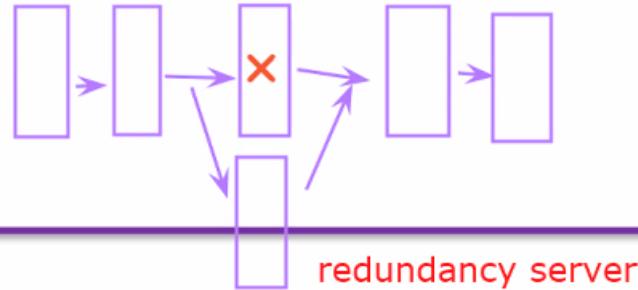Issue -> Incident

Incident

redundancy server

- Any <u>unplanned</u> event that causes or may cause disruption to <u>normal</u> service operations

- An <u>unplanned</u> interruption to an IT Service or a reduction in the Quality of an IT Service.

Stability = Availability + Performance
or Quality   (uptime)   (running at optimal experience)

example: 60m x 24h x 30d =43200m | downtime=30m | (43200-30)/43200 = 99.93% availability

- **Incident Management** is the process for dealing with all incidents; this includes failures, questions or queries reported by users, by technical staff, or automatically detected and reported by event monitoring tools

command center

Incident Management - Objective

Restore normal service operation as quickly as possible and minimize the adverse impact on business operations thus ensuring that the best possible levels of service quality and availability are maintained
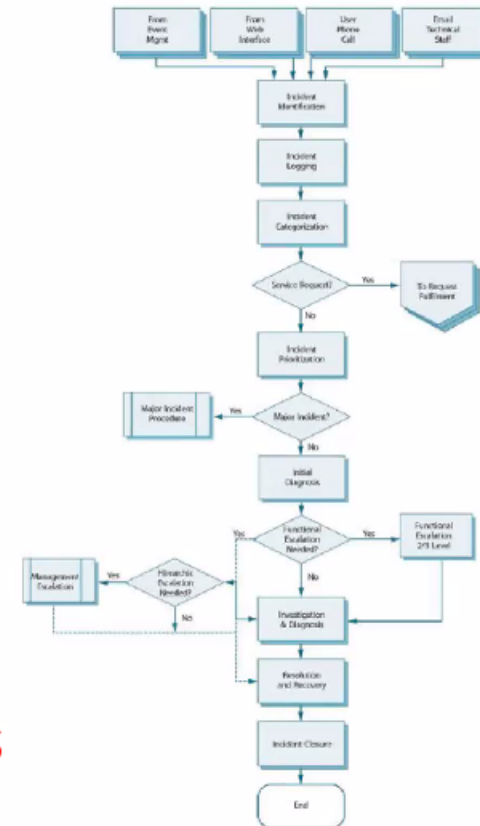
Incident Management Model

The Incident Management Model should include:

- The steps that should be taken to handle the incident

- The chronological order these steps should be taken in, with any dependencies or co-processing defined

- Responsibilities; who should do what

- Timescales and thresholds for completion of actions

- Escalation procedures; who should be contacted and when

Incident Management – Activities

- *Identification*

- *Logging*

- *Categorization*

- *Prioritization*

- Initial diagnosis

- Escalation

- Investigation and diagnosis

- Resolution and recovery

44

Incident Management – Activities
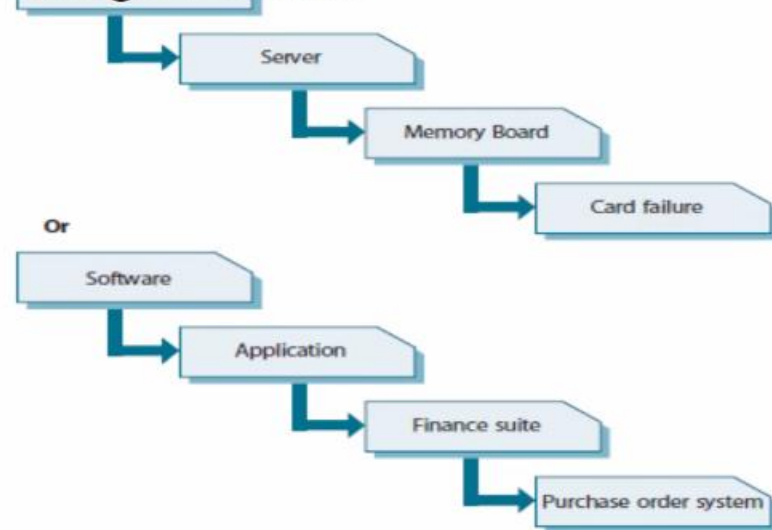
Incident Categorization

Figure 4.3 Multi-level incident categorization

Incident Prioritization

Table 4.1 Simple priority coding system

		Impact			
		High	Medium	Low	
	High	1	2	3	
Urgency	Medium	2	3	4	
	Low	3	4	5	

Priority code	Description	Target resolution time
1	Critical	1 hour
2	High	8 hours
3	Medium	24 hours
4	Low	48 hours
5	Planning	Planned

45

Incident Mgt – Key Performance Indicators

- Total number of incidents (as a control measure)

- Breakdown of incidents at each stage

- Size of current incident backlog

- Number and percentage of major incidents

- Mean elapsed time to achieve incident resolution or circumvention, broken down by impact code

Incident Mgt – Roles

- Incident Manager supervisory level

- First-line Support   L1   Contact center

- Second-line Support   L2   Technical resources - DBA / Sys Ad / Net Ad / App Support (debug) [General IT Knowledge]

- Third-line Support (Technical Management, IT Operations, Applications Management, Third-party suppliers)   L3   Masters / Experts / Consultants   -specialized knowledge / expertise for DBA / Sysad / Netad / AppSupport

Incident Mgt – Challenges

- Ability to detect incidents as quickly as possible (dependency on Event Management)

- Ensuring all incidents are logged

- Ensuring previous history is available (Incidents, Problems, Known Errors, Changes)

- Integration with Configuration Management System, Service Level Management, and Known Error Database (CMS, SLM, KEDB)

49

Request Fulfillment

- The term "**Service Request**" is used as a generic description for many varying types of demands that are placed upon the IT Department by the users

- Many of these are actually small changes - low risk, frequently occurring, low cost, etc.

Request Fulfillment –Basic Concepts

- Service Request

  – A request from a user for information or advice or for a Standard Change

- Request Model (similar to incident model)

- Self-help