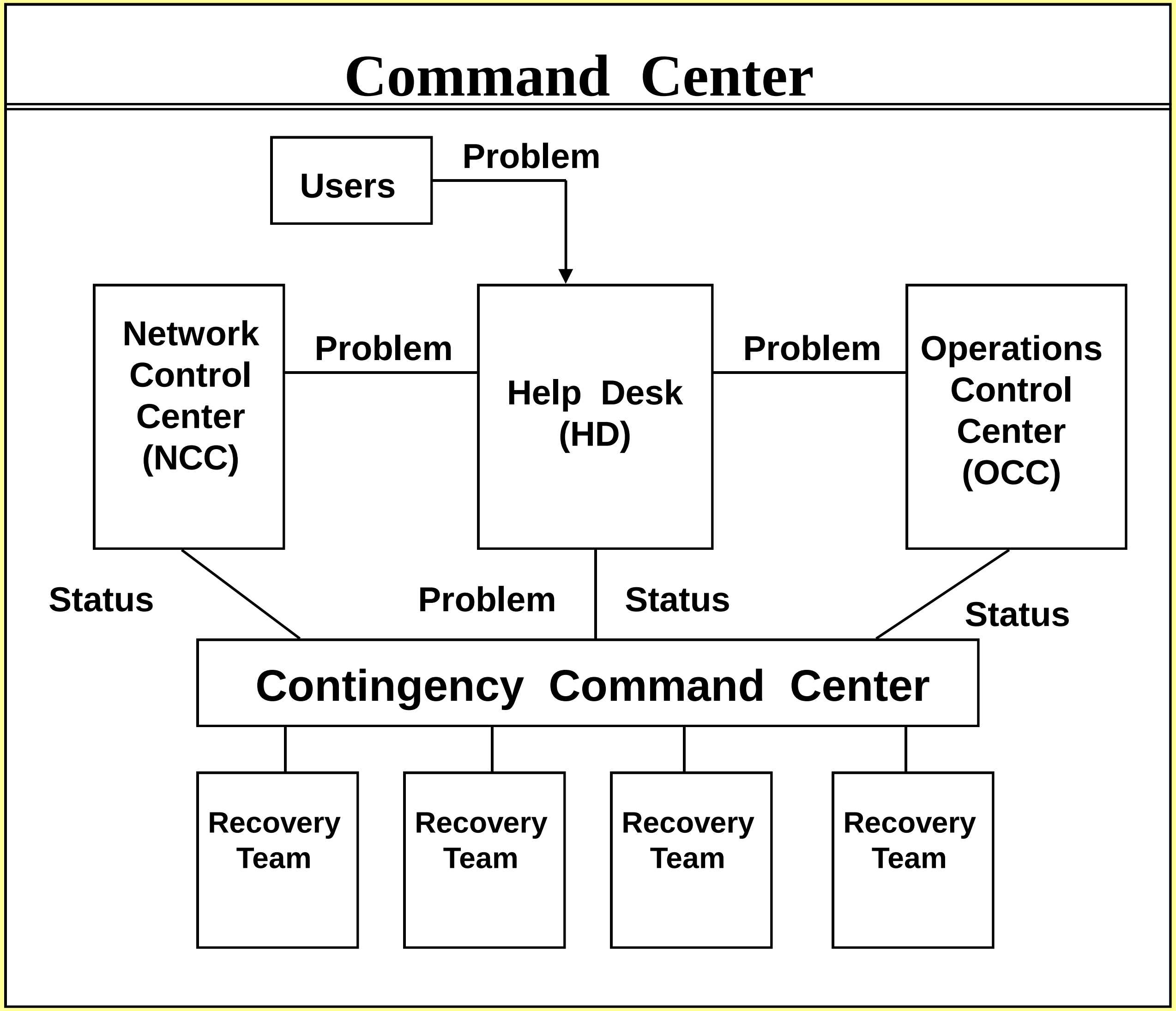
Problem Matrix Contents:

- Table of Contents Lists Problem Types.
- Page is provided for Problem Specific Data.
- Specific problem information assists in analyzing problem and provides Actions to be Taken when problem occurs.
- Problem Circumvention / Bypass is provided, if available.
- Causes of problem are provided, if possible.
- Personnel to contact when problem occurs, and escalations, are provided.
- Flowchart of problem resolution actions is provided, if possible.

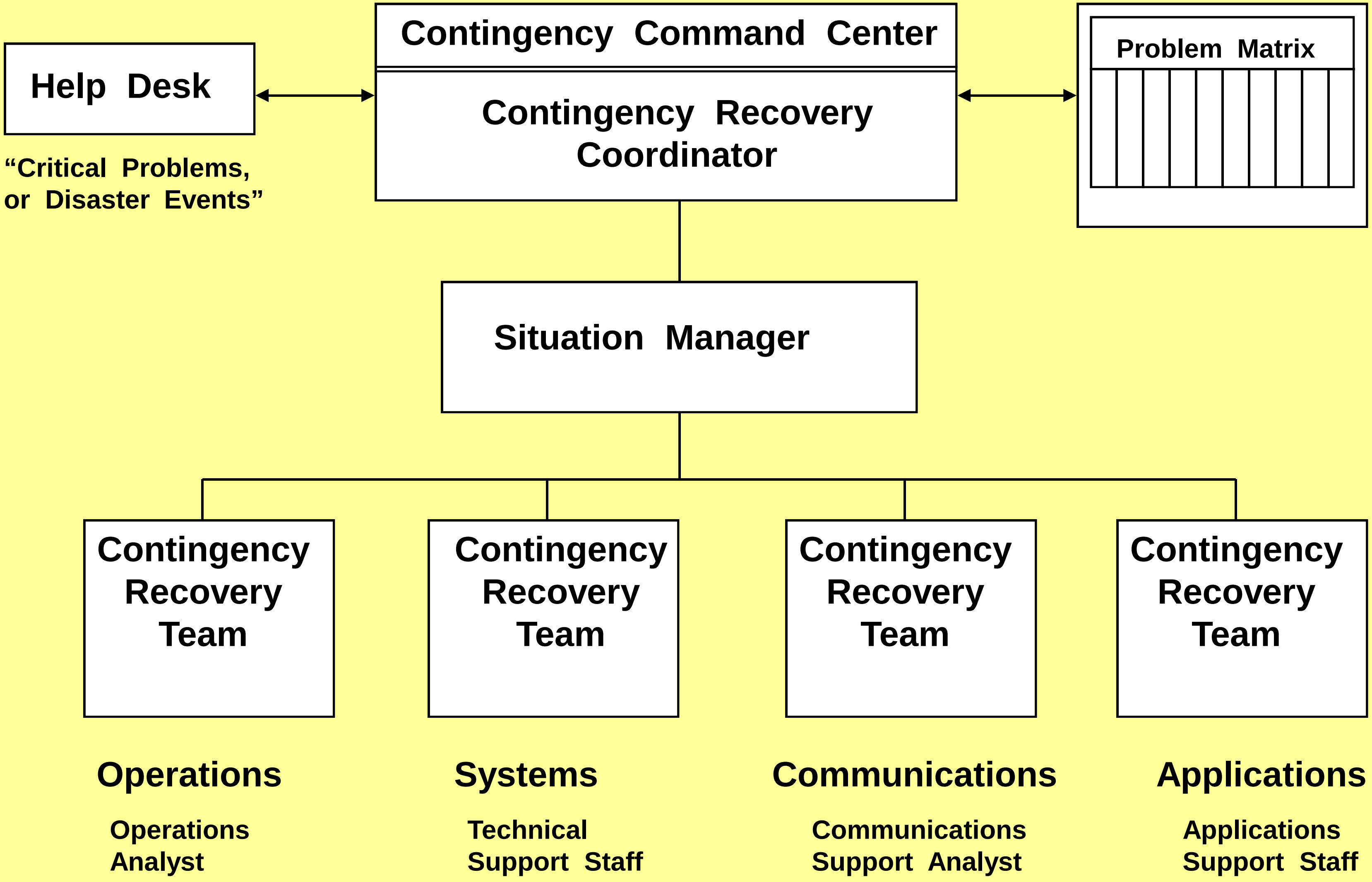
Contingency Command Center

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.**



Contingency Command Center Organizational Structure



Help Desk

"Critical Problems,
or Disaster Events"

Contingency Command Center

Contingency Recovery
Coordinator

Problem Matrix

Situation Manager

Contingency
Recovery
Team

Contingency
Recovery
Team

Contingency
Recovery
Team

Contingency
Recovery
Team

Operations

Operations
Analyst

Systems

Technical
Support Staff

Communications

Communications
Support Analyst

Applications

Applications
Support Staff

Contingency Recovery Coordinator

The roles and responsibilities of the Contingency Recovery Coordinator are:

- Review and analyze results of all recovery problems.
- Act as the primary representative for recovery procedure documentation and concerns.
- Secure the assistance of all appropriate parties to assess recovery management plans.
- Escalate appropriate recovery problems to management with supporting facts about proposed changes and recommended courses of action.
- Periodically evaluate and revise, when necessary, Recovery Management documentation.
- Perform discipline self assessments on an annual basis.
- Act as the focal point for questions and concerns about the recovery process.
- Attend weekly change review meetings, technical assessments, and pre-install meetings to ensure that recovery procedures have been reviewed, updated, and tested prior to installation.
- Analyze scheduled and unscheduled backup recovery exercises for success.
- Coordinate annual recovery procedure testing.

Situation Manager

The role of the Situation Manager is to maintain committed service levels by:

- Analyzing component failures in a timely manner.
- Implementing specific recovery processes.
- Activating the appropriate situation plan.
- Activating predefined situation teams using the support matrix.
- Being accountable for recovery.
- Authorizing any actions taken.
- Coordinating actions and schedules with all affected parties.
- Conducting management notifications.
- Acting as a focal point for notifications and escalations.
- Performing post recovery analysis and feedback.

Operations Analyst

The roles and responsibilities of the Operations Analyst are:

- Maintaining, in the computer room area, up-to-date recovery documentation.
- Executing recovery procedures for all host systems and host applications with assistance from appropriate support areas.
- Testing all host system and application recovery procedures.
- Recording pertinent information in the Turnover Log, including documentation and procedural problems.
- Logging host system and application outages in the Problem Management System.
- Ensuring all Operations recovery procedures adhere to standards and conventions.
- Informing the Quality Assurance department of any uncovered standards or convention violations that have been detected.
- Reviewing and supplying the necessary updates to the Standards and Procedures Manual for sections related to Operations and Production Support (i.e., Batch, On-Line, and Recovery Management).

Technical Support Staff

The roles and responsibilities of the Technical Support Staff are:

- Providing recovery procedures to Operations, Client / Server administration, and Network Control Center representatives as applicable.
- Testing recovery procedures prior to production installation.
- Ensuring recovery methods are included in the procedures.
- Ensuring existing recovery procedures are regression tested following system, network, or Client / Server changes.
- Ensuring that all applicable personnel are aware of and trained on the recovery procedures.

Communications Support Analyst

The roles and responsibilities of the Communications Support Analyst are:

- Maintaining up-to-date recovery documentation in the network operations support and LAN operations support areas.
- Executing recovery procedures for all communications systems and applications with assistance from any appropriate support area.
- Testing all communications system and application recovery procedures.
- Recording pertinent problem information in the Turnover Log including procedural and documentation problems.
- Logging communications system and application outages in the Problem Management System.
- Logging recovery time components for outages in the Problem Management System.
- Ensuring all communications recovery procedures adhere to standards and conventions.
- Informing Quality Assurance of communications recovery procedures not adhering to standards and conventions.
- Reviewing and supplying the necessary updates to the Standards and Procedures Manual that pertain to the communications environment.

Application Support Staff

The roles and responsibilities of the Applications Support Staff are:

- **Ensuring recovery methods are included in the development of new applications and changes to existing applications.**
- **Testing system recovery procedures prior to production installation.**
- **Ensuring recovery methods are included in the operational procedures.**
- **Ensuring existing recovery procedures are regression tested following system changes.**

Component Failure Impact Analysis (CFIA)

Systems & LPAR's Components:	System 1			System 4		
	LPAR 1	LPAR 2	LPAR 3	LPAR 1	LPAR 2	LPAR 3
Systems	VM	CPUX	CPUY	CPUA	CPUB	BACKUP
Channels						
Parallel	18	10	3	25	17	17
ESCON	1	44	25	35	38	7
Applications:	Devl./ Maint.	Test	QA	Prod01	Prod02	D/R, etc.
Environmentals:						
HVAC						
Power						
Water, etc...						

LPAR Configurations

ES / 9021 - 972 - SY1

LP1 - VM

512 MB CSTOR
768 MB ESTOR
120 MIP's Allocated
3 CP's Defined
18 Parallel Channels
1 ESCON Channels

Applications:

LP2 - CPUX

512 MB CSTOR
1280 MB ESTOR
140 MIP's Allocated
5 CP's Defined
10 Parallel Channels
44 ESCON Channels

Applications:

LP3 - CPUY

512 MB CSTOR
1024 MB ESTOR
100 MIP's Allocated
5 CP's Defined
3 Parallel Channels
25 ESCON Channels

Applications:

ES / 9021 - 972 - SY4

LP1 - CPUA

980 MB CSTOR
1024 MB ESTOR
235 MIP's Allocated
6 CP's Defined
25 Parallel Channels
35 ESCON Channels

Applications:

MTS
COMMODITIES
SWAPS
CMC

LP2 - CPUB

512 MB CSTOR
1024 MB ESTOR
125 MIP's Allocated
6 CP's Defined
17 Parallel Channels
38 ESCON Channels

Applications:

All Testing for
CPUF and CPUX

LP3 - BACKUP

64 MB CSTOR
64 MB ESTOR
0 MIP's Allocated
2 CP's Defined
17 Parallel Channels
7 ESCON Channels

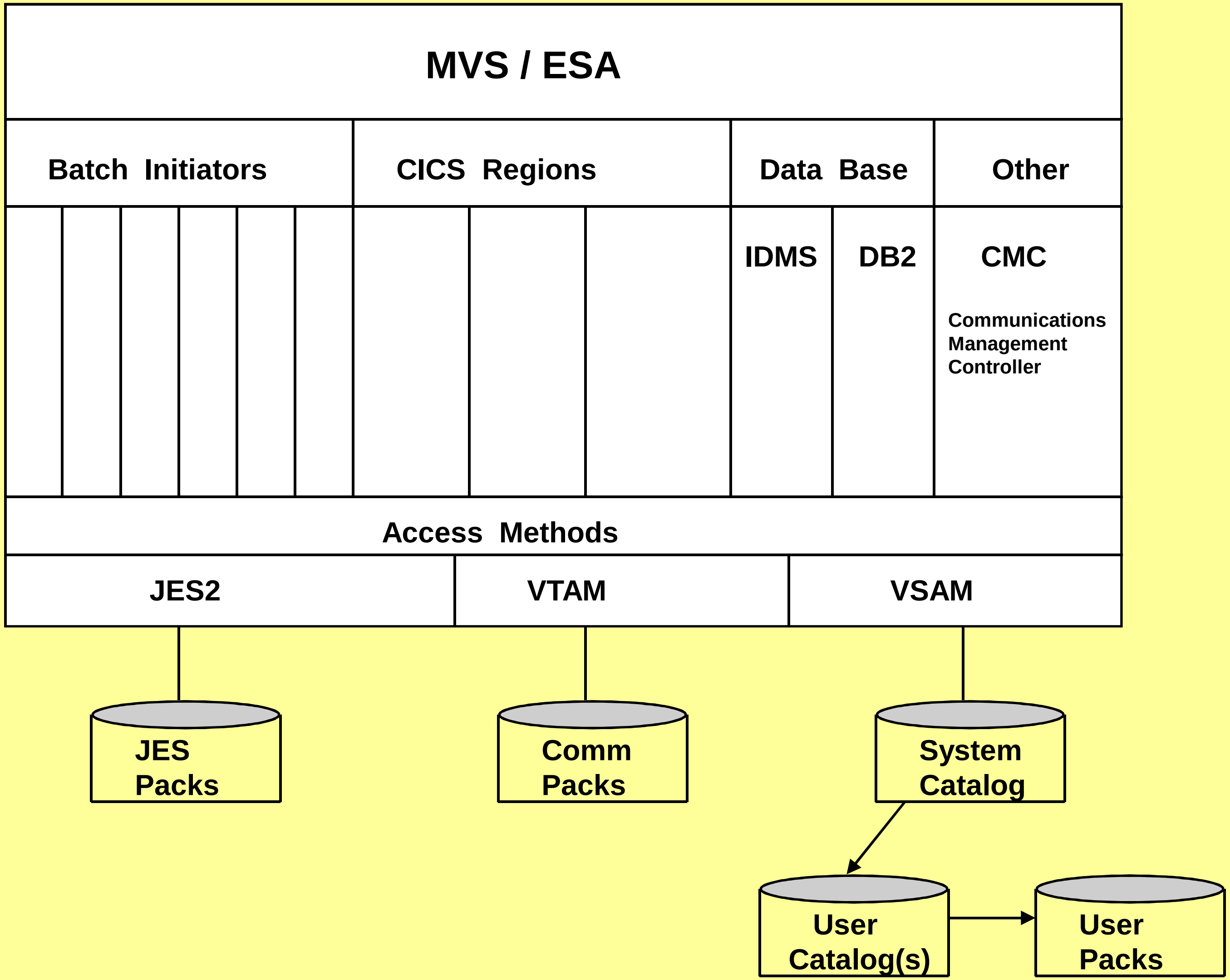
Applications:

Backup for VM
Testing for VM / ESA
Testing for MVS 4.3

LPAR Contents

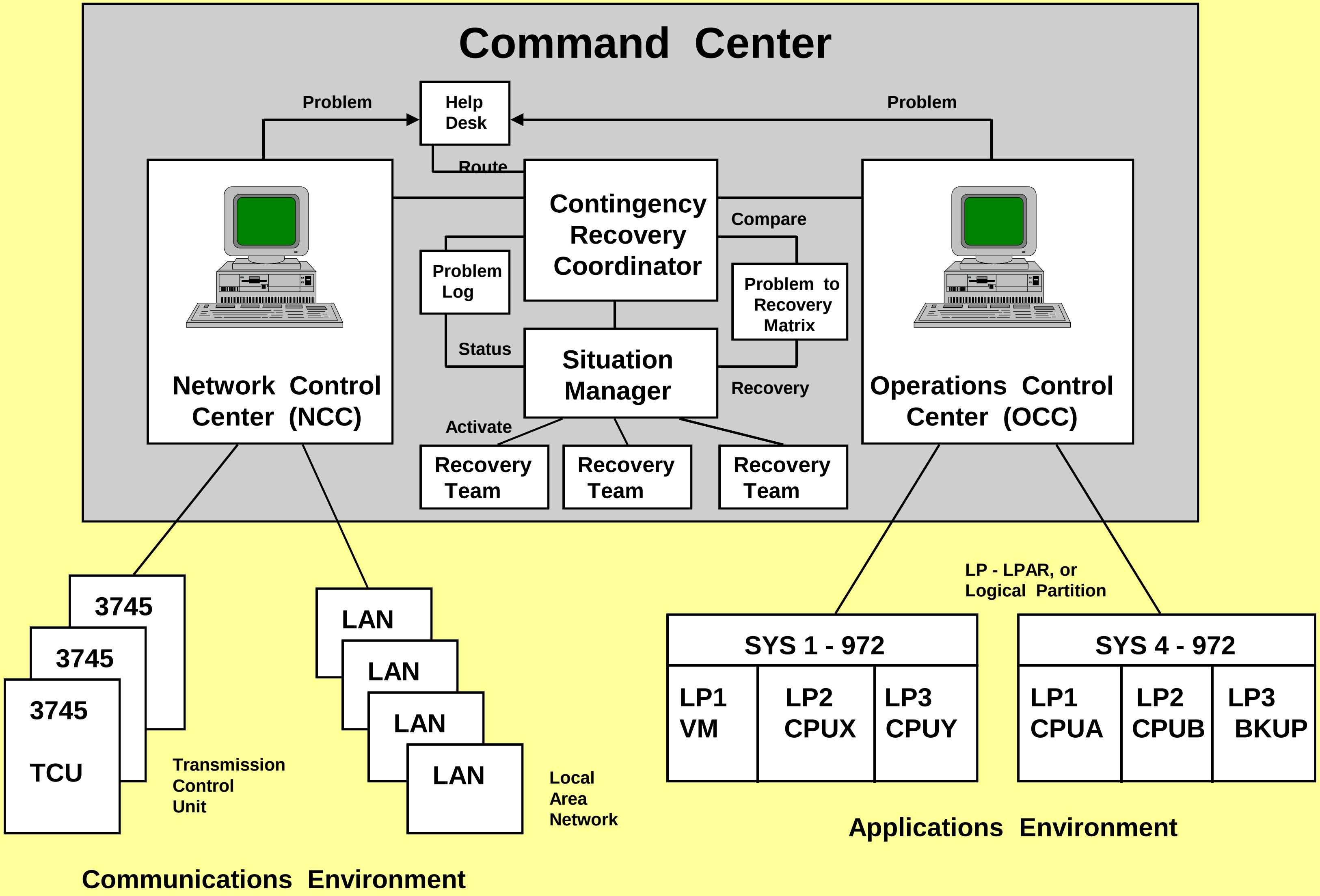
Recoveries must exist for:

LPAR's,
Batch Jobs;
CICS Tasks;
Data Bases;
JES2;
Communications;
and
Logrec filling;
JES2 Spool failure.



Command Center

"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."



Command Center

Problem

Help Desk

Problem

Route

Contingency Recovery Coordinator

Compare

Problem Log

Problem to Recovery Matrix

Status

Situation Manager

Recovery

Network Control Center (NCC)

Operations Control Center (OCC)

Activate

Recovery Team

Recovery Team

Recovery Team

LP - LPAR, or Logical Partition

3745

3745

3745

TCU

Transmission Control Unit

LAN

LAN

LAN

LAN

Local Area Network

SYS 1 - 972

LP1 VM

LP2 CPUX

LP3 CPUY

SYS 4 - 972

LP1 CPUA

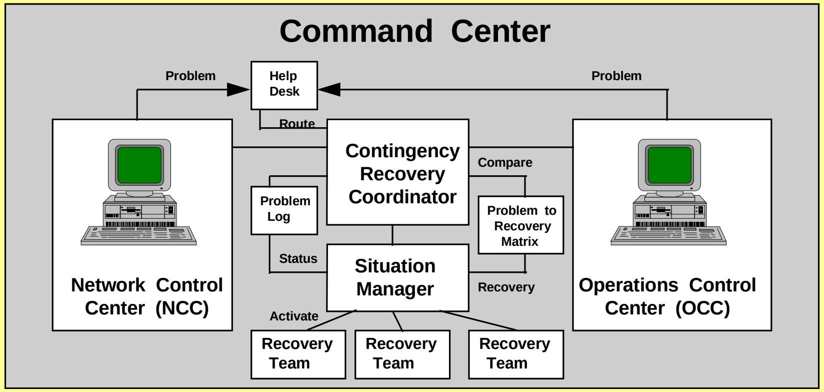
LP2 CPUB

LP3 BKUP

Applications Environment

Communications Environment

Command Center Operation



When a problem is reported to the Help Desk that is classified as a potential crisis situation, the problem is routed to the Contingency Recovery Coordinator.

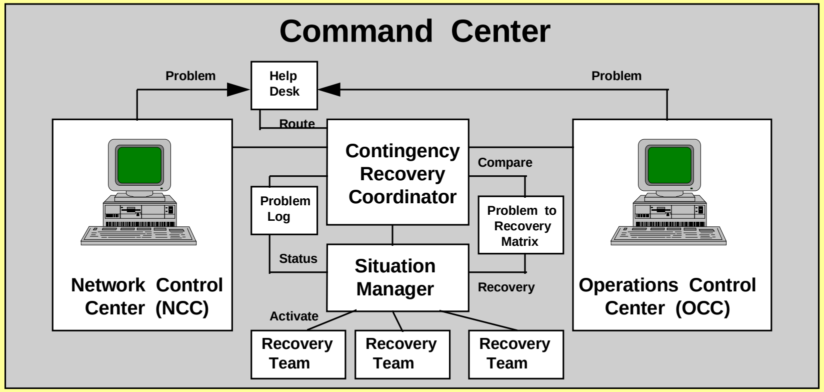
The Contingency Recovery Coordinator will compare the problem with the Recovery Matrix to select the recovery plan that best responds to the reported problem. Once the recovery plan has been selected, the Contingency Recovery Team is activated.

Upon activation, the Contingency Recovery Team takes appropriate recovery actions to restore damaged resources and establish an environment capable of continuing to supply business services. Recoveries can be as simple as restarting a job, or as complex as relocating operations to a recovery facility located in another state.

Because of the range of problem and recovery possibilities, it is essential that problems are classified and recovery procedures supplied to the operations staff when something new is added to the production environment, or when an existing process is altered.

Also, by establishing standards and procedures governing the acceptance of products and services within the business environment, it will be possible to reduce problem situations and the potential crisis' that can accompany them.

Command Center Components



Network Control Center (NCC)

Responsible for all operational functions within the communications environment and for monitoring operations for performance flaws and problems. When problems arise, the NCC operator will take appropriate actions to circumvent the problem (if possible) and then report the problem to the Help Desk.

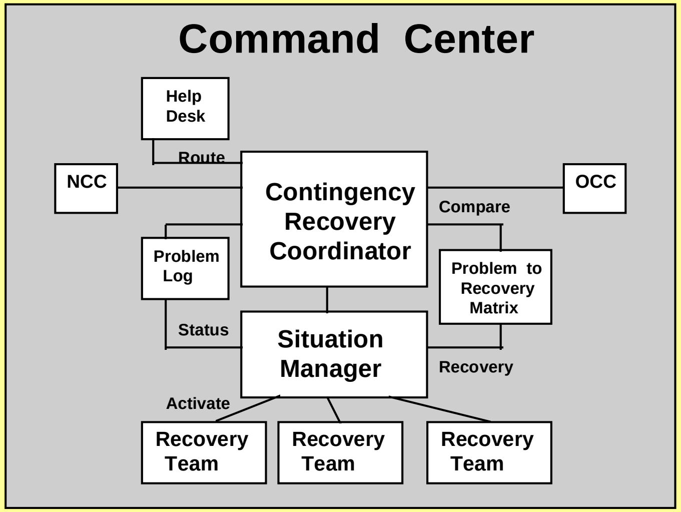
Operations Control Center (OCC)

Responsible for controlling and monitoring the mainframe operational environment and for responding to system demands. When problems arise, OCC personnel will take appropriate circumvention actions (if possible) and report the problem to the Help Desk.

Help Desk

Responsible for accepting problem related calls from all company locations, logging the problem event and interacting with callers to validate problem conditions. If possible, the Help Desk staff will try to resolve problem conditions with the caller - either directly, or by connecting the callers with company personnel responsible for the functional area related to the problem. When problems are considered potential crisis situations, then the Help Desk staff will route the problem to the Contingency Recovery Coordinator.

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.

Specific Recovery Techniques

Batch Recovery

Job Overrides
Proc Recovery Steps
Messages and Abend Codes

On-Line Recovery

Transaction Messages and Codes
Forward Recovery

Data Recovery

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

Communications Recovery

Problem Circumventions

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

Job Override

Proc Steps

Proc COND Steps for Recovery

Production Steps

Recovery Steps driven by COND statements on Production Steps.

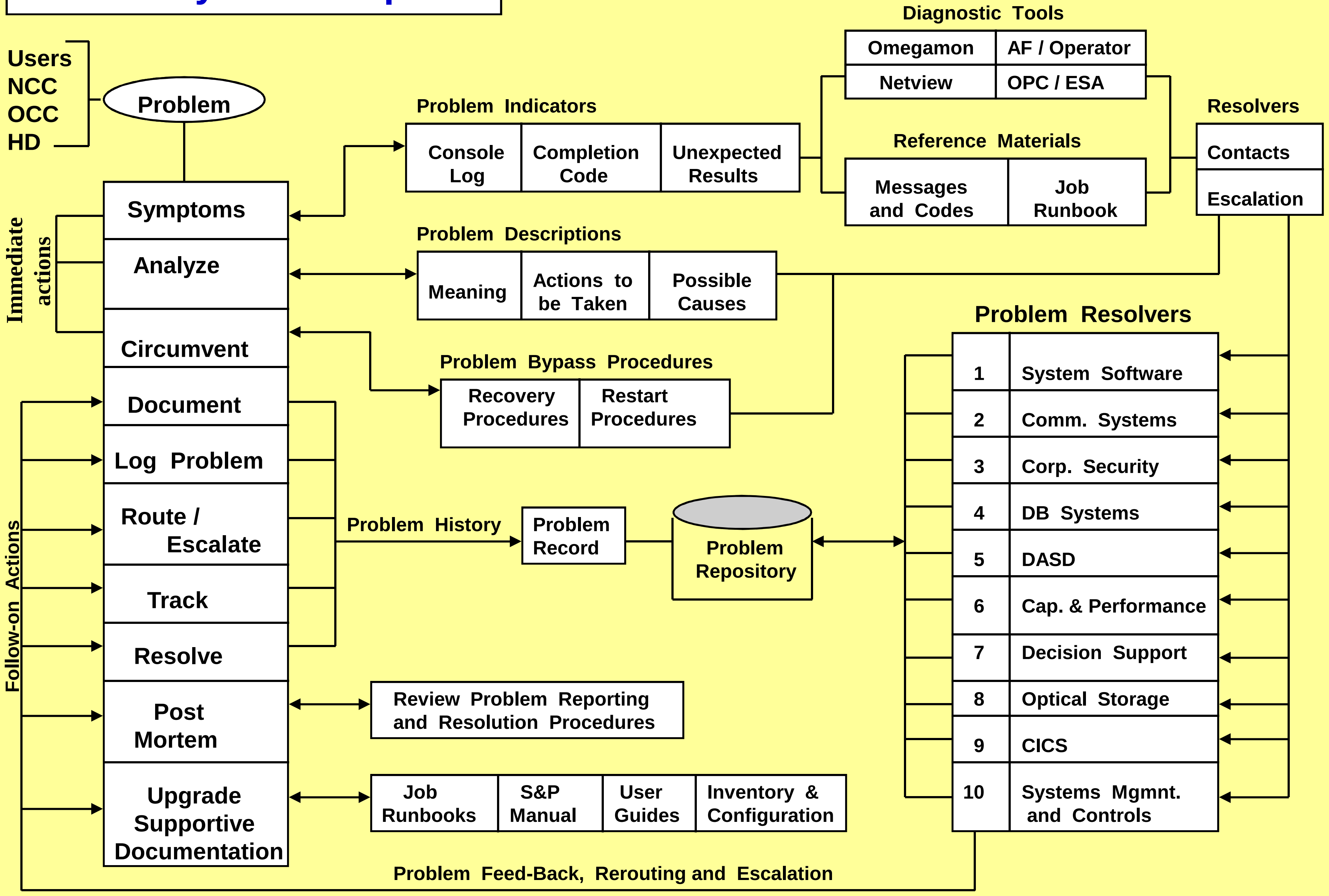
Messages and Codes

Meaning
Actions to take
Possible Causes

Job Runbook

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

Recovery Techniques



Users
NCC
OCC
HD

Problem

Immediate actions

Symptoms

Analyze

Circumvent

Follow-on Actions

Document

Log Problem

Route / Escalate

Track

Resolve

Post Mortem

Upgrade Supportive Documentation

Problem Indicators

- Console Log
- Completion Code
- Unexpected Results

Diagnostic Tools

Omegamon	AF / Operator
Netview	OPC / ESA

Reference Materials

- Messages and Codes
- Job Runbook

Resolvers

- Contacts
- Escalation

Problem Descriptions

- Meaning
- Actions to be Taken
- Possible Causes

Problem Bypass Procedures

- Recovery Procedures
- Restart Procedures

Problem History

Problem Record

Problem Repository

Problem Resolvers

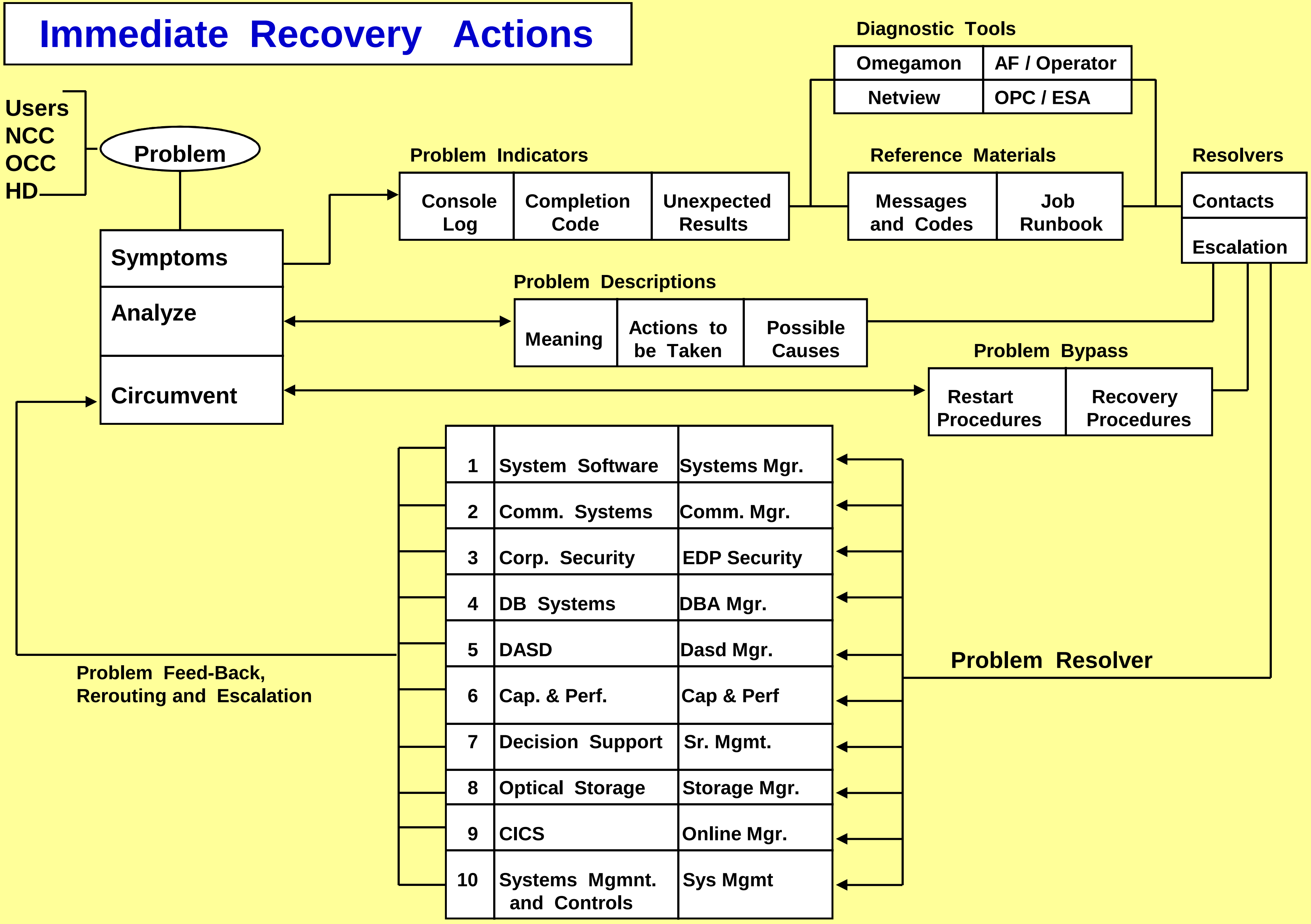
1	System Software
2	Comm. Systems
3	Corp. Security
4	DB Systems
5	DASD
6	Cap. & Performance
7	Decision Support
8	Optical Storage
9	CICS
10	Systems Mgmnt. and Controls

Review Problem Reporting and Resolution Procedures

- Job Runbooks
- S&P Manual
- User Guides
- Inventory & Configuration

Problem Feed-Back, Rerouting and Escalation

Immediate Recovery Actions



Users
NCC
OCC
HD

Problem

Symptoms

Analyze

Circumvent

Problem Indicators

Console Log

Completion Code

Unexpected Results

Diagnostic Tools

Omegamon	AF / Operator
Netview	OPC / ESA

Reference Materials

Messages and Codes

Job Runbook

Resolvers

Contacts

Escalation

Problem Descriptions

Meaning

Actions to be Taken

Possible Causes

Problem Bypass

Restart Procedures

Recovery Procedures

1	System Software	Systems Mgr.
2	Comm. Systems	Comm. Mgr.
3	Corp. Security	EDP Security
4	DB Systems	DBA Mgr.
5	DASD	Dasd Mgr.
6	Cap. & Perf.	Cap & Perf
7	Decision Support	Sr. Mgmt.
8	Optical Storage	Storage Mgr.
9	CICS	Online Mgr.
10	Systems Mgmnt. and Controls	Sys Mgmt

Problem Feed-Back,
Rerouting and Escalation

Problem Resolver

Immediate Recovery Actions continued...

When Problem Occurs:

The goal of Immediate Recovery Actions is to define the Problem and perform any recovery activities that allow a controlled restart of the failing component. If possible, an immediate bypass / circumvention of the failure should be performed, so that the impact of the problem will be limited. Trying to allow other systems to continue processing, without interruption, limits disruptions to the delivery of business services. A description of Immediate Recovery Actions follows.

Symptoms:

- **Define Problem Symptoms via Problem Indicators:**
  - Console Log Error Message,
  - Completion Code,
  - Describe Unexpected Results,
  - Condition of Jobs processing on system at time of failure and immediately afterwards.
- **Utilize Diagnostic Tools to Assist in Analyzing Problem Symptoms.**
  - Omegamon Status Displays,
  - Netview Status Displays,
  - OPC / ESA Error Messages,
  - AF / Operator Console Messages.
- **Refer to Reference Materials for Symptom Explanations,**
  - Messages and Codes Manuals,
  - Job Runbooks.

Immediate Recovery Actions continued...

Analyze:

- Analyze Problem Symptoms to Fully Define Problem:
  - Problem Category derived from symptoms (i.e., Wait, Loop, Abend, Message, incorrect, Results, or Performance),
  - Meaning of problem from Messages and Codes, or Job Runbook,
  - Actions to be taken when problem arises,
  - Possible Causes.

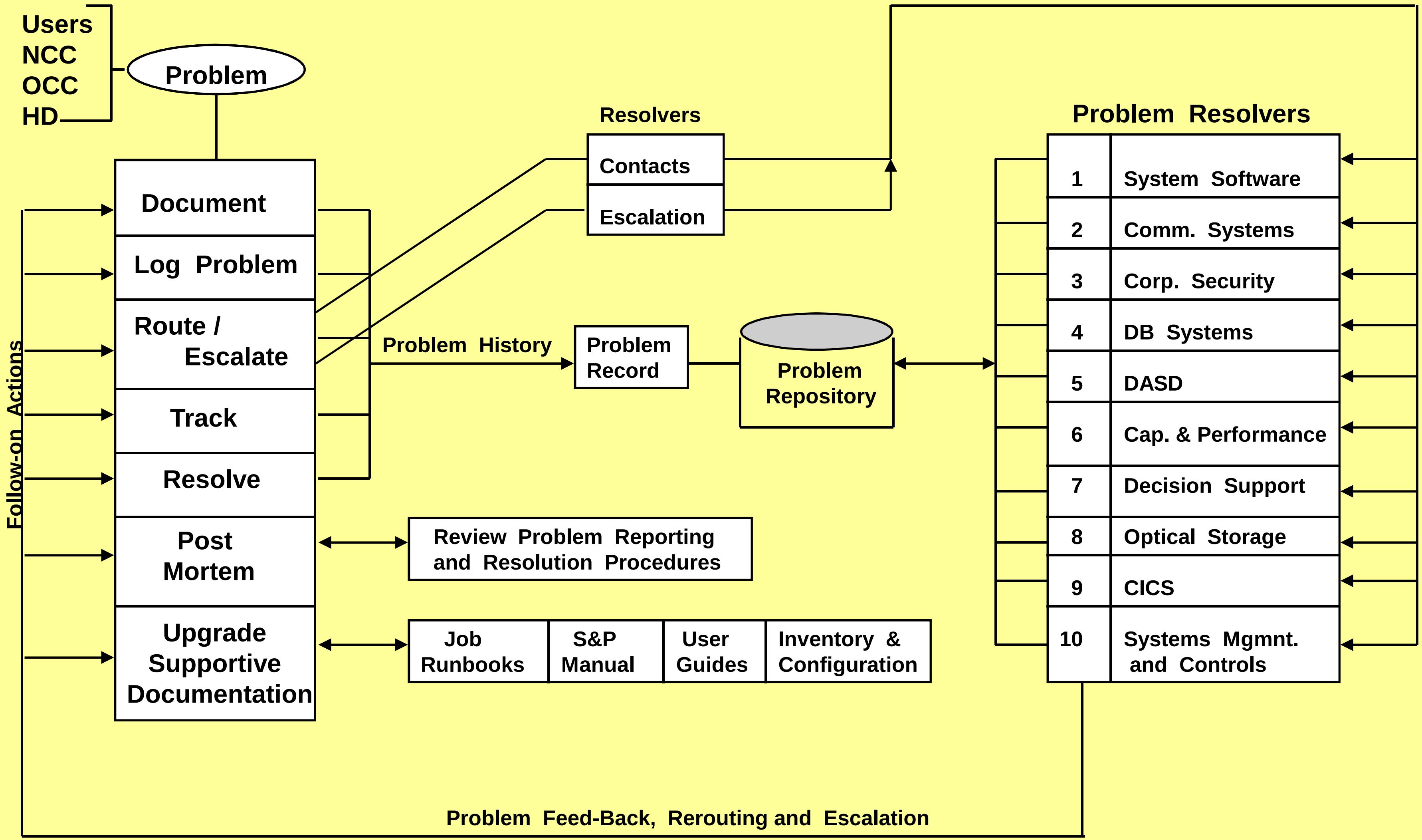
Circumvent:

- Circumvent / Bypass Problem with Recovery / Restart Procedures: if Available:
  - Recover to point just prior to problem,
  - Restart job at recovery point prior to failure.

Coordinate:

- Coordinate all Problem Related Activities with Problem Resolvers:
  - Communicate with Problem Resolver about system activities at time of problem event and immediately afterwards,
  - Notify Tech Ops. and Management of any unusual events that may be related to the problem, no matter how remote.
  - Make recommendations for improvement in problem diagnosis and recovery / restart procedures, whenever possible.

Follow-On Recovery Activities



Follow-On Recovery Activities continued...

After Immediate Problem Actions have been completed:

Document:

- Complete Problem Report, or call Help Desk and have them enter problem data,
- Obtain authorization to submit Problem Report, if necessary,
- Include Error Message and 24 Sense Bytes from Operator's Console,
- List major Jobs impacted by DASD Equipment Check,
- Provide description of Recovery / Restart process used to Circumvent / Bypass filing device,
- Submit time that Vendor Service Representative was notified about problem.

Log Problem:

- The HELP DESK creates a Problem Record for this incident,
- A unique Problem Number is assigned to this specific event.
- Problem is listed in Problem Report used as agenda for next problem meeting.
- Problem status is provided to next Operations shift during turnover.

Follow-On Recovery Activities continued...

Route / Escalate:

- All problems are entered as URGENT when initially assigned,
- Problem is routed to DASD Manager for review (who is Beeped via APRIORI),
- Problem is assigned to Vendor Service Representative for repair,
- Escalation is based on criticality of failing component, but usually:
  - 60 minutes after call is placed and Vendor Service Rep. has not arrived,
  - 60 minutes after Service Rep. has arrived and problem still exists,
  - 30 minutes, or less, when problem is connected to very critical component.

Track:

- Problem is initially entered by Help Desk, or Operator,
- Problem record is periodically updated to reflect additional problem information,
- Escalations are recorded in problem record,
- Problem status is constantly monitored and reported on during Problem Meetings and Turnover Meetings,
- Problem is Tracked until resolved,
- History record of problem is maintained.

Follow-On Recovery Activities continued...

After Immediate Problem Actions have been completed:

Resolve:

- Problem assigned to Resolver by Help Desk (Vendor Service Representative),
- Notification provided to in-house manager of component (i.e., DASD Manager),
- Resolver determines “Root Cause’ and devises problem resolution.
- Problem is repaired immediately, if possible,
- Change Control form is completed (emergency Change Notification System - ECNS is available if needed), if problem resolution requires extensive change,
- Help Desk is informed of problem resolution.

Post Mortem:

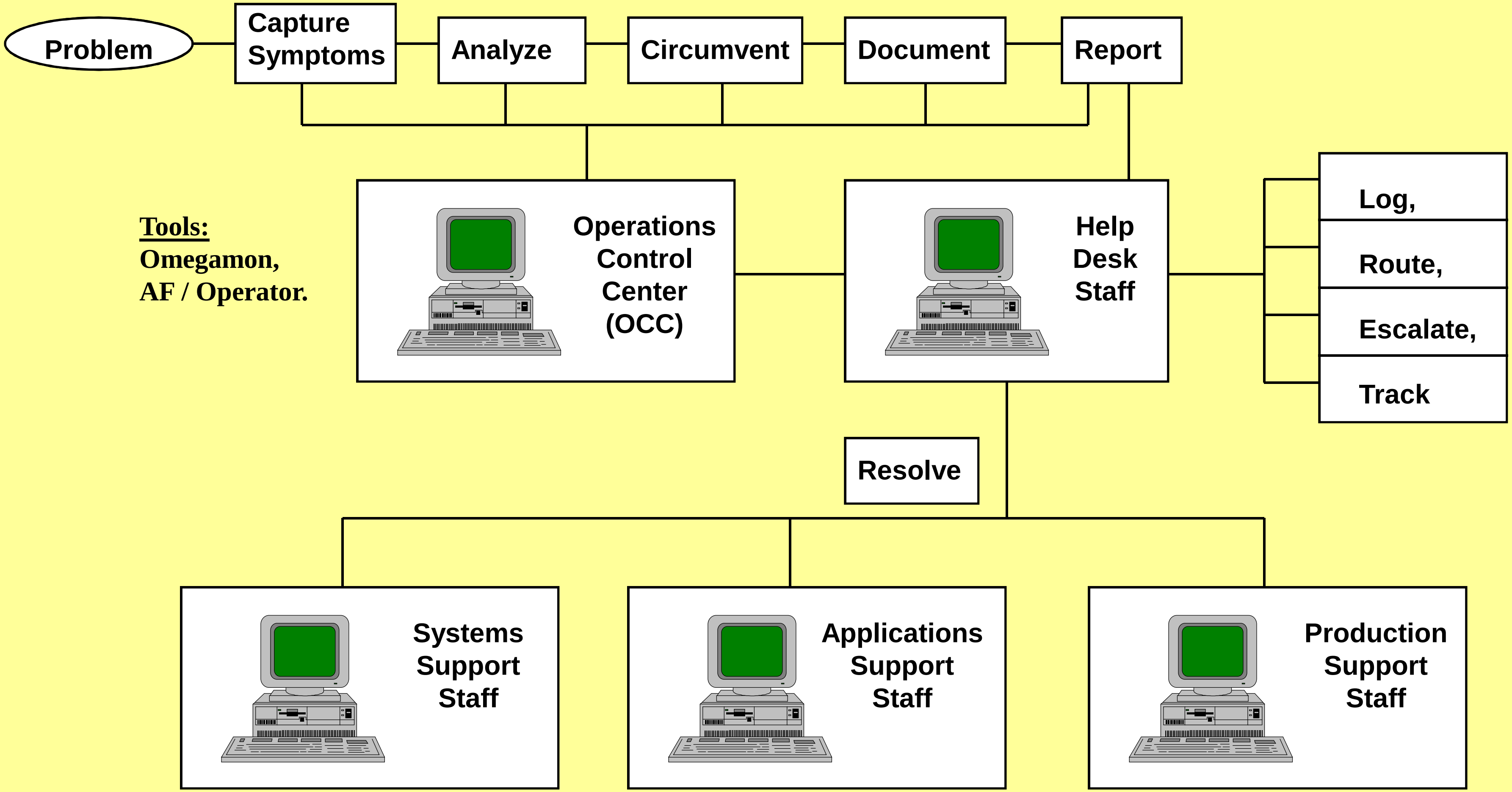
- After problem resolution has been applied,
- Problem History provided to meeting attendees,
- Discussion intended to Improve Problem Procedures associated with:
  - Problem Diagnosis,
  - Recovery / Restart procedures,
  - Supportive Tools.
- Goal is to reduce Problem Volume and Problem Life Cycle.

Follow-On Recovery Activities continued...

Upgrade Supportive Documentation:

- Post Mortem and Problem history reviewed,
- Quality of Supportive Documentation researched,
- Training of personnel associated with problem reporting and resolution examined,
- Quality and availability of existing documentation is appraised,
- Upgrade and / or purchase of documentation is determined,
- Training courses purchased / scheduled for personnel.

Batch Recovery Techniques



Problem

Capture Symptoms

Analyze

Circumvent

Document

Report

Tools:
Omegamon,
AF / Operator.

Operations Control Center (OCC)

Help Desk Staff

Log,

Route,

Escalate,

Track

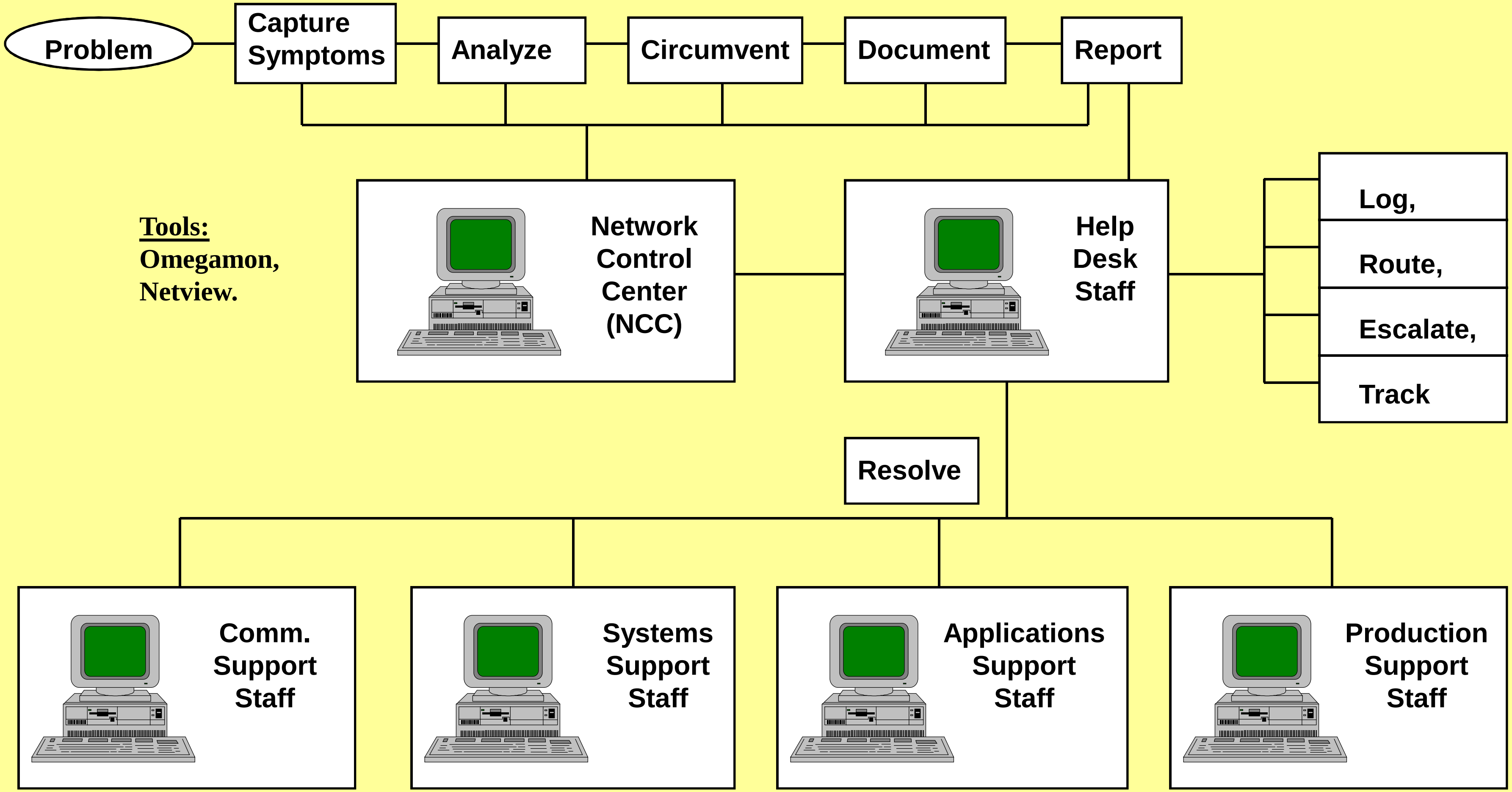
Resolve

Systems Support Staff

Applications Support Staff

Production Support Staff

On-Line Recovery Techniques



Problem

Capture Symptoms

Analyze

Circumvent

Document

Report

Tools:
Omegamon,
Netview.

Network Control Center (NCC)

Help Desk Staff

Log,

Route,

Escalate,

Track

Resolve

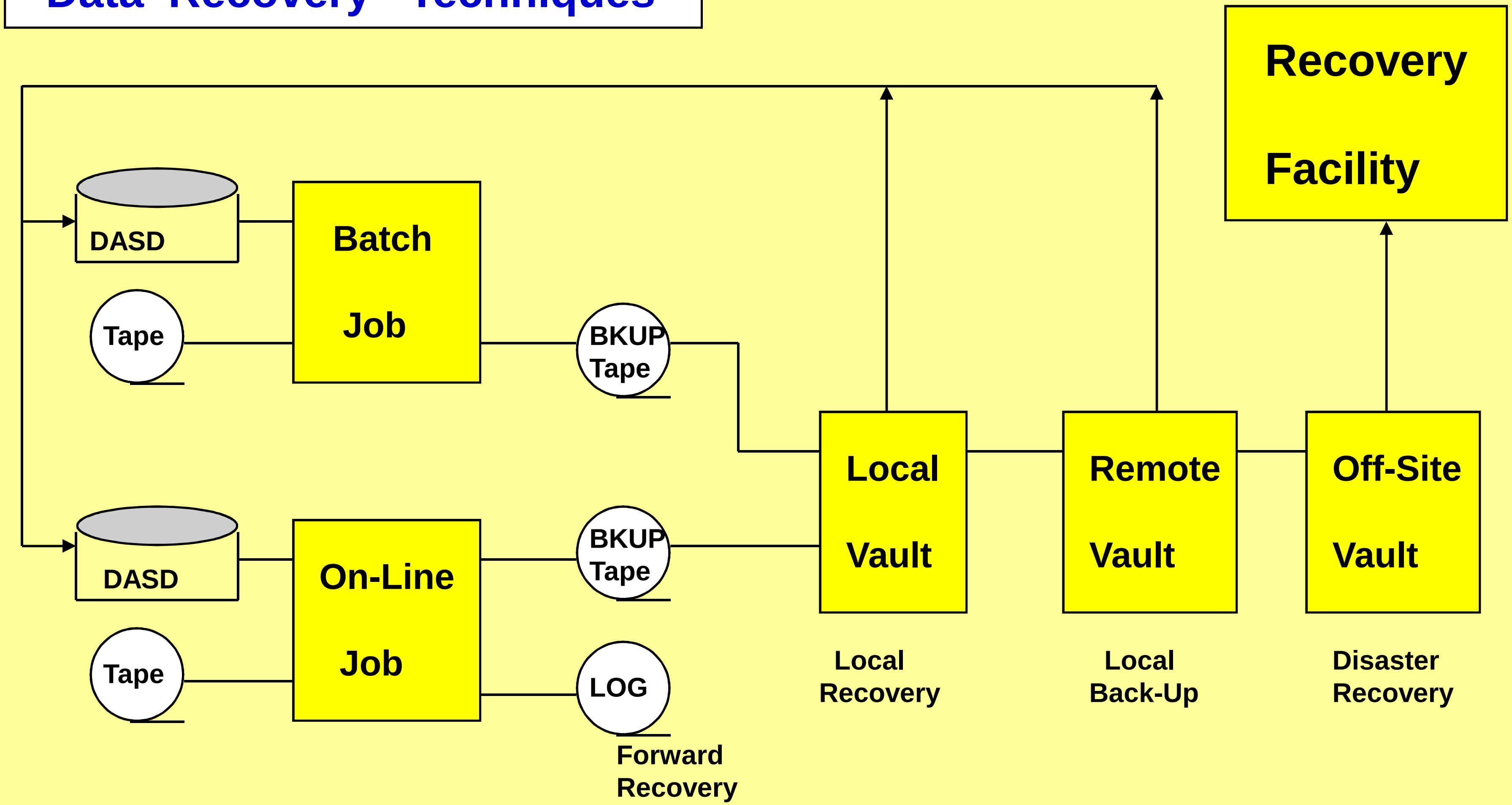
Comm. Support Staff

Systems Support Staff

Applications Support Staff

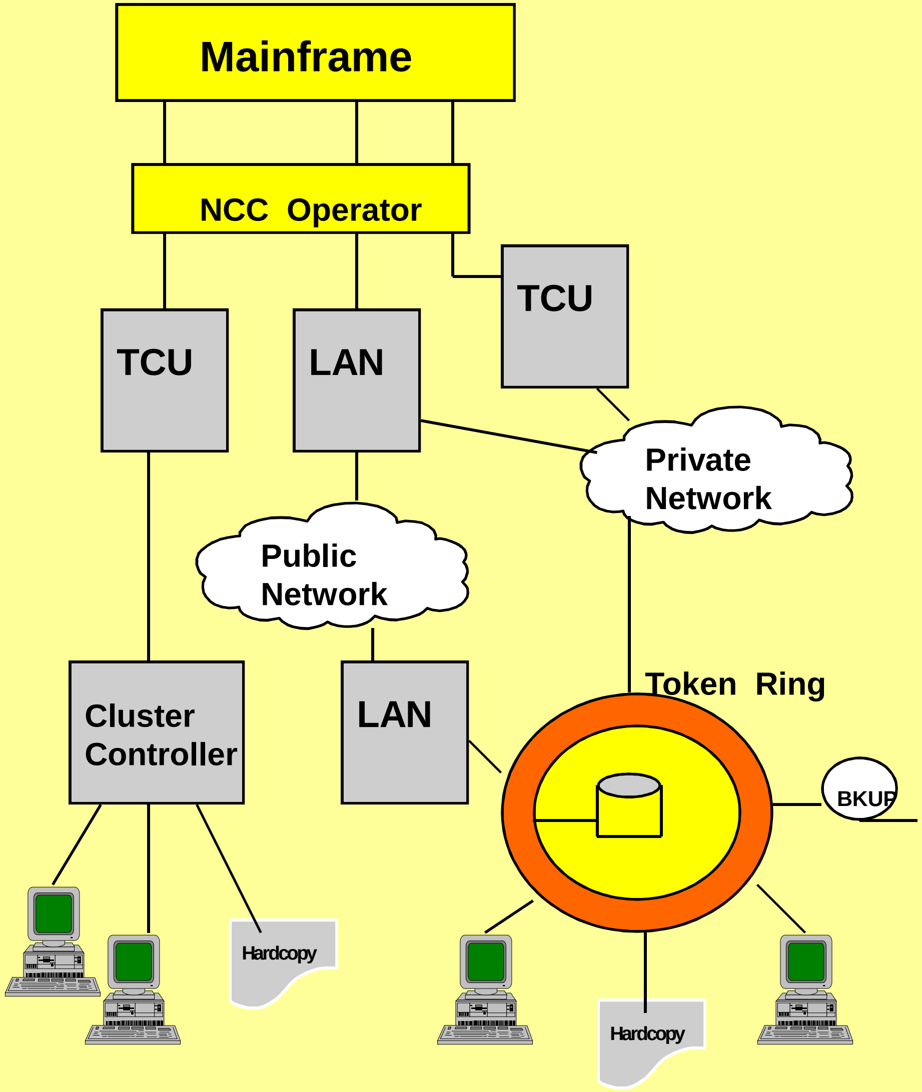
Production Support Staff

Data Recovery Techniques



Data Recovery, or Vital Records Management, is responsible for identifying critical data files and providing back-up / recovery procedures to safeguard against potential loss of information. Once identified, data files are copied to transportable media (i.e., Tape, or Cartridge). A copy of the media is stored in the Local Vault to restore data to failed devices (should an Equipment / Data Check occur). Secondary copies are stored at the Remote Vault (away from the data center) and Off-Site Vault (usually a Vendor Facility). Off-Site back-ups are utilized to support Disaster Recovery Operations.

Communications Recovery Techniques

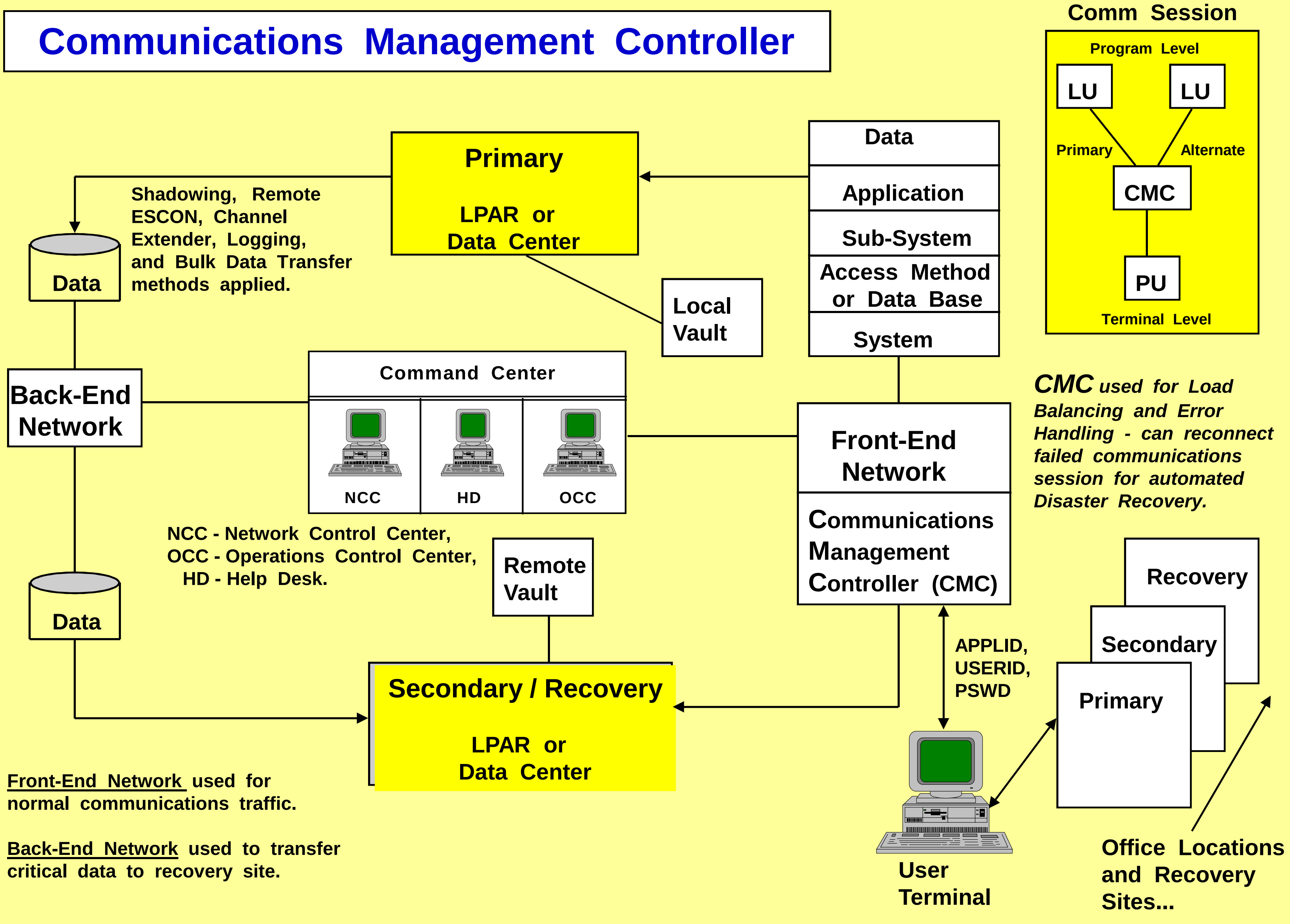


Communications Sessions are established between users connected on terminals (or PCs) and mainframe resident applications. These sessions are transmitted over communications lines and through Transmission Control Units (TCU's), or Local Area network (LANs). Data can be forwarded through Private Networks (i.e., owned by the company), or Public Network (i.e., the Internet, America On-Line, CompuServe, 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).

Communications Management Controller



Comm Session

Program Level

LU

LU

Primary

Alternate

CMC

PU

Terminal Level

CMC used for Load Balancing and Error Handling - can reconnect failed communications session for automated Disaster Recovery.

Primary

LPAR or Data Center

Data

Application

Sub-System

Access Method or Data Base

System

Shadowing, Remote ESCON, Channel Extender, Logging, and Bulk Data Transfer methods applied.

Data

Local Vault

Back-End Network

Command Center

NCC

HD

OCC

Front-End Network

Communications Management Controller (CMC)

NCC - Network Control Center,
OCC - Operations Control Center,
HD - Help Desk.

Remote Vault

Data

Secondary / Recovery

LPAR or Data Center

APPLID,
USERID,
PSWD

User Terminal

Recovery

Secondary

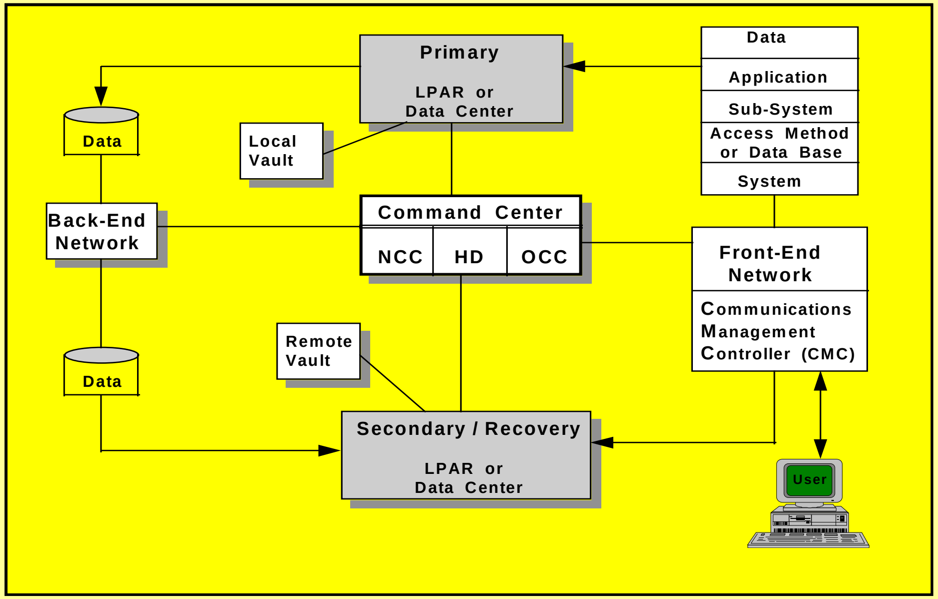
Primary

Office Locations and Recovery Sites...

Front-End Network used for normal communications traffic.

Back-End Network used to transfer critical data to recovery site.

CMC Operational Overview



Communications Management

The CMC is responsible for two things:

Load Balancing; and,
Error handling.

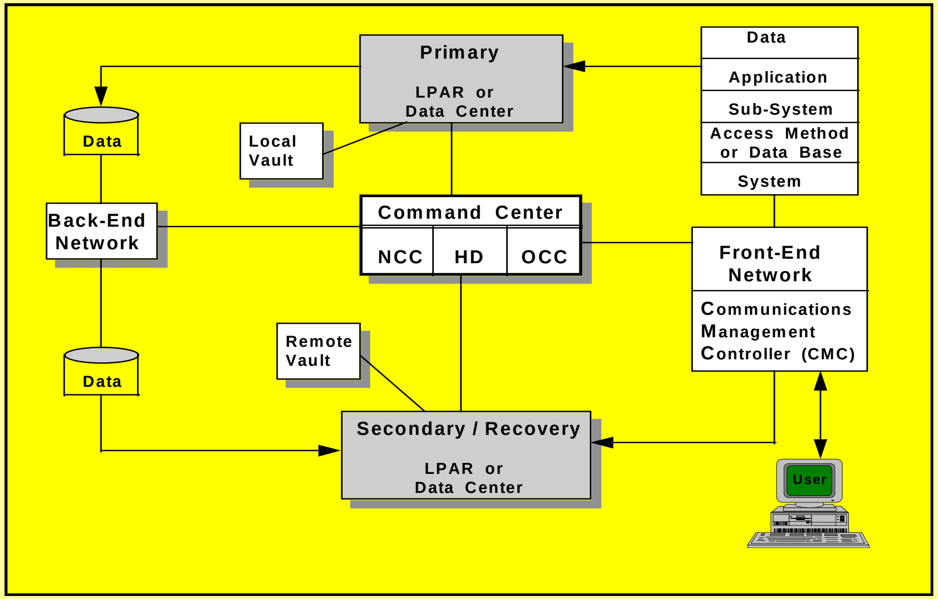
Load Balancing

When users log onto the system, they connect directly to the CMC and supply APPLID, USERID and PSWD information. The CMC then determines where the requested APPLID resides and the number of existing users already connected to the APPLID (Application). If the APPLID resides in multiple locations, the CMC will connect the requesting user to the location with the fewest existing users. This Load Balancing property of the CMC helps distribute business resources evenly across the business community.

Error Handling

Whenever an error condition occurs, the CMC can respond to the outage through predefined recovery operations contained within a library of named operations. These recoveries can re-establish connections, switch devices, and move users from an application residing on one machine to another machine - even if the machine is in a different physical location. Through the error handling features of a CMC it is possible to automate recovery operations, either within the data processing primary location (from one LPAR to an LPAR on a different machine), or with the recovery facility. The largest concern needed to be addressed when planning CMC recovery operation, is the synchronization of data between the primary, secondary and recovery locations.

CMC Data Concerns



Front-End Network

Responsible for supplying communication services to the general user community. The CMC monitors this environment and can perform problem circumvention and recovery operations for encountered problems.

Back-End Network

Responsible for maintaining data synchronization between the primary location and the recovery site. Because of the large amount of data needed to support recovery operations, it is more efficient to utilize a Back-End Network so that the performance and response times associated with supporting the general user community are not affected.

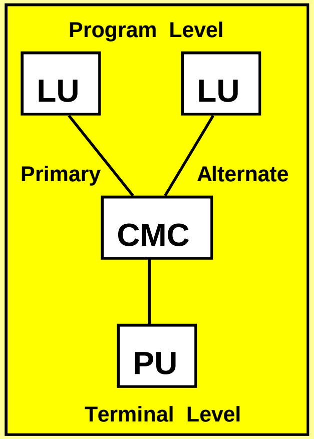
Local Vault

When data files are backed up they are transferred to transportable media. To provide recovery for data residing on damaged equipment, a copy of the data is stored in the Local Tape Library, which is classified as the Local Vault. Should a devise be damaged and its data destroyed, the information can be restored via back-up media maintained within the Local Vault.

Remote Vault

Similar to the Local Vault, but kept at a secondary, or Recovery, locations. Remote Vault media is used to recover information when the Local Vault is not accessible, or when the Primary or Secondary sites have experienced a disaster event.

CMC Managing Communications Sessions



Connecting Users to Applications

Initially, users log onto systems by providing the APPLID of the application they want to be connected to. Additionally, the User's USERID and PSWD are provided for validating authorization to be connected to the application. After validating the users authority and determining the best location to connect the requesting user to, the CMC establishes a communication session between the end user and the application. This connection is depicted as a Logical Unit (LU) for the application program and a Physical Unit (PU) for the user's terminal. In SNA terms, it is considered to be a BOUND Communication Session.

Reconnecting Users when Disasters Occur

Should the communication session between the user and application be broken, because the application resident mainframe is lost due to a disaster, it is possible for the CMC to re-establish the session by Re-BINDING the user to the LU associated with the secondary / recovery application. This reconnection can be accomplished without operator intervention and can result in automated reconnections that are transparent to the end user.

Recommended Direction

It is recommended that the implementation of a CMC be considered. Although requiring more effort initially, the rewards that can be received through CMC Load Balancing and Recovery operations far exceed the efforts associated with its implementation.

Problem Sample

1. DASD Equipment Check.

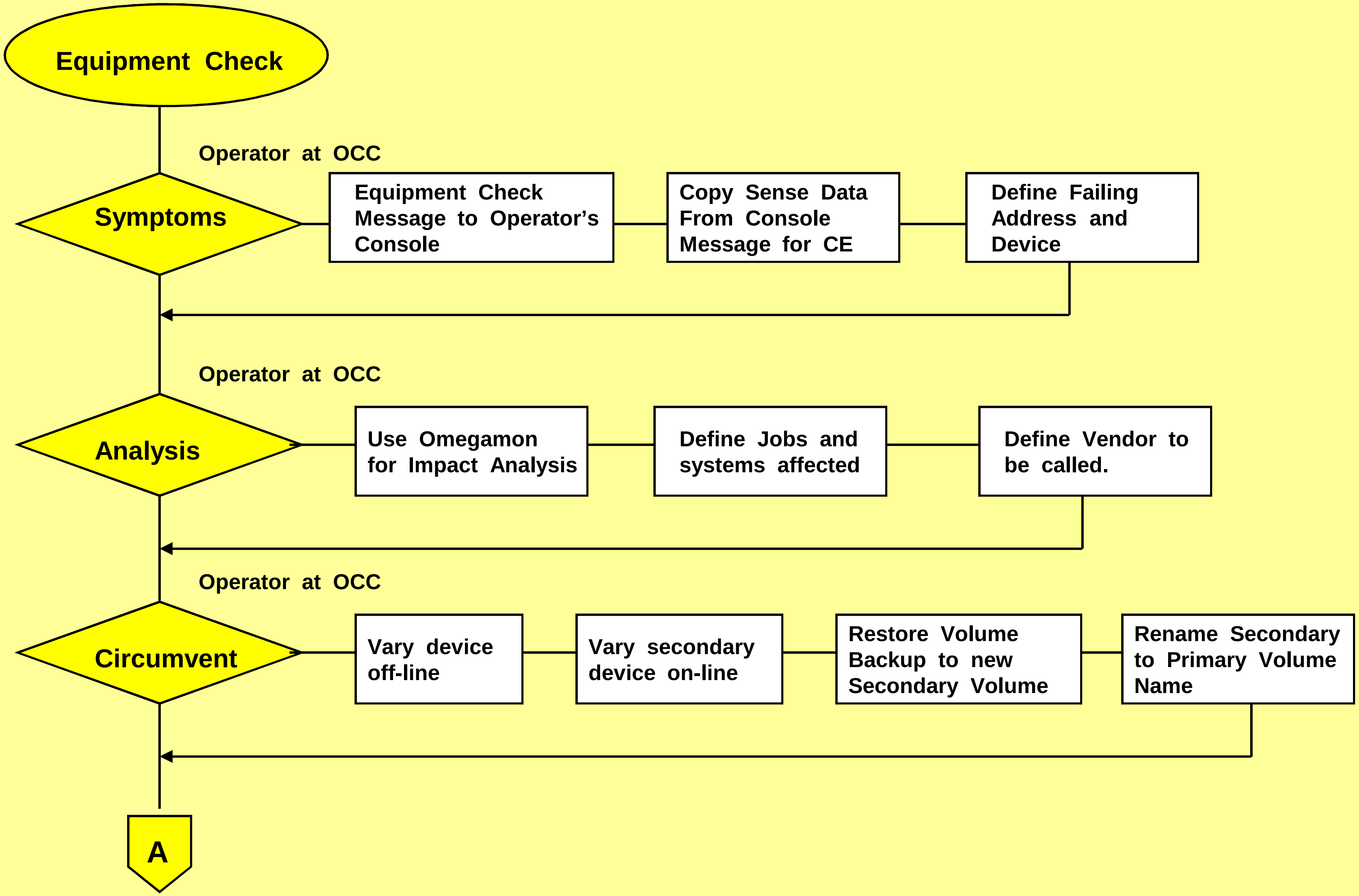
This example is in the format of the Problem Matrix and provides an overview of the information contained in that manual.

1. DASD Equipment Check.

Specific Problem Index Page

Device Problem - DASD Equipment Check.

1.1 DASD Equipment Check - Problem Resolution Flow Chart.



Equipment Check

Operator at OCC

Symptoms

Equipment Check Message to Operator's Console

Copy Sense Data From Console Message for CE

Define Failing Address and Device

Operator at OCC

Analysis

Use Omegamon for Impact Analysis

Define Jobs and systems affected

Define Vendor to be called.

Operator at OCC

Circumvent

Vary device off-line

Vary secondary device on-line

Restore Volume Backup to new Secondary Volume

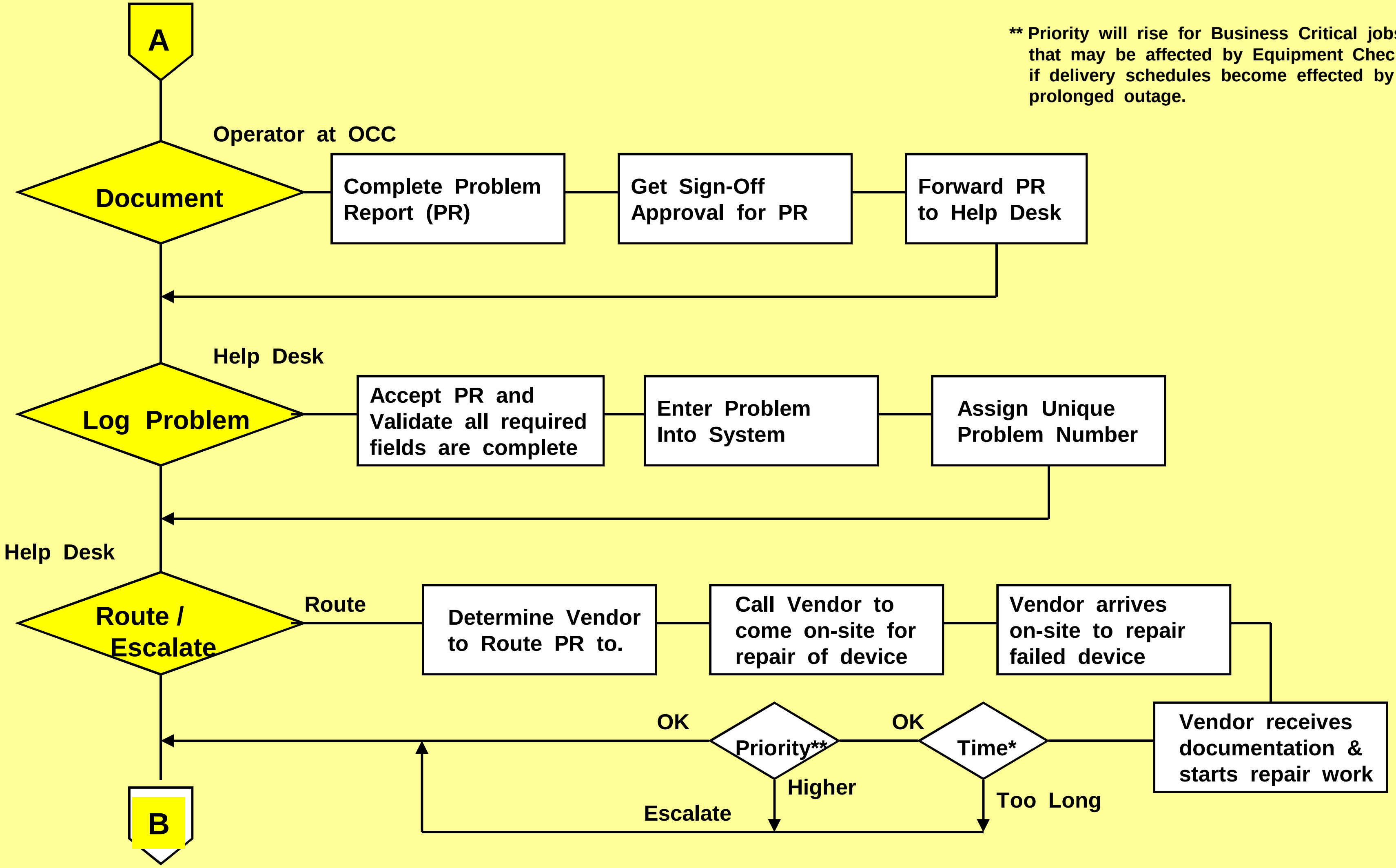
Rename Secondary to Primary Volume Name

1.1 Problem Resolution Flow Chart continued...

Legend:

* Escalation Time for Critical Components is if vendor does not arrive within 60 minutes of original call, or is problem is not repaired within 60 minutes of CE's arrival.

** Priority will rise for Business Critical jobs that may be affected by Equipment Check, or if delivery schedules become effected by a prolonged outage.



A

Operator at OCC

Document

Complete Problem Report (PR)

Get Sign-Off Approval for PR

Forward PR to Help Desk

Help Desk

Log Problem

Accept PR and Validate all required fields are complete

Enter Problem Into System

Assign Unique Problem Number

Help Desk

Route / Escalate

Route

Determine Vendor to Route PR to.

Call Vendor to come on-site for repair of device

Vendor arrives on-site to repair failed device

Vendor receives documentation & starts repair work

Time*

OK

Too Long

Priority**

OK

Higher

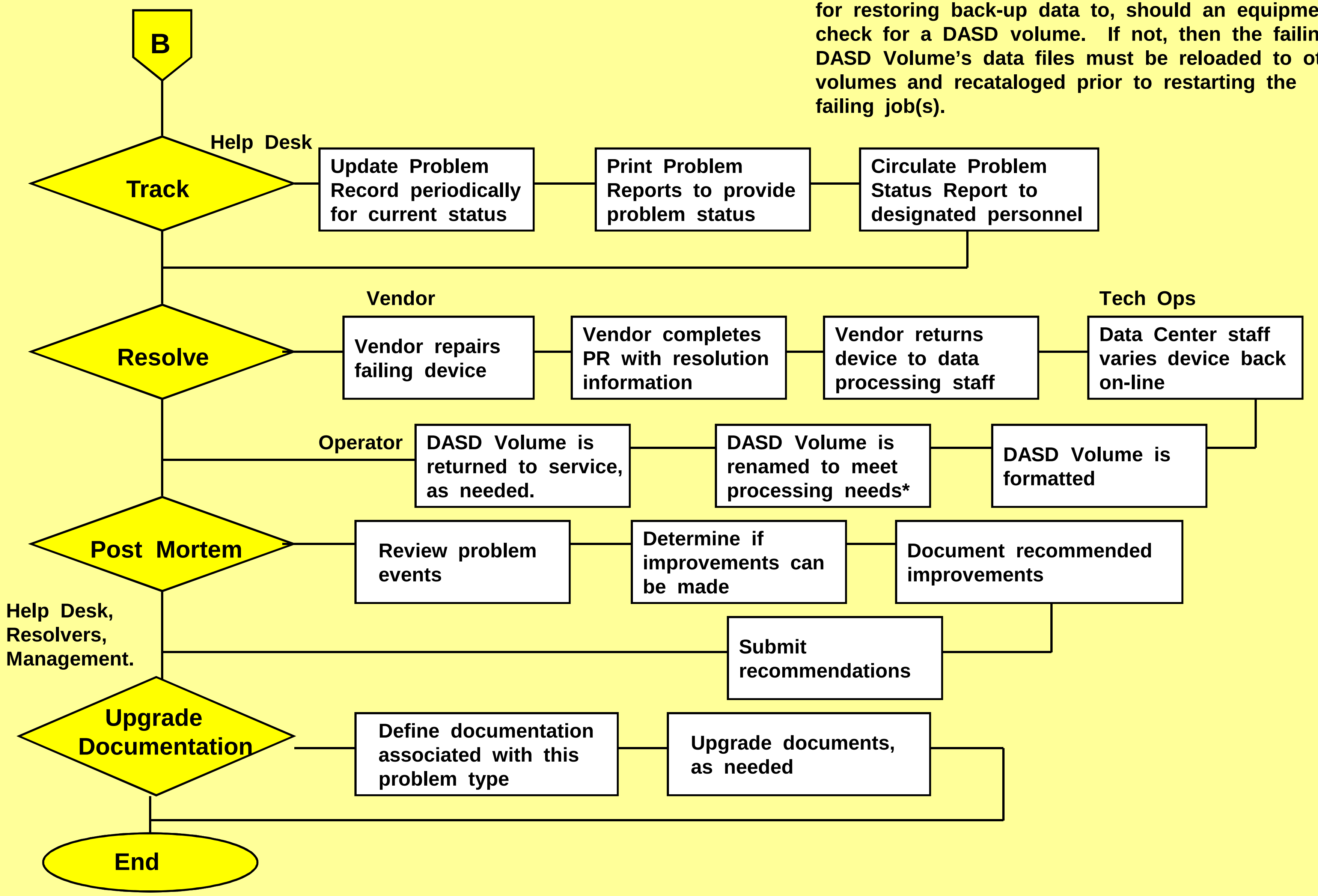
Escalate

B

1.1 Problem Resolution Flow Chart continued...

Legend:

* Ideally, a spare DASD volume should be available for restoring back-up data to, should an equipment check for a DASD volume. If not, then the failing DASD Volume's data files must be reloaded to other volumes and recataloged prior to restarting the failing job(s).



B

Help Desk

Track

Update Problem Record periodically for current status

Print Problem Reports to provide problem status

Circulate Problem Status Report to designated personnel

Vendor

Resolve

Vendor repairs failing device

Vendor completes PR with resolution information

Vendor returns device to data processing staff

Tech Ops

Data Center staff varies device back on-line

Operator

DASD Volume is returned to service, as needed.

DASD Volume is renamed to meet processing needs*

DASD Volume is formatted

Post Mortem

Review problem events

Determine if improvements can be made

Document recommended improvements

Help Desk, Resolvers, Management.

Submit recommendations

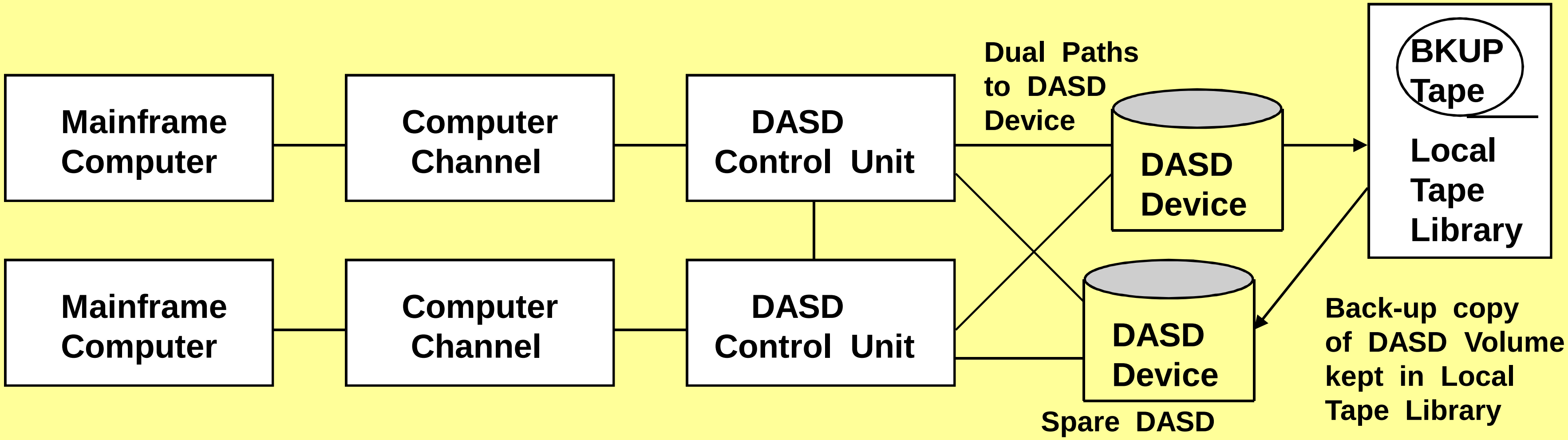
Upgrade Documentation

Define documentation associated with this problem type

Upgrade documents, as needed

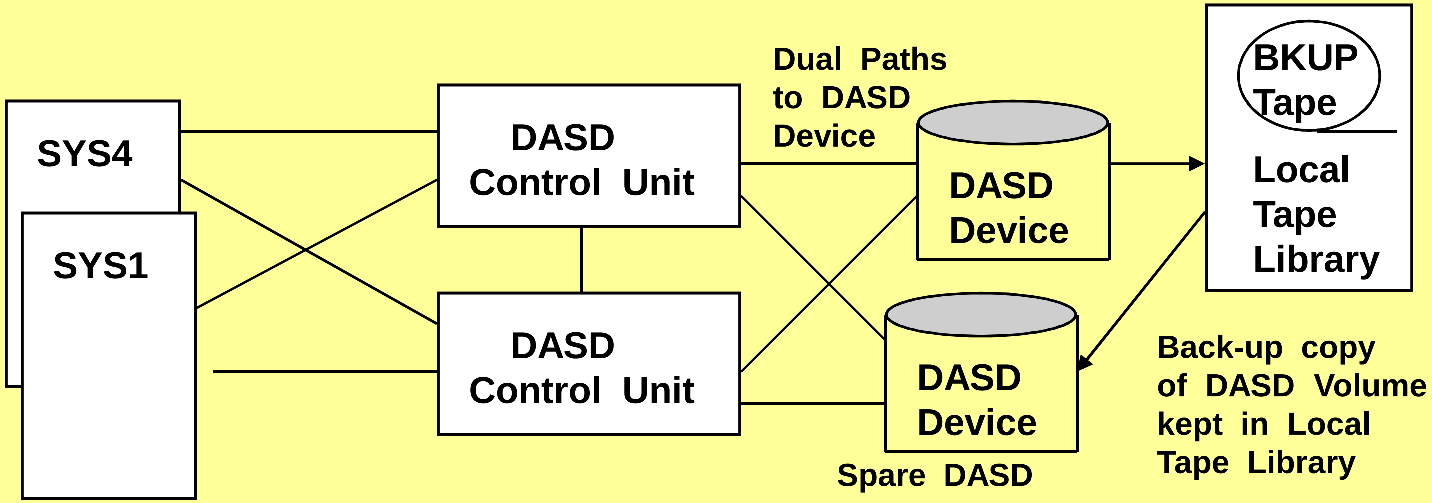
End

1.2 Problem Description - DASD Device Equipment Check



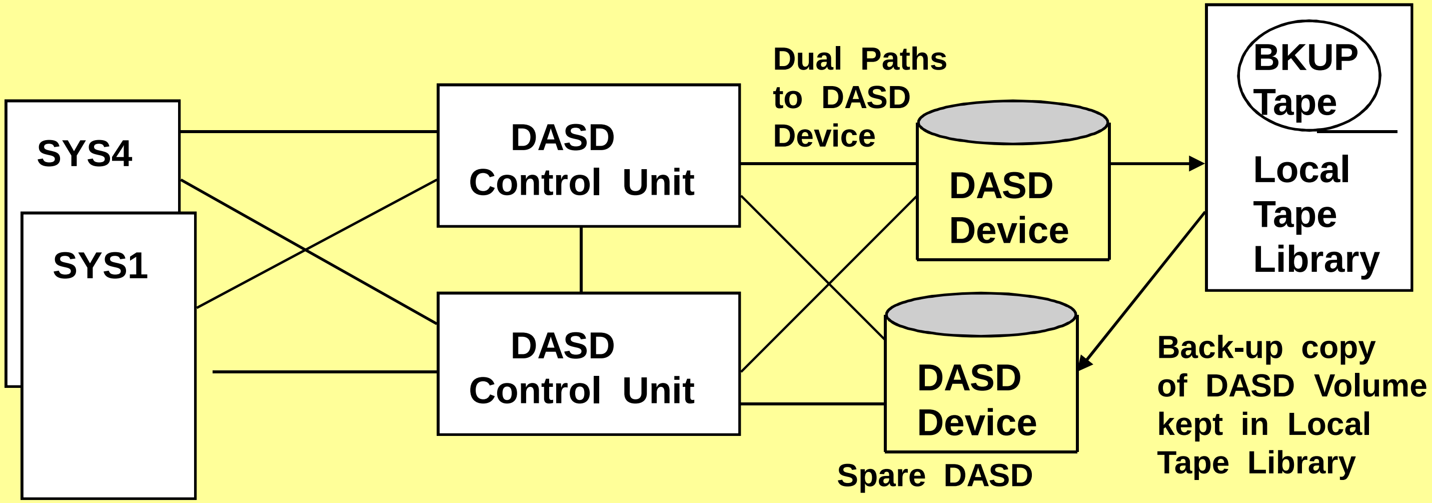
- Equipment Checks are caused by mechanical or electronic device failures.
- Only Vendor Service Representative can repair failing component.
- All DASD Devices are shared in the data processing environment.
- Many systems and users can be effected by DASD Equipment Check.
- Some DASD Volumes are more sensitive than others because of their contents and usage (i.e., JES2 Checkpoints, Catalogs, Critical Business Data, etc.) .
- Spare DASD Volumes are essential to recover from DASD Equipment Checks.
- Circumvention's / Bypass’ must be available for DASD devices, especially those DASD Devices housing most critical business data and highly used data sets.
- DASD Back-Up’s are stored in Local Tape Library.
- Usually, weekly full-volume back-up with daily incremental back-ups.
- Requires restoring full-volume and then incrementals.

4.3 Problem Symptoms - DASD Device Equipment Check



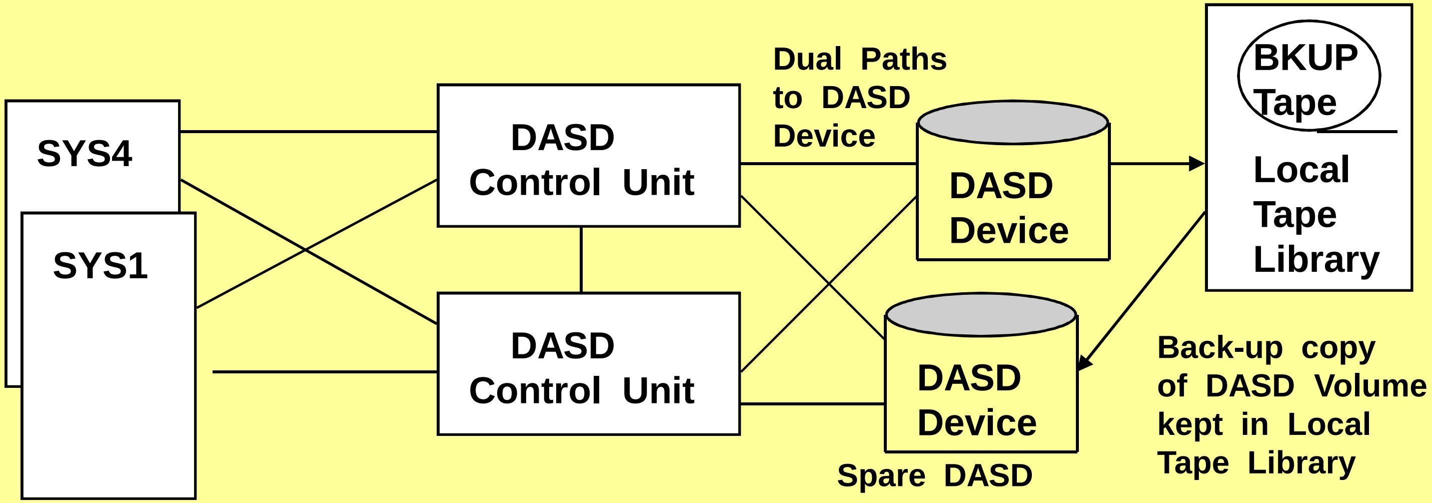
- Error message on Operator’s Console.
- 24 bytes of Sense Information used to describe problem.
- Omegamon display will pinpoint filing device and Jobs enqueued on resource.
- Processing Jobs start entering Wait State on failing device.
- Operator notices that Jobs are not processing normally.
- Operator copies Error Message and Omegamon information onto Problem Report.
- Operator notifies Supervisor, Help Desk and DASD Manager.
- Vendor’s Service Representative is notified.

4.4 Actions to be Taken - DASD Device Equipment Check



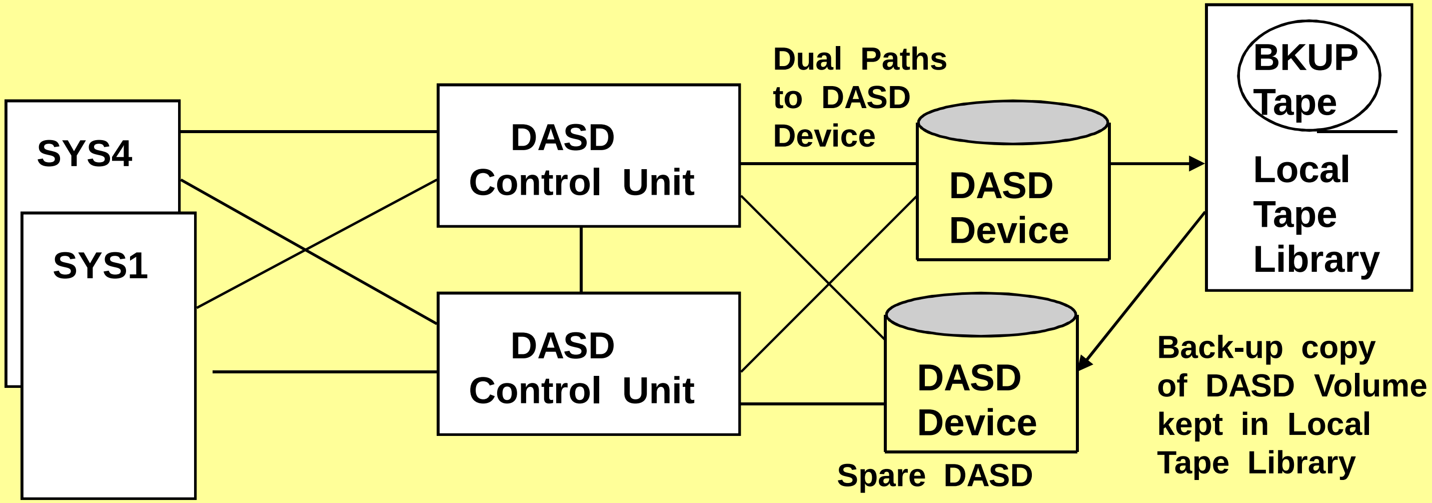
- Refer to Messages and Codes Manual for problem description.
- Record Console Message and Omegamon information on Problem Report.
- Notify Local Tape Library to pull Back-Up tape for failing DASD Volume.
- Vary failing device off-line.
- Notify DASD Manager of failure.
- Notify Help Desk of Failure.
- Locate spare DASD Volume to replace failing device.
- Prepare to restore Back-Up tape / cartridge to Spare DASD Volume.
- Coordinate restore operations with DASD Manager.
- Notify Vendor Service Representative of failure.

4.5 Circumvention / Bypass - DASD Device Equipment Check



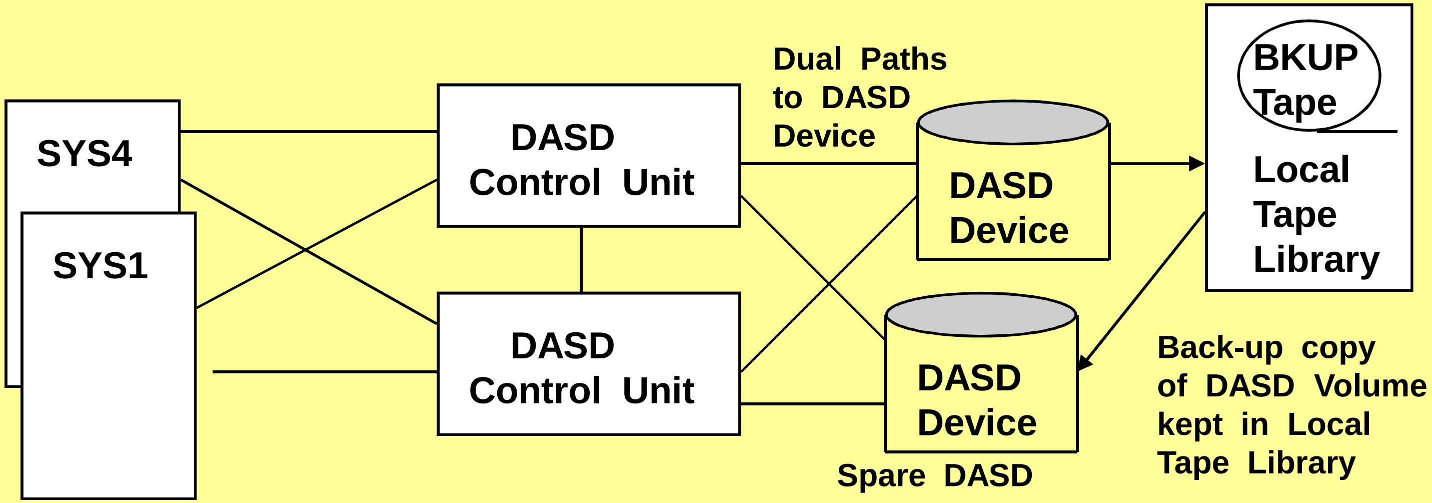
- Locate Spare DASD Volume that is accessible from same systems that failing device communicates with.
- Obtain Back-Up Tape / Cartridge from Local Tape Library.
- Notify DASD Manager.
- Prepare to copy Back-up Tape / Cartridge to Spare DASD Volume.
- Vary failing device off-line.
- Copy Back-Up Tape / Cartridge to Spare DASD Volume.
- Vary Spare DASD Volume on-line (its VOLSER must be the same as failing device).
- Jobs waiting on device will either start processing again, or continue in Wait State.
- Restart Jobs in Wait State.
- Document events in Problem Report.
- Notify Help Desk and provide them with Problem Report.
- Monitor Vendor Service Representative actions and escalate if necessary.

4.6 Probable Causes - DASD Device Equipment Check



- Vendor device failure.

4.7 Personnel to Notify - DASD Device Equipment Check



- Operations Shift Manager / Supervisor.
- DASD Manager.
- Vendor Service Representative.
- Help Desk.
- Tape Librarian.
- Tech Ops.
- Systems Support.

Return to DCAG Home Page