1. Service Design – Service Continuity Management

Dr. Franklin Leung

Many financial companies lost their data centres in 9/11.

You may anticipate the disaster, but the disaster doesn't happen in the way you expect.

Not well prepared for a disaster, a company may go bankrupt.

IT Service Continuity Management(ITSCM)

Definition

- ITSCM is the process responsible for the technology element of Business Continuity Management. It assesses & manages risks to IT services by examining CI values, threats & vulnerabilities弱点, developing appropriate countermeasures, creating an IT Service Continuity Plan & Managing any disaster situations that occur.

ITSCM

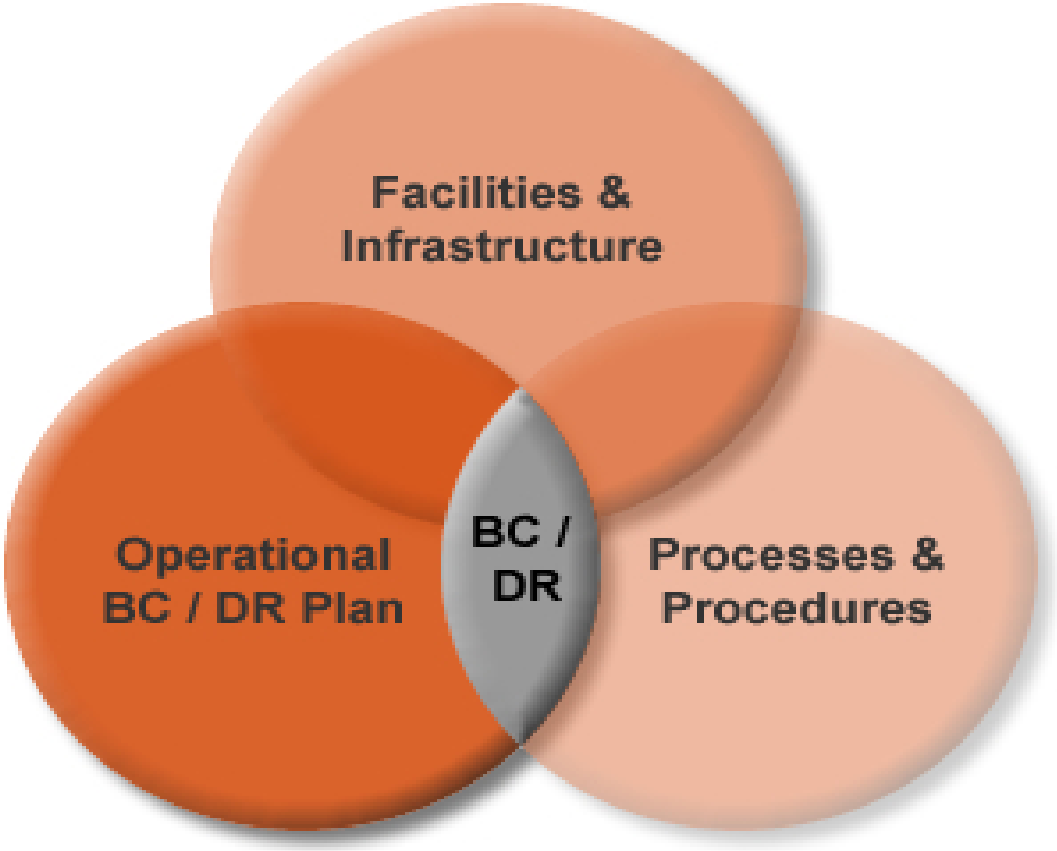
Goal

- To support the overall Business Continuity Management process by ensuring that the required IT technical & services facilities (including computer systems, networks, applications, telecommunications, technical support & service desk) can be recovered within required and agreed business timescales.

ITSCM versus BCM

- ITSCM (or Disaster Recovery Management) is focused on the continuity of IT Services for the business. BCM (Business Continuity Management) is concerned with the management of Business Continuity that incorporates all services upon which the business depends, one of which is IT.

Business Continuity /Disaster Recovery



Key ITSCM processes

- **Stage 1 : Initiation**
- **Stage 2: Requirements & Strategy**
- **Stage 3: Implementation**
- **Stage 4: Operational Management**

1.1 ITSCM Stage 1 Initiation

- A well planned project initiation enables ITSCM work to proceed with the necessary sponsorship, buy-in & awareness, with all contributing members of the organisation aware of their responsibilities & commitment.

ITSCM Stage 1 Initiation

- The initiation process covers the whole of the organisation & consists of the following 5 activities
  - Policy setting
  - Specify Terms of Reference (TOR) & scope
  - Allocate resources
  - Define the project organisation & control structure
  - Agree project & quality plans

1.2 ITSCM Stage 2 Requirements & Strategy

- Business Impact Analysis (quantify the impact loss of IT service)
- Risk Assessment (risk identification and risk assessment to identify potential threats to continuity)
- Business Continuity strategy

ITSCM Stage 2 Requirements & Strategy (Cont'd)

- Options need to be considered
  - People & communication
  - IT systems, network & processes
  - Critical services such as power, water, post etc.
  - Critical assets such as records, reference material

ITSCM Stage 2 Requirements & Strategy

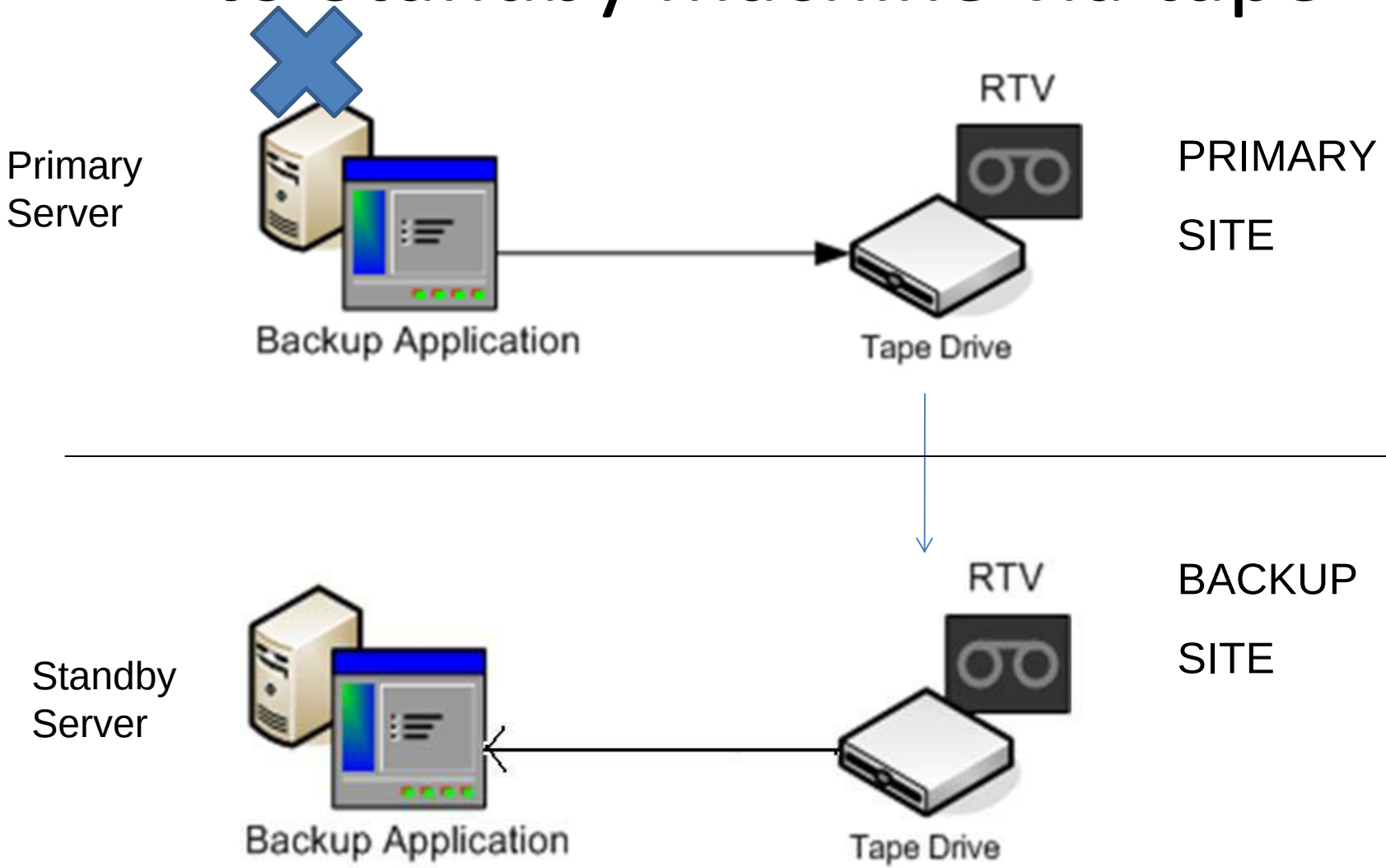
- Specific IT recovery options
  - Do nothing
  - Manual work-arounds
  - Reciprocal互惠arragements
  - Graduate recovery ‘Cold Standby’
  - Intermediate recovery ‘Warm Standby’
  - Immediate recovery ‘hot standby’

Cold Standby

Data restored from tape to standby machines in the backup site

- No significant cost in the telecommunication line between the primary and the backup site.
- Cost : Low
- Risk of data loss: High
- Recovery timeframe: Long

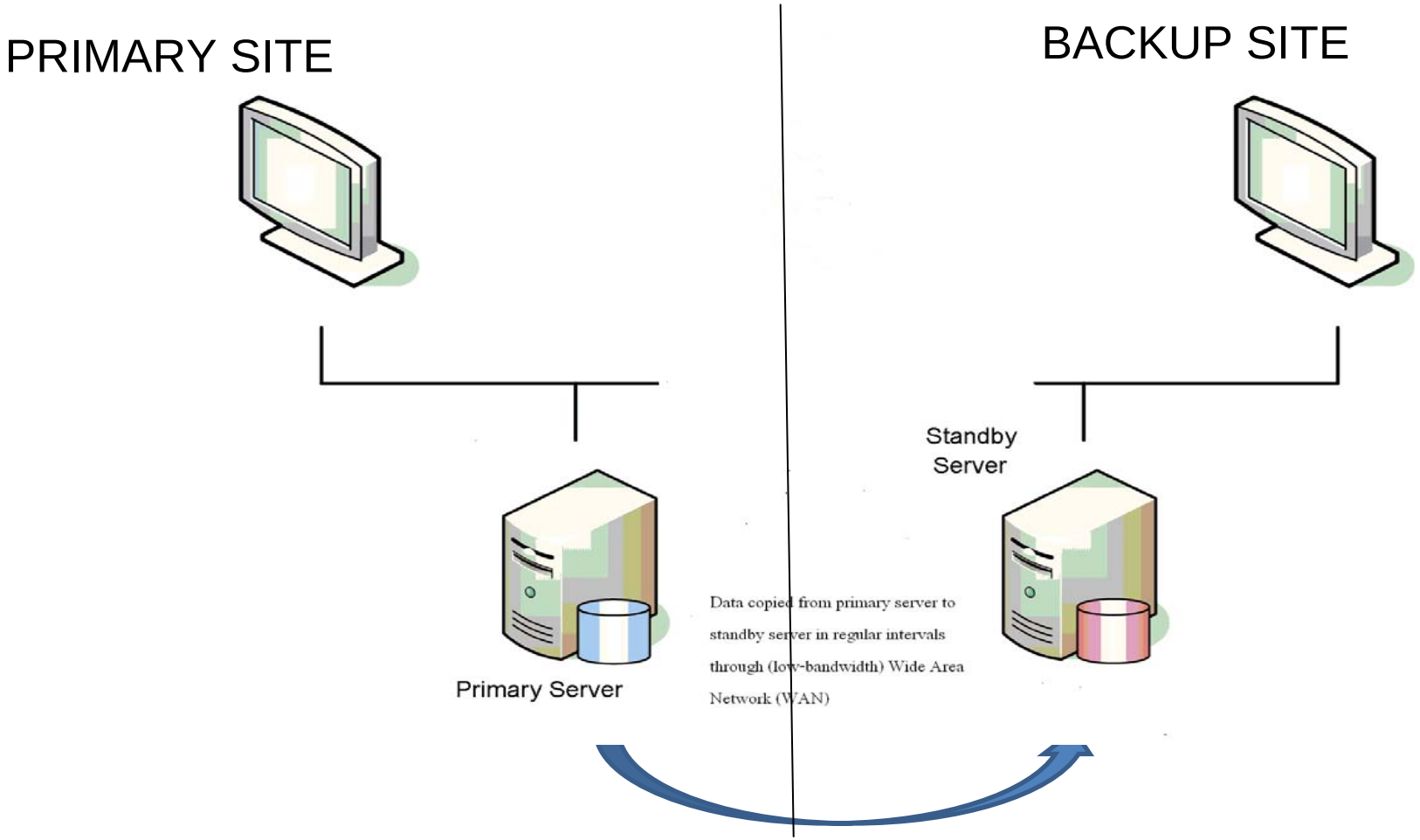
Primary machine fails, data restored to Standby machine via tape



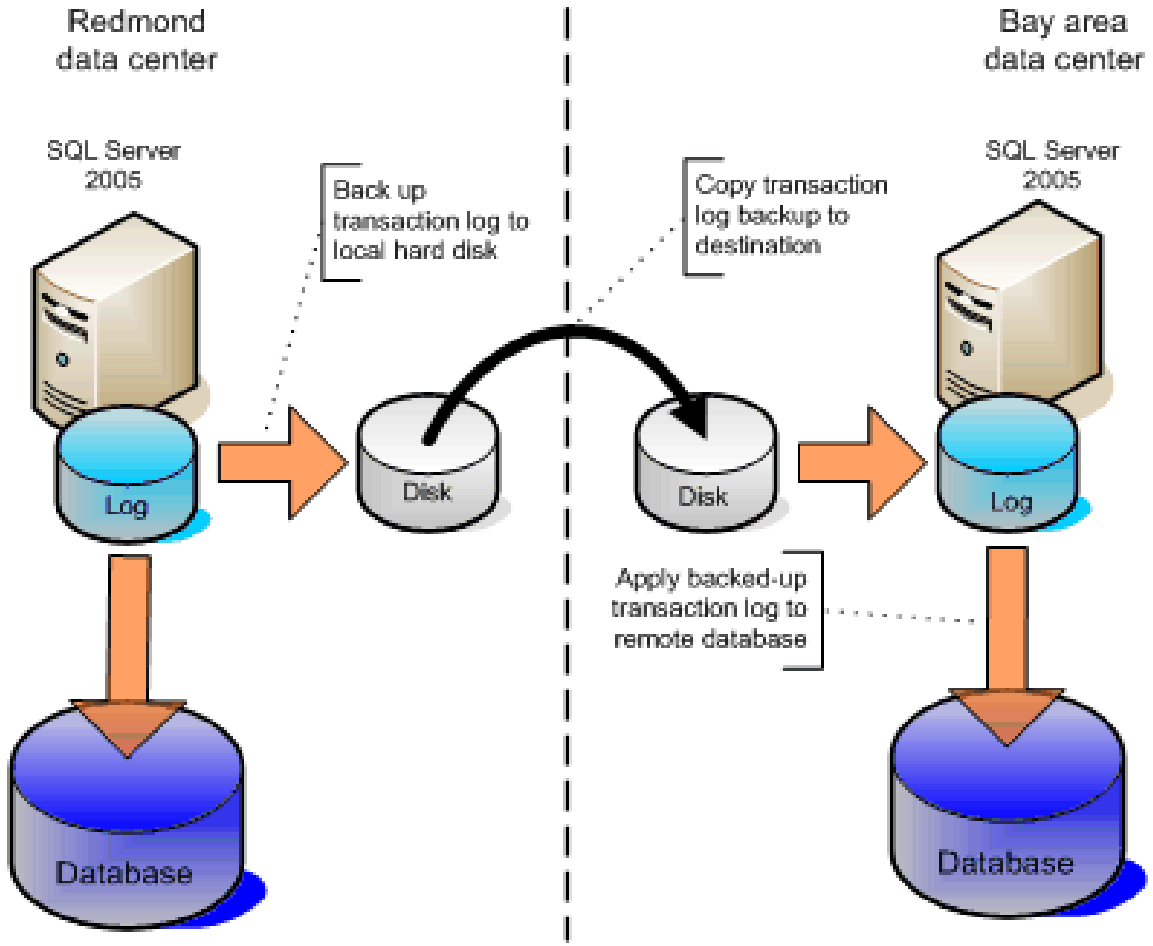
Warm Standby

- Asynchronous data replication/log copying across sites
- A low-medium speed linking the primary site and backup site
- Cost : medium
- Risk of data loss: medium
- Recovery timeframe: medium

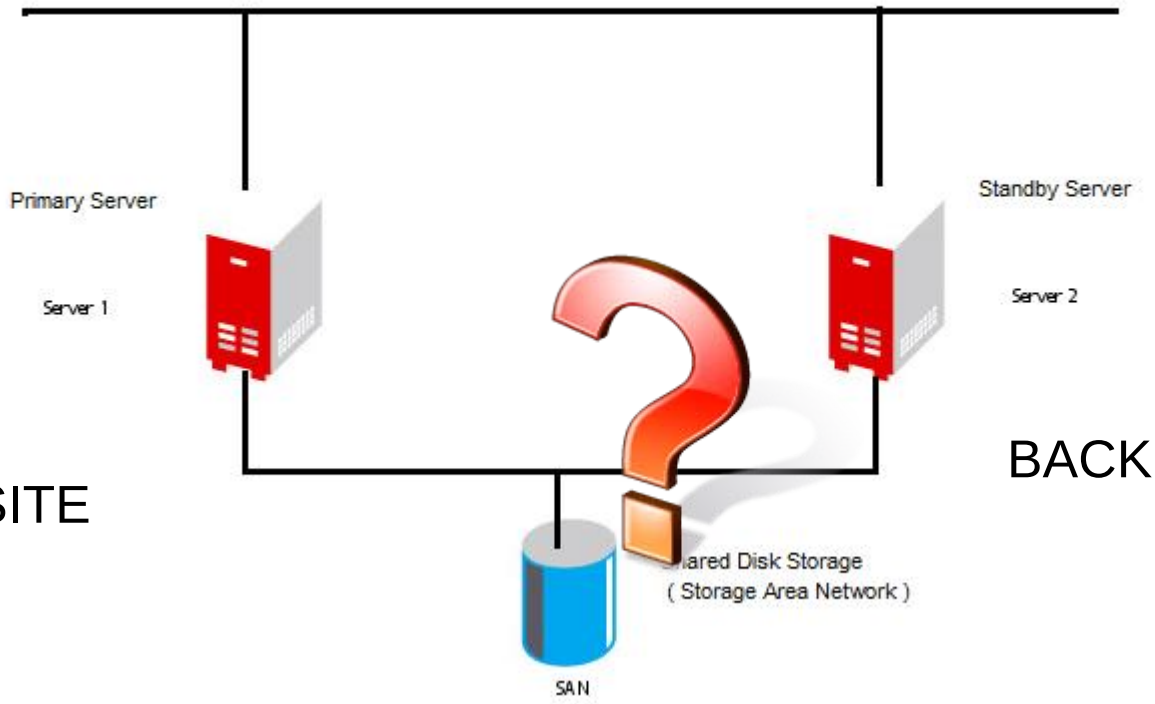
Warm Standby – Data copied from primary to standby machine regularly



Sample Warm Standby scenario



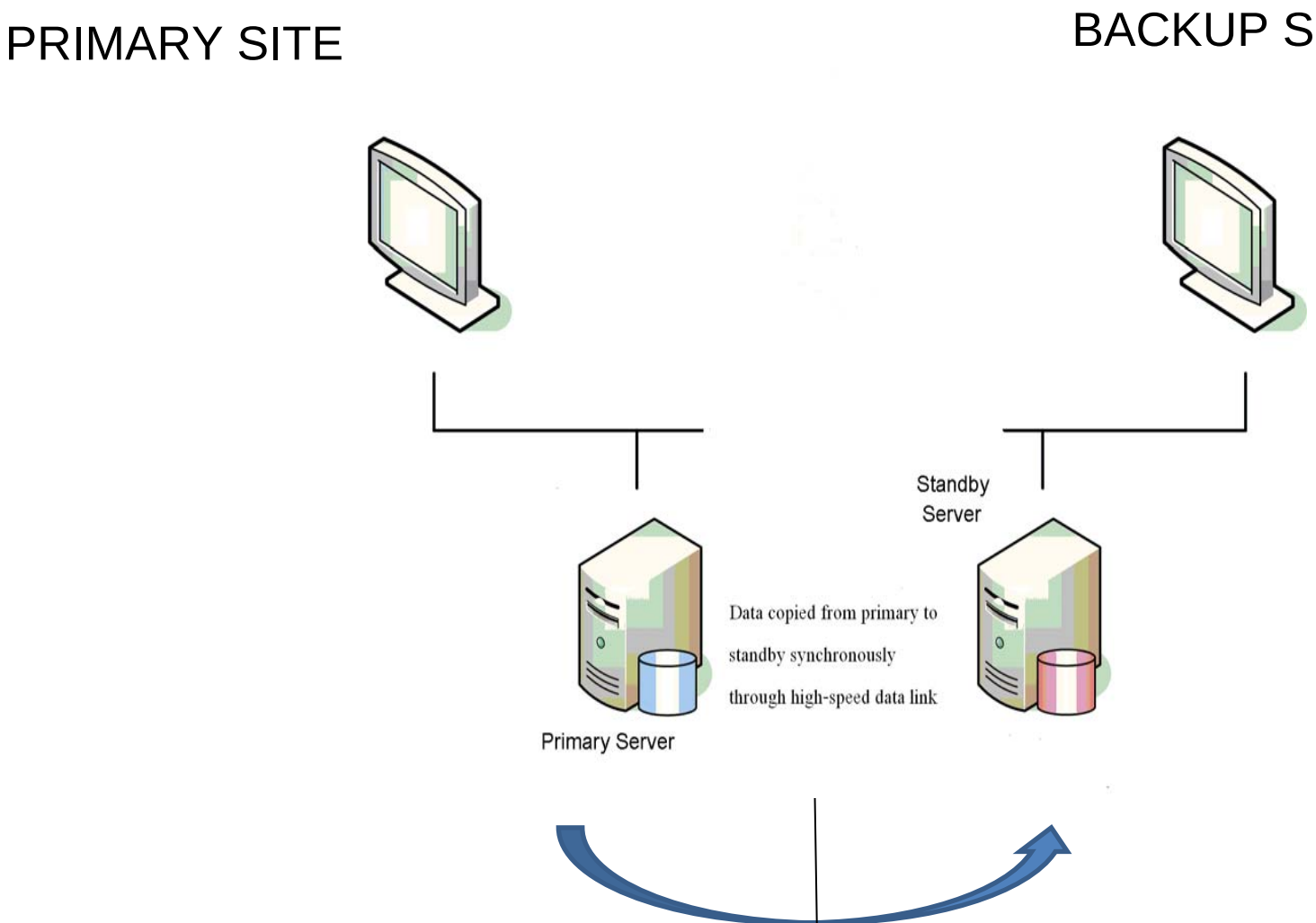
Hot Standby - Shared Storage cannot be employed in disaster recovery and sharing storage across different sites is not practicable.



PRIMARY SITE

BACKUP SITE

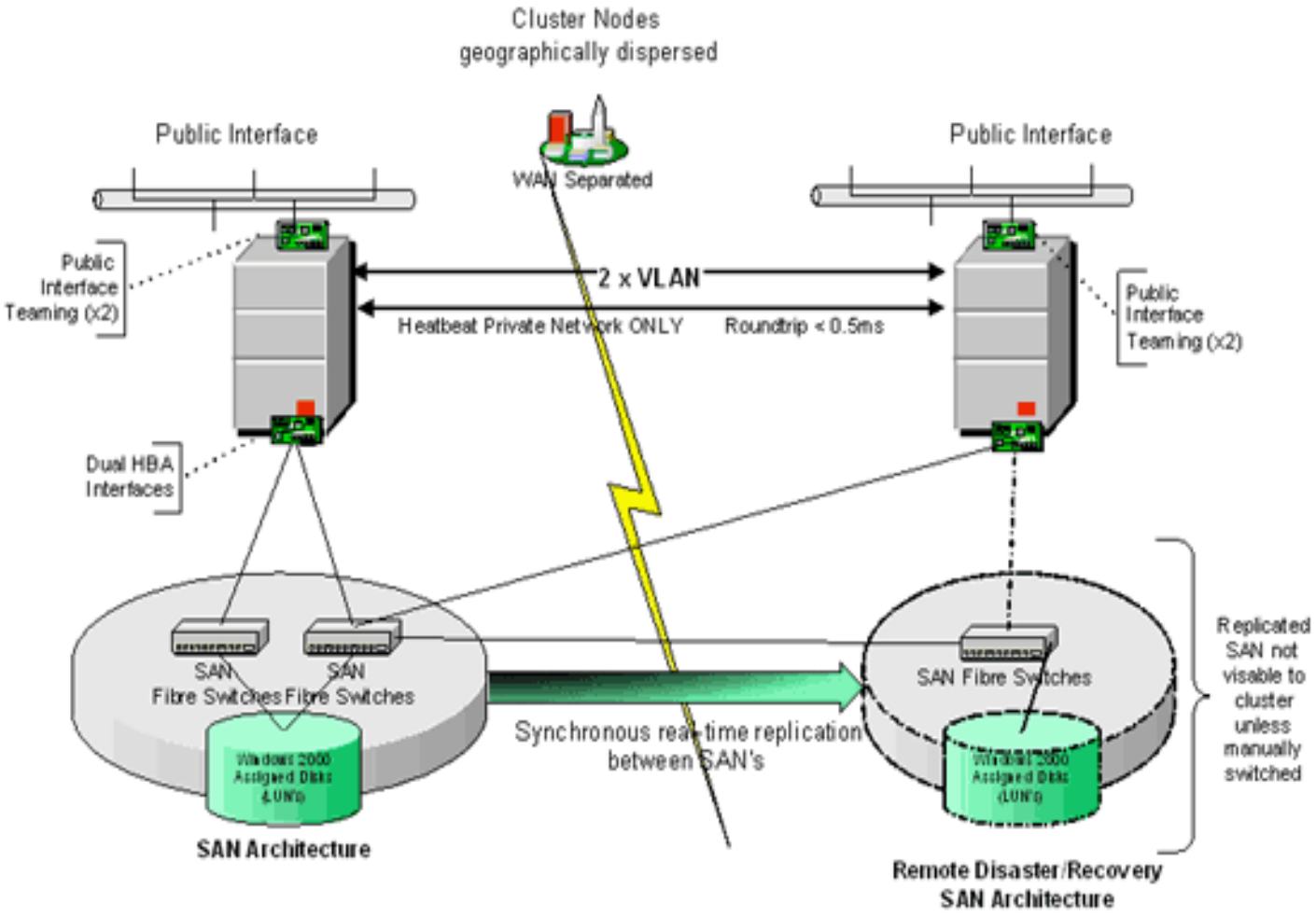
Hot Standby – Adopt similar Warm Standby scenario but use special storage system supporting synchronous data replication across high speed links



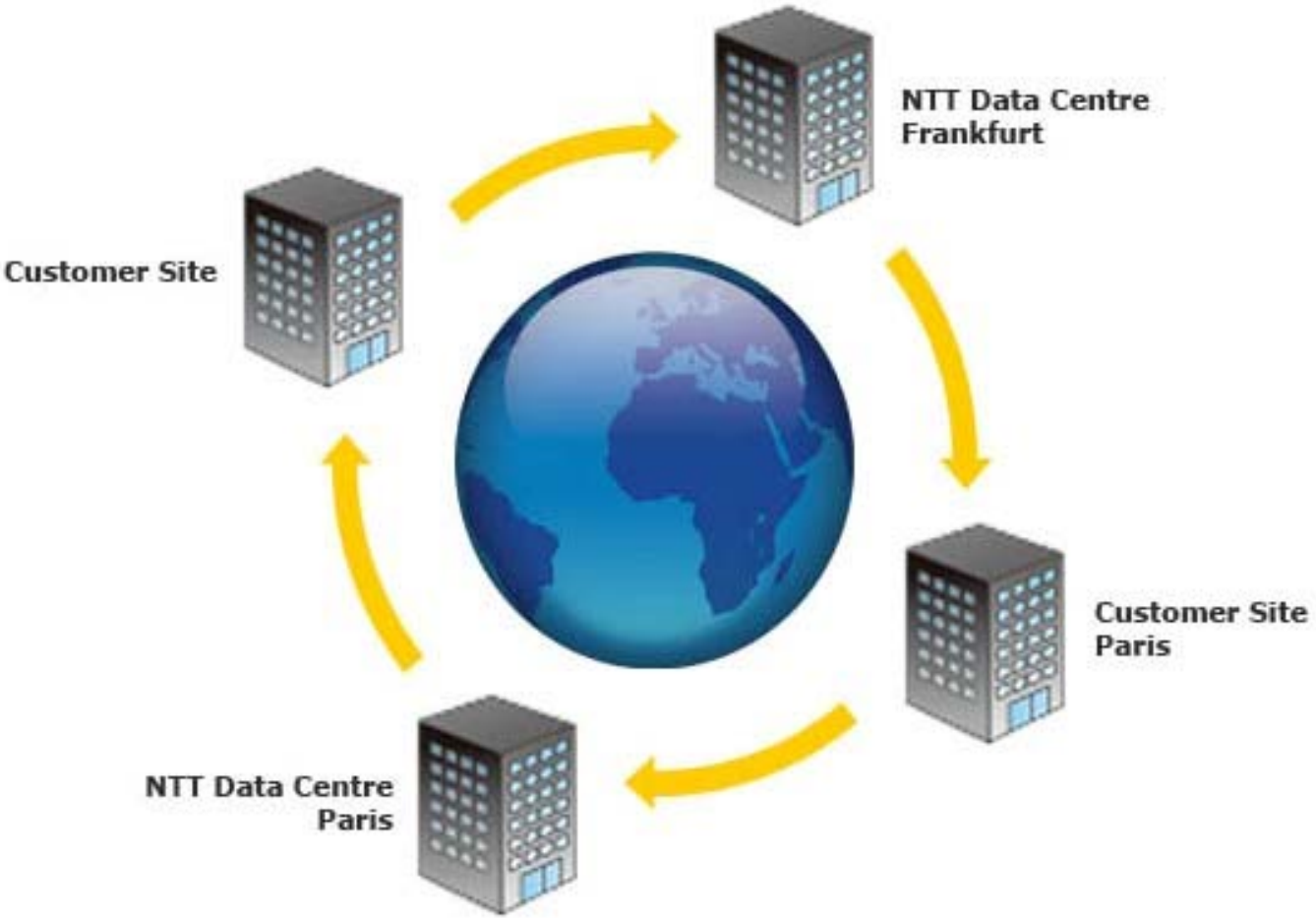
Hot Standby

- Like a hot standby recovery across sites
- Synchronous data replication
- High-speed link (usually fiber network link) linking primary and backup sites
- Cost : high
- Risk of data loss: low
- Recovery timeframe: short

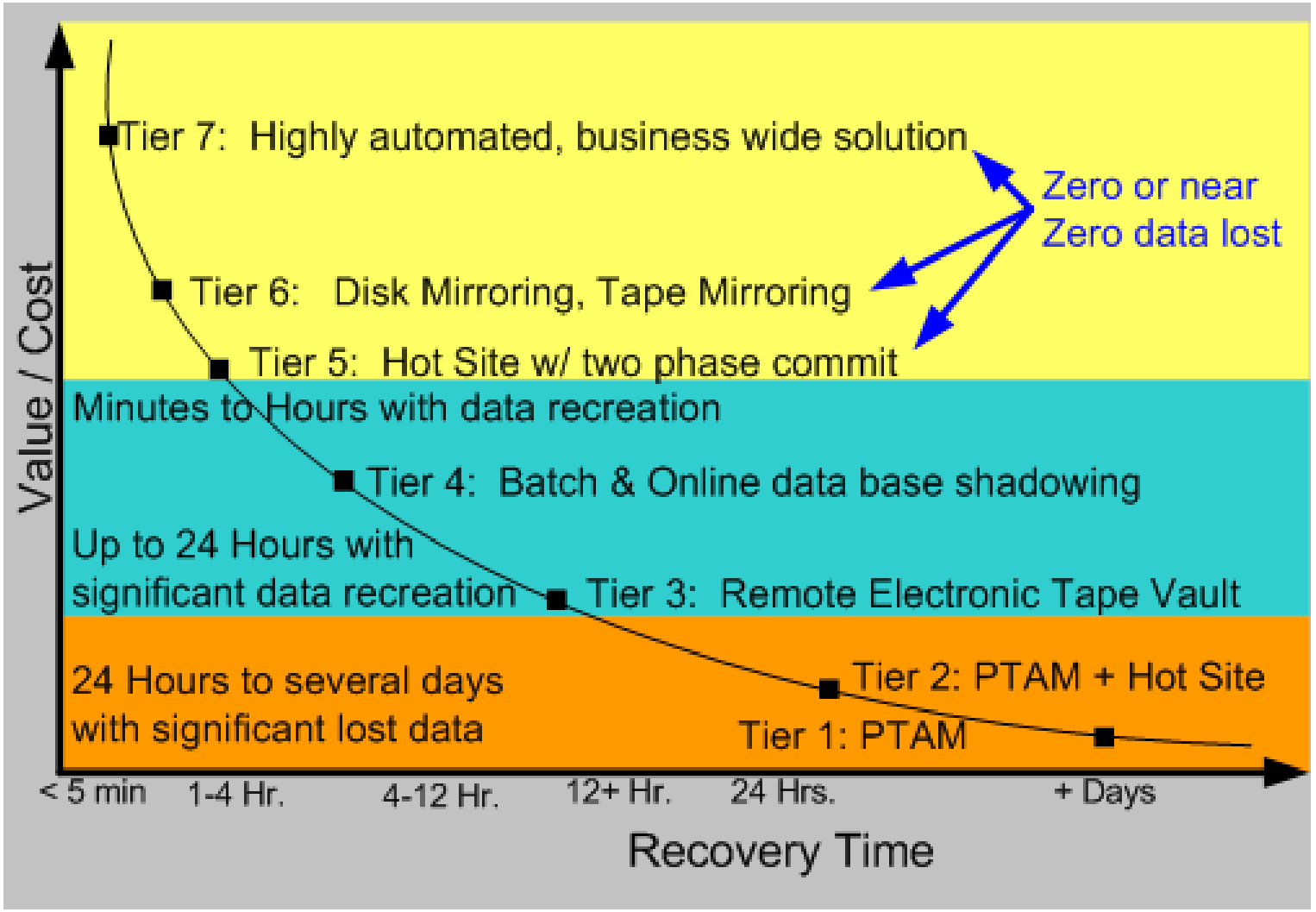
Hot standby Sample DR scenario



And, of course, locating primary and backup data centres should be located far apart



Cost versus Recovery Time



1.3 ITSCM Stage 3 Implementation

- Organisation & Implementation planning
- Develop (recovery) ITSCM plans
- Develop procedures
- Initial Testing
  - Testing is a critical part of ITSCM & is the only way of ensuring that stand-by arangements and business recovery plans will work in practice

1.4 ITSCM Stage 4 Operational Management

- Invocation
- Education & Awareness
- Review & Audit
- Testing (Regular testing after initial testing)
- Change Control
- Assurance

ITSCM – Invocation启动& Responsibilities

- Invocation is the ultimate test of the Business Continuity & ITSCM plans
- Decision to invoke by the Crisis危机Management team
- Consider the cost & disruption to the business
- Plans available in the office & at home
- Summary list available at all times the location of the plans, the associated key action & decision points, contact details of the crisis management team
- Once the recovery has been completed, the business should be able to operate from the recovery site at the level determined & agreed in the BCM strategy

ITSCM
Generating Awareness引起体认

- Awareness & commitment from the board & senior management, fully endorsed & sponsored required
- The best & most effective way to raise senior management awareness is to highlight the potential risks & business impacts facing an organisation in terms of business failure to meet key performance indicators
- Initial awareness for buy-in
- Ongoing awareness (training)

ITSCM benefits

- Potential lower insurance保险premiums
- Management of risk & the consequent reduction of the impact of failure
- Ability to meet regulatory监管or mandatory requirements

ITSCM Possible Problems

- Gaining buy-in & assistance from the business
- Availability of components, resources & data to test the IT recovery & BCM plans
- Overlooking critical components, applications & dependencies & misinterpreting business impacts

ITSCM benefits

- Business can survive a disaster
- Opportunity to compete for business, increased customer confidence & organisational credibility
- Reduced business disruption干扰in the event of a disaster, with ability to recover services efficiently

2. Service Design – Capacity Management

Dr. Franklin Leung

Definition

- Capacity Management is the process responsible for ensuring that IT processing and storage capacity provision match the evolving demands of the business in a cost effective & timely manner.
- Examples: Management on CPU capacity, memory capacity, disk storage capacity, bandwidth

Goal

- To understand the future business requirements (the required service delivery), the organisation's operation (the current service delivery), the IT infrastructure (the means of service delivery) & ensure that all current & future capacity & performance aspect of the business requirements are provided cost effectively.

Scope

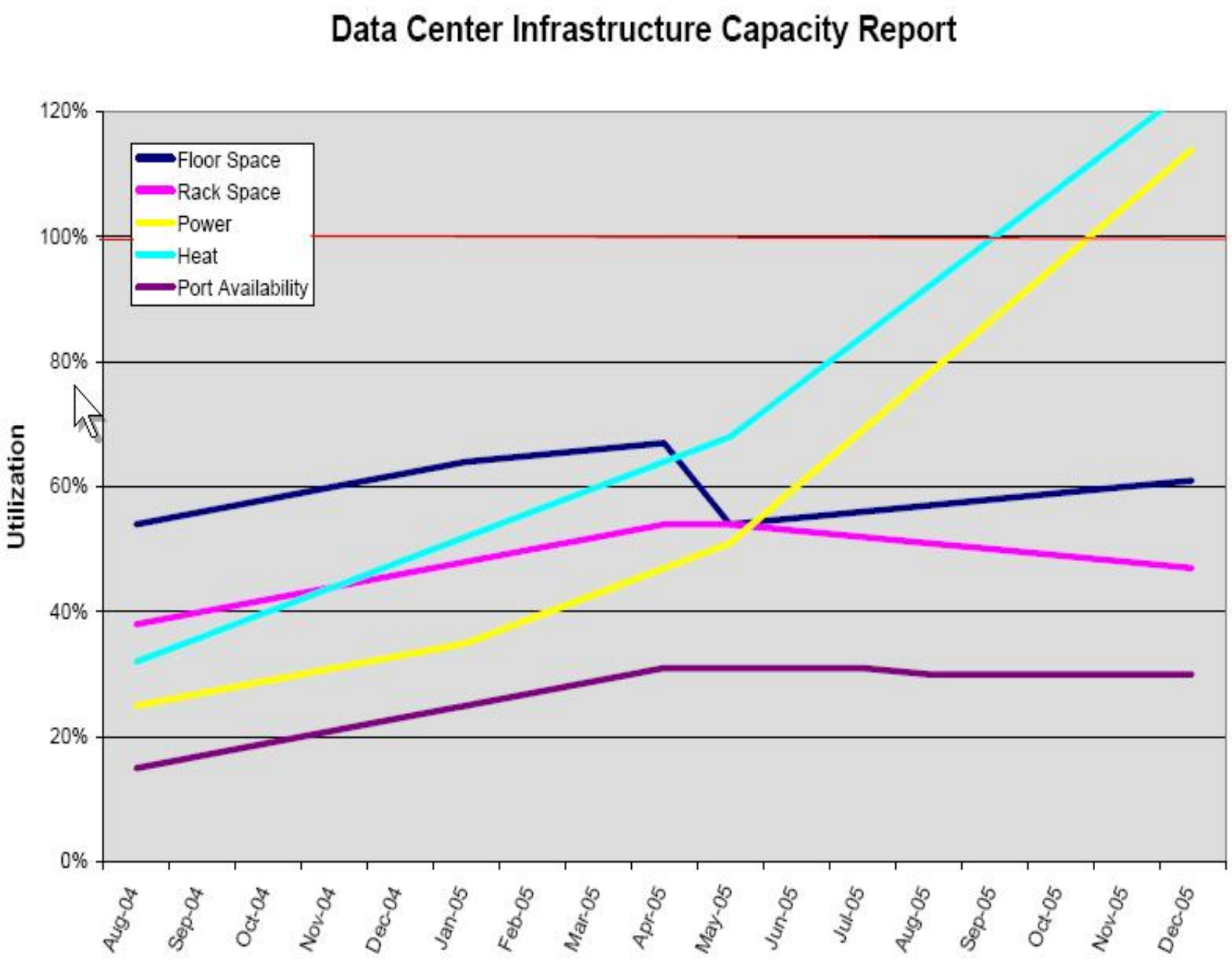
- The scope includes all hardware, networking equipment, peripherals and software for both the operational & development environments & is the focal point for all IT performance & capacity issues.

3 key elements

- Business Capacity Management (BCM)
  - Trend, forecast, model, size & document future business requirements
- Service Capacity Management (SCM)
  - Monitor, analyze and report on service performance; establish baseline & profiles
- Resource Capacity Management (RCM)
  - Monitor, analyze and report on the utilisation of components, establish baselines & profiles

Examples of Capacity Data

- Processor Utilization
- Memory Utilization
- Per cent processor per transaction type
- IO (input-output) rates and device utilization
- Disk Utilization
- Transaction rates
- Network traffic rates (bandwidth utilization)
- Batch Duration


Data Center Infrastructure Capacity Report
Floor Space
Rack Space
Power
Heat
Port Availability
Utilization
120%
100%
80%
60%
40%
20%
0%
Aug-04
Sep-04
Oct-04
Nov-04
Dec-04
Jan-05
Feb-05
Mar-05
Apr-05
May-05
Jun-05
Jul-05
Aug-05
Sep-05
Oct-05
Nov-05
Dec-05

Key activities

- Monitoring
- Analysis
- Tuning
- Implementation
- Modeling
- Application sizing

Capacity database

- Inputs: business data, service data, technical data, financial data, utilization data
- Storage: Capacity database
- Outputs: Service & Component based reports, exception reports, capacity plan & forecasts

Roles & Responsibilities

- Ensuring adequate IT capacity to meet required levels of service
- Ensure optimized use of existing capacity
- Responsible for advising the SLM process about appropriate service levels
- Assesses new technology & its relevance to the organization
- Recommend resolutions to performance related incidents

Benefits

- *Increased efficiency & cost savings resulting in more economic provision of IT services*
- *Planned buying & panic buying*
- *Reduced risks of performance problems & failures*

Possible problems

- Customer expectations exceed technical capacity or are not prepared to pay
- Over expectation of the benefits to be gained from tuning/upgrade
- Unrealistic & unachievable performance figures from equipment suppliers & manufacturers
- Unreliable & inaccurate business forecasts & information

3. System Design – Other processes

Other processes

- Information Security Management
- Supplier Management

Other activities in Service Design

- Organizing for Service Design
  - Activity Analysis
  - Skills
  - Roles and responsibilities
    - Service Design Manager
    - IT Designer/Architect
    - Service Level Manager
    - Availability Manager
    - IT Service Continuity Manager
    - Capacity Manager

4 Service Transition
- Change Management

By Dr. Franklin Leung

Change Management

Definition

- The process of controlling Changes to the infrastructure or any aspect of services, in a controlled manner, enabling approved Changes within minimum disruption.

Goal

- Ensuring that changes are recorded, evaluated, authorized, prioritized, planned, tested, implemented, documented and reviewed in a controlled manner.

Goal of Change Management

- To ensure that standardised methods & procedures are used for efficient & prompt handling of all Changes, in order to minimise the impact of change-related Incidents upon service quality & consequently to improve the day-to-day operations of the organisation
- Examples: large-scale desktop PC installation, operating system upgrade, adding additional CPU or hard disk storage, router configuration, firewall rules change, database scheme modification

Change Management

That means we want to:

- Reduce unplanned outages
- Improve service availability
- Reduce unnecessary urgent changes

Change Management

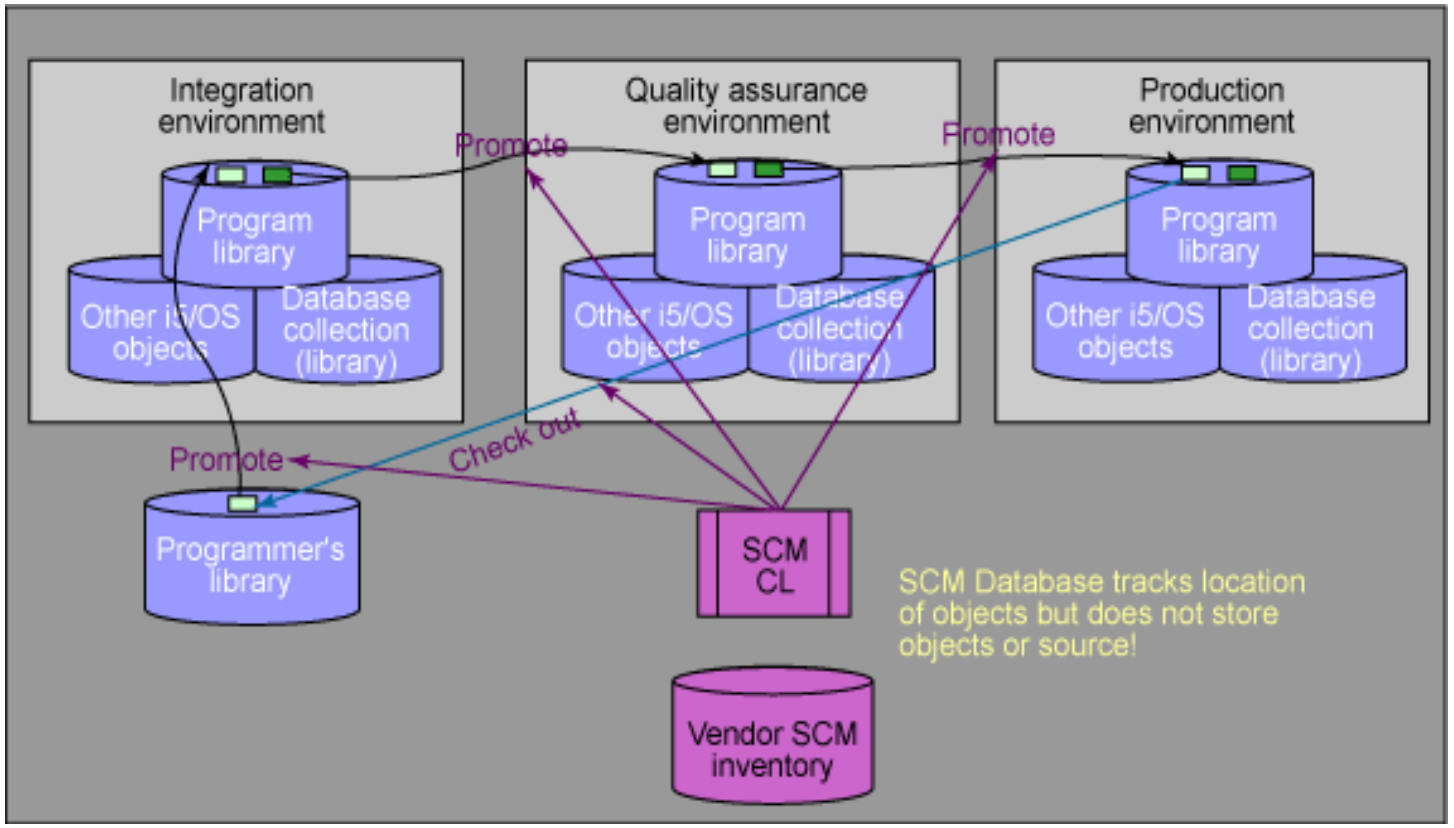
Scope

- Change management is responsible for managing Change processes involving hardware, software, communications equipment, system software, ‘live’ application software, & all documentation & procedures associated with the running, support & maintenance of live systems.

Challenges of Change Management

- Test before Implement (Availability of Testing Environment)
- Documentation of Changes
- Interrelated components (e.g. compatibility issue such as “Can the existing database version run on new operating system? Can new operating system run on existing hardware? Can existing application run on the new platform?)
- Limited Time Window for carrying out changes

Three environments:
(a) Development/System Integration Env.
(b) Quality Assurance or User Acceptance Env. (c) Production Env.



Terms

- **Change Request –** Request to make a change to a particular system and service
- **Change Manager -** The person who makes sure that the change management process is followed
- **Change Advisory Board (CAB) –** The group that reviews and approves (or rejects) change requests
- **RFC (Request for Change)**

Change Management - RFCs

- A request for Change (RFC) is a form or screen used to record details of a request for a Change for any CI within an infrastructure or to procedures & items associated with the infrastructure
- An incident is not a change
- Customers/support staff can raise an RFC

RFC

- RFC can be raised
  - To apply the fix for an Incident or Problem
  - The proposed purchase of a CI
  - The removal of a CI
  - Proposed Upgrade of a CI
  - Location change
  - Product or service changes from vendors or contractors

Change Advisory Board (CAB)

- The change advisory board is a group of people who can give expert advice to Change Management on the implementation of changes. This Board is likely to be made up of senior representatives from all areas within IT (e.g, network, server, application) and , sometimes, senior representatives from business units.

Key activities

- Change logging & filtering
- Allocation of priorities (immediate, high, medium, low)
- Change categorisation (minor, significant, major impact)
- CAB meetings
- Impact & resource assessment
- Approving & scheduling of RFCs
- Building, testing & implementing RFCs
- Change Review

A Good Change

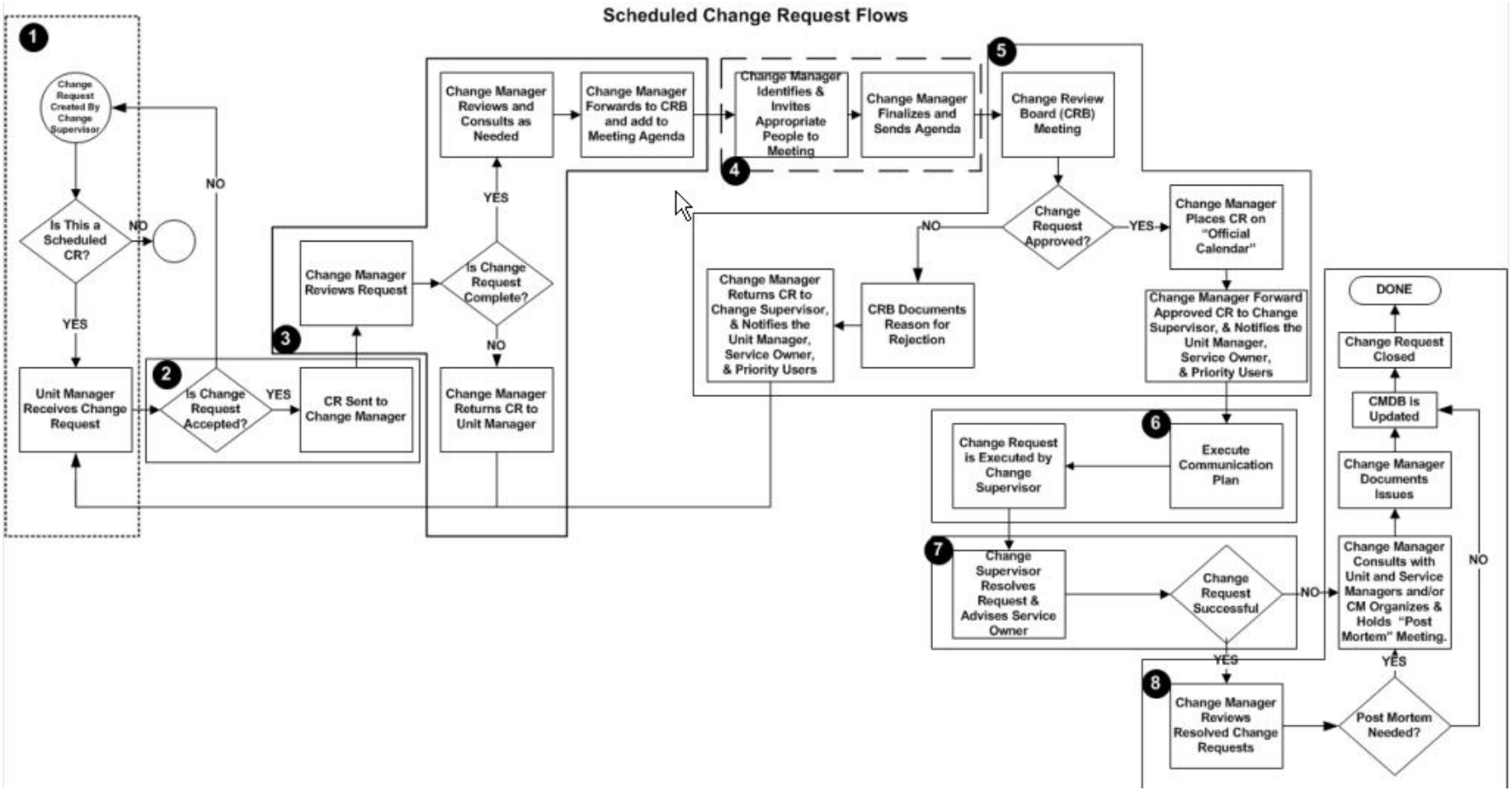
Must have

- Impact statement
- Business justification
- Approvals
- Test plan
- Implementation plan
- Fallback plan
- Useful and meaningful information

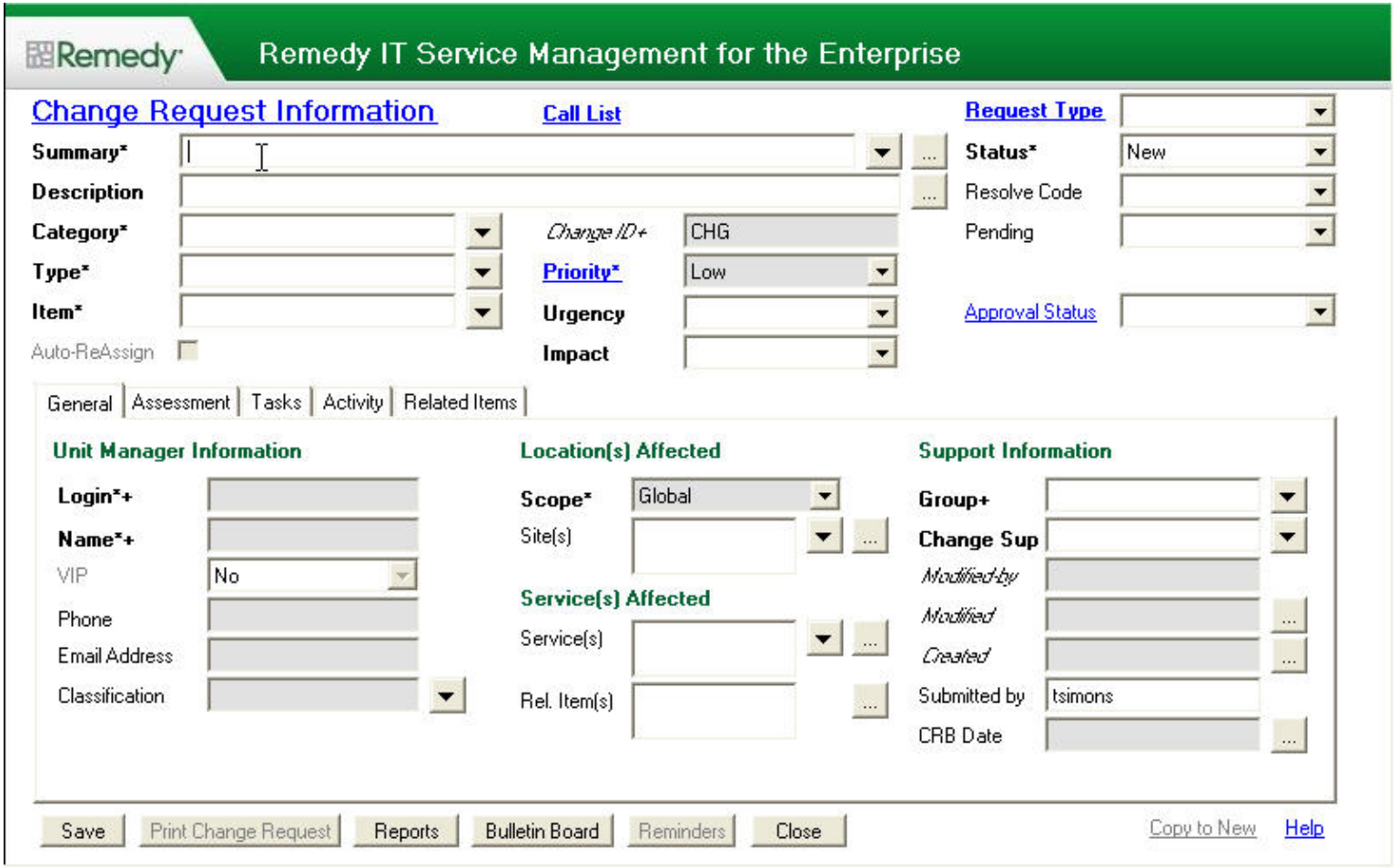
Segregation of duties

- Due to security considerations, no single party has the full authority and access rights to change the system
- For example, technical support engineers do not have the super-user (administrator) rights to critical servers because the administrator can have the rights to even erase audit trail.

Scheduled Change Flow



Remedy Change Request



Change Management

Benefits

- Minimize the impact of change-related incidents upon service quality
- Increase productivity by reducing disruptions for both users and IT staff
- Improve communication with affected Service Owners, support staff and users
- Improve risk assessment – balance need for Change against impact of the Change

Change Management

Possible Problems

- Non-adherence to CM procedures
- Implementing CM control of ‘all’ Cis & versions (i.e. level too low/detailed)
- Lack of control over urgent changes
- Lack of accurate CMDB
- Detection of unauthorized changes

Case on Service Transition - Change Management

Case Background

- A local sizable company's ITD does not have much change control. Log is entered voluntarily by system administrator and no supervisor approval is needed. For major changes, review by peers is needed.
- Changes carried out sometime have an unanticipated impact on the network environment, e.g. changing firewall rules once led to the disconnection of the whole network.
- Hire an external consultant to review the process

Major Changes (Process)

#	Major Changes	Benefits
1	Separate Change Mgmt activities from existing SDLC and Migration process	A single Change Mgmt process for consistency and efficiency
2	Centralized Change Mgmt function under a single Change Mgr	Consistency in RFC handling and improve process efficiency; Improve service availability via better coordination of Changes
3	Classification of RFC into different type with different approval and handling process	Streamline the RFC handling and more resources are focused on major changes
4	Introduction of Standard Change	Expedite the handling of repeated low-risk changes and reduce administration overhead.
5	More structured review of changes via CAB	Improve Change successful rate and service availability.

Benefit of Adopting ITSM Change Mgmt Practice

- A single Change Management process to manage all Changes in the Production environment to improve the process efficiency
- Improved Change successful rate via more structured and comprehensive Change review (planning, technical & deployment) and CMDB integration
- Tightly integrated with Incident, Problem Mgmt & other processes to ensure the required fix are implemented
- Centralized Change Management Function under a Change Mgr
  - An overall pictures of all changes in production environment so as to improve the service availability
  - Consistency in Change Management
  - Adopt "Standard" change model so as to expedite the handling of repeated low risk changes.

Major Activities of Change Manager

Daily/Weekly	Monthly	Ad-hoc
• Review the accuracy & completeness of RFC • Maintain the Change Approval matrix and monitor the status of RFCs • Conduct pre-change assessment meeting before major changes • Conduct post-mortem review on failed change • Chair & Coordinate CAB & ECAB meeting • Maintain the Forward-Schedule-of-Change and resolve conflict	• Prepare Change Mgmt report and identify improvement area via KPI measurement	• Conduct review of the Change Mgmt process for process improvement

5. Service Transition – Release and Deployment Management

Definition of Release Management

- The process of designing and implementing efficient procedures for the distribution & installation of Changes to IT systems into the live system

Goal of Release Management

- To take a holistic view of a Change to an IT Service & ensure that all aspects of a Release, both technical & non-technical, are considered together.

Scope of Release Management

- To undertake the planning, design, build, configuration & testing of hardware & software to create a set of Release components for a live environments. Activities also cover the planning, preparation & scheduling of a Release

6. Service Transition – Service Asset and Configuration Management

Dr. Franklin Leung

Configuration Management

Definition

- The process of identifying & defining Configuration Items (CIs) in a system, recording & reporting the status of CIs & requests for changes, & verifying the completeness & correctness of CIs.

Configuration Management

Goal

- To provide a logical model of the IT&T infrastructure or a service by identifying, controlling, maintaining & verifying the versions of configuration items in existence.

Configuration Management

Scope

- The identification, recording & reporting of IT&T components, including their versions, constituent components & relationships are part of the scope of Configuration Management. Items include hardware, software & associated documentation.

Challenges in Configuration Management

- Does your company have a whole picture of the configuration of all the PCs (e.g. how many are running Microsoft XP, how many PCs are running Microsoft 2003 etc.)?
- Is the configuration record accurate? (how to check the accuracy without involving significant manpower)?

Challenges in Asset Management

- Is the company's asset record accurate? (will any PC go missing but the asset record fails to record this?)
- Does a company establish the mechanism to detect and prevent the installation of unauthorized software (unlicensed software)?

Configuration management & Asset Management

- Not the same but related
- Asset Management is an accounting process that includes depreciation & details above a certain value
- Configuration Management also maintains the relationships between assets
- Many organisations start with Asset Management & then move to Configuration Management

5 key elements

- Planning
- Identification
- Control
- Status Accounting
- Verification & audit

CMDB

- The CMDB (Configuration management database) should hold all relevant system component details & the relationships between all system components, including incidents, problems, known errors, changes & releases. The CMDB also contains information & corporate data about employees, suppliers, locations & business units
- A configuration is anything that needs to be controlled

CMDB (Cont'd)

- CIs – a component within a configuration (hardware, software, documentation, staff)
- Attributes – describes a CI (name, version number, serial number, status)
- Naming conventions – should be unique & consider existing name structures (e.g. file server names)
- Baselines – the configuration at a specific point in time (snapshot)
- Labeling CIs – for easy identification

Configuration Management Tools

- Support more effective configuration management
- Easy addition & deletion of new & old Cis
- Maintenance of a history of all CIs
- Support for the use of baselines
- Good reporting facilities including inventory reports for audits, impact analysis, trend analysis & hierarchy relationships

Configuration Management

Benefits

- Providing accurate information on CIs & their documentation
- Making software changes visible
- Contributing to contingency planning
- Enabling the organisation to reduce the use of unauthorised software
- Providing problem management with data on trends

Research Paper on Configuration Management

The People, the Process or the Technology? Using the ACE framework to make tradeoffs in Service Delivery Improvement - Ramanathan et. Al.(2009)

Service Delivery Improvement

- Example case: PC Build and Install
- 100 requests for PC orders were received every month
- Request on standard configuration mixed with non-standard configuration
- Separate teams work together to provide the following services: help desk, request management, inventory management, approvals, billing, deployment, assembly/

Service Improvement Challenge

- Reduce the PC deployment time
- Develop a repeatable and scalable methodology that enabled continuous improvement through a monitoring and management framework
- Show “Return on the Investment” in best practices (ITIL) training and adoption of a CMDB

Service Analysis

- “As-is” versus “to-be” process
- Reference framework: ITIL, SCOR(plan-source-make-deliver), ACE(adaptive Complex Enterprise)
- “As-is” process study: adopt time-and-motion study, detailed time analysis for PC installation, site survey, cabling, approval, inventory etc (queue time, execution time)

“To-be” process

- Prioritizing those 80% standard configuration requests
- Eliminate the approval step for standard config PC request
- Maintain a up-to-date CMDB
- Optimize the assembly step by keeping an inventory of pre-imaged PCs