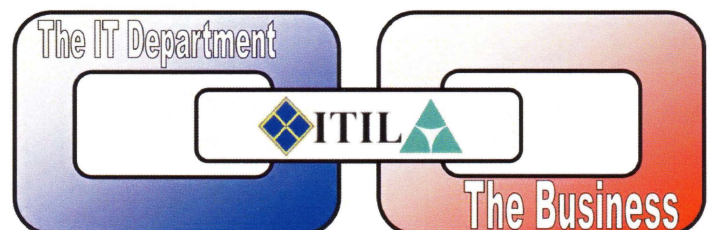




Learning Solutions

ITIL Fundamentals Foundation Certificate

Dimension Data Learning Solutions
www.DDLS.com.au
ph: 13 12 01



Other training available from DDLS: Microsoft, Cisco, Project Management, Soft Skills, Skills Based™ Desktop Applications training, ITIL, Computer Security, Citrix, Check Point, Lotus and Novell.



Introduction

History

In the late 1980's, the British Government surveyed roughly 1,000 organisations of all sizes and in all industries, in order to identify any consistencies in how these organisations managed their IT. These consistencies formed the basis for the IT Infrastructure Library (ITIL), as it is the collation of the best parts of these IT Management practices and is in constant development with contributions from organisations around the world. Because of its universal relevance it has become the de-facto global standard in IT Service Management.

Process Approach

ITIL organises the management of IT in processes rather than departments. Processes comprise a series of inputs, activities and outputs that cross department boundaries in order to meet a business goal.

Business First

ITIL is a collection of recommendations on managing IT. It should be considered a set of suggestions – the decision on how much depth to go into in each process depends on the business. IT should always be designed so as to be most appropriate for the organisation in which it exists.

Benefits

There has been a significant increase in interest about ITIL recently due to the benefits which it can bring. These include:

- Services that meet business, customer and user requirements
- Learning from previous experience
- Integrated centralised processes
- Demonstrable performance indicators

Process outline

For understanding and definition each process has three key features:

A Goal – the purpose of the process

Definitions – specific ITIL terminology

Activities – the responsibilities of each process

The ITIL Service Support Processes

Incident Management

Goal: To restore service as quickly as possible

Definitions:

- Incident – any event which is not part of the standard operations of a service and which causes, or may cause, an interruption to or a reduction in the quality of that service
- Impact – A measure of how greatly the activities of an organisation are effected by an incident
- Urgency – A measure of how quickly an incident needs to be resolved

Activities:

- Incident detection and recording
- Classification and initial support
- Investigation and diagnosis
- Resolution and Recovery
- Incident closure
- Ownership, monitoring, tracking and communication

Problem Management

Goal: To minimise the impact of incidents and to improve the stability of the infrastructure through root cause analysis of incidents.

Definitions:

- Problem: the unknown underlying cause of one or more incidents
- Known Error: An incident or problem, for which the root cause is known and for which a temporary workaround or a permanent alternative has been identified.

Activities:

- Proactive Problem management
- Reactive Problem Management
- Reviews

Service Desk

Goal: to be the single point of contact for users with IT-related queries and complaints

Definitions:

- Local Service Desk – A service desk providing assistance only to those people located in its own geographic location
- Centralised Service Desk – A single service desk which supports a number of different physical locations
- Virtual Service Desk – A service desk which is not located in one location, but can be contacted by a single phone number or email address. The Service Management database is the core of this type of service desk

Activities:

- Structure and People
- Processes
- Technology

Configuration Management

Goal: To centralise information relating to the IT Infrastructure and make it available to relevant parties

Definitions:

- CI (Configuration Item) – Any component of the infrastructure which is under the control of Configuration Management
- CMDB – the Configuration Management database

Activities:

- Planning

- Identification
- Control
- Status Accounting
- Verification

Change Management

Goal: To ensure changes are handled effectively, consistently, promptly and appropriately.

Definitions:

- RFC – Request for Change
- CAB (Change Advisory Board) – the body who considers RFCs and makes recommendations based on the business need
- Standard Change – the accepted solution to an identifiable and relatively common set of requirements, where authority is effectively given in advance or implementation.

Activities:

- Change logging and filtering
- Allocation of priorities and categorisation
- Impact and resource assessment
- Change approval and scheduling
- Change building and testing
- Authorisation and implementation
- Change review

Release Management

Goal: To ensure that all aspects of a release, both technical and non-technical are considered together.

Definitions:

- DSL (Definitive Software Library) – The DSL contains all authorised versions of all software approved for use in the organisation
- DHS (Definitive Hardware Store) – An area set aside for the secure storage of hardware spares

Activities:

- Release Planning
- Designing, Building and Configuring
- Testing and Acceptance
- Rollout planning
- Communication, Preparation and Training
- Distribution and Installation

The ITIL Service Delivery Processes

Service Level Management

Goal: To maintain and improve business aligned IT Service quality

Definitions:

- Service Catalogue – A document detailing the key features of all possible services provided by IT
- OLA (Operational Level Agreements) – An internal agreement covering the delivery of services which support the IT organisation in their delivery of services
- SLA (Service Level Agreement) – a written agreement between a service provider and the customer

Activities:

- Planning

- Implementation
- Ongoing Improvement

Financial Management

Goal: Aid the IT organization in implementing a cost-effective strategy for delivering IT services.

Activities:

- Budgeting
- Accounting
- Charging

Availability Management

Goal: To deliver a cost effective and sustained level of availability that enables the business to satisfy its business objectives

Definitions:

- VBF (Vital Business Function) – The business critical elements of the business process supported by an IT service

Activities:

- Availability Planning
- Availability Improvement
- Measurement and Reporting

Capacity Management

Goal: To ensure that cost justifiable IT Capacity always exists and that it is matched to the current and future needs of the business

Activities:

- Iterative Activities
- Modelling
- Demand Management
- Application Sizing
- Production of the Capacity plan

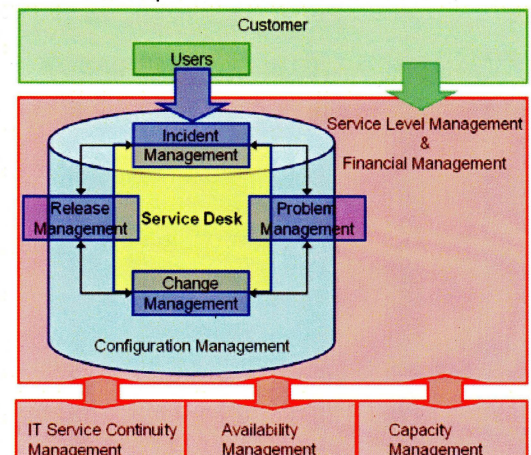
IT Service Continuity Management

Goal: To support the overall Business Continuity Management process by ensuring that the required IT technical and services facilities can be recovered within required, agreed business timescales

Activities:

- Initiation
- Requirements and Strategy
- Implementation
- Operational Management

The following diagram captures the interrelationships between the ITIL processes outlined



ITIL Foundation Certificate



Learning Solutions

THE IT INFRASTRUCTURE LIBRARY (ITIL)

Day 1



Learning Solutions

Introduction

- Who am I?
- Who are you?

© Redworld, 2004




Learning Solutions

Introduction

- Course Hours
- Meals
- Restrooms
- Phones
- Course Structure
- Questions

© Redworld, 2004


ITIL Foundation Certificate



ITIL Mission

"To provide a comprehensive, consistent and coherent set of **best practices** for IT Service Management processes - promoting a quality approach to achieving **business effectiveness and efficiency** in the use of information systems"

© Redworld, 2004



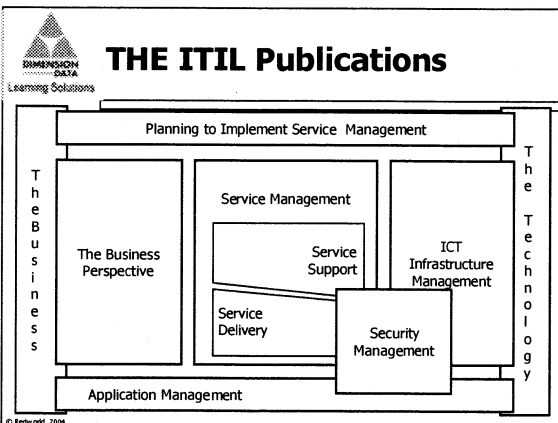
ITIL Reality

" 80% of infrastructure management improvements will come from ITSM* processes – only 20% will come from improved technology "

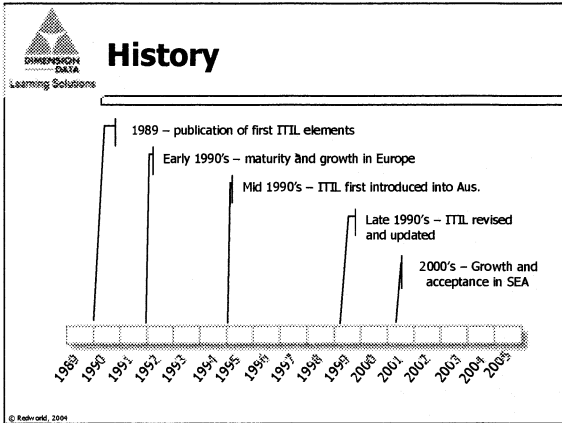
Gartner 20/11/2002

* IT Service Management




© Redworld, 2004



ITIL Foundation Certificate



ITIL Stakeholders

- OGC 
- EXIN 
- ISEB 
- itsMF 
- Tool Providers
- ITIL specialist organisations (consultancies, etc.)


© Redworld, 2004

ITIL Certification

	Fundamental/ Foundation	Practitioner	Masters/ Manager's
Prereq.	None	Foundation	Foundation
Format	3 days 1 hour multiple choice exam	3 days 2 hour multiple choice exam	12 days 2 x 3 hour essay exams and in course assessment
Target Audience	Anyone involved in any of the processes: technical staff; Help Desk; engineers; Change Management; business analysts; IT Management; Network Managers	Those who are responsible for a process and its refinement: Change Managers; Help Desk Managers; Configurations Managers; process owners	Those responsible for the overall implementation of the processes: IT Management; Consultants

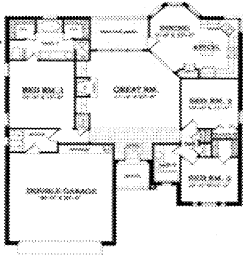
© Redworld, 2004

ITIL Foundation Certificate




ITIL Philosophy

- A library
- A framework
- Business focussed
- A process model




© Redworld, 2004



A Functional Model

The Help Desk	Human Resource	Network Mgmt	Finance/Accounts
☆	☆	☆	☆
☆	☆	☆	☆
☆	☆	☆	☆
☆	☆	☆	☆
☆	☆	☆	☆

© Redworld, 2004

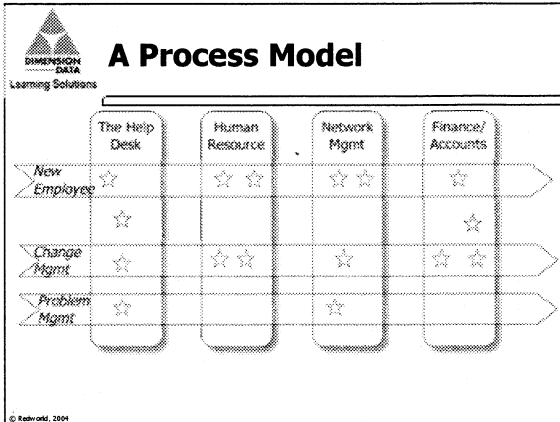


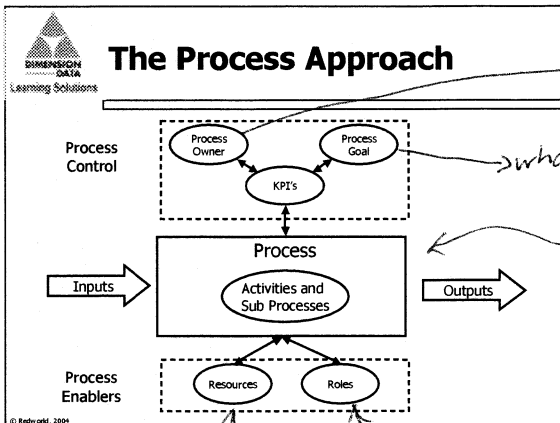
A Process Model

	The Help Desk	Human Resource	Network Mgmt	Finance/Accounts
New Employee	☆	☆	☆	☆
Change Mgmt	☆	☆	☆	☆
Problem Mgmt	☆	☆	☆	☆

© Redworld, 2004

ITIL Foundation Certificate





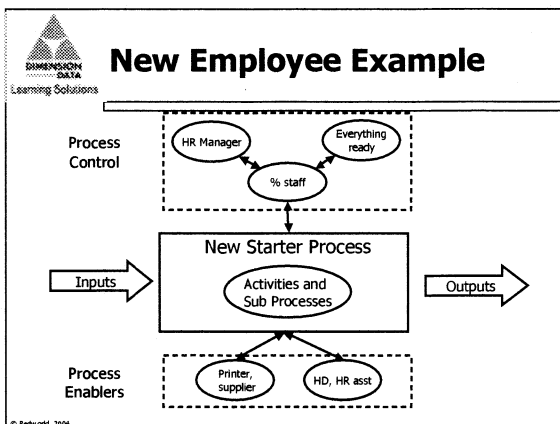
→ person who controls thing

→ what the outcome needs to be


→ getting done

parts and documentation

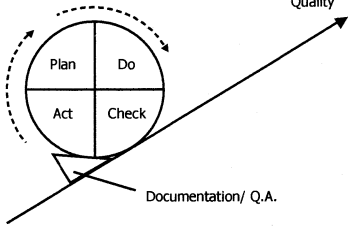
who does what



ITIL Foundation Certificate


 **ITIL And Standards**

The Deming Cycle



© Redworld, 2004

continuous improvement


 **Benefits**

- IT organisation built on understanding business needs
- Demonstrable performance indicators
- Consistency in service delivery
- Information sharing across the organisation
- IT contributing to the growth and health of the organisation as a whole

© Redworld, 2004

Communication

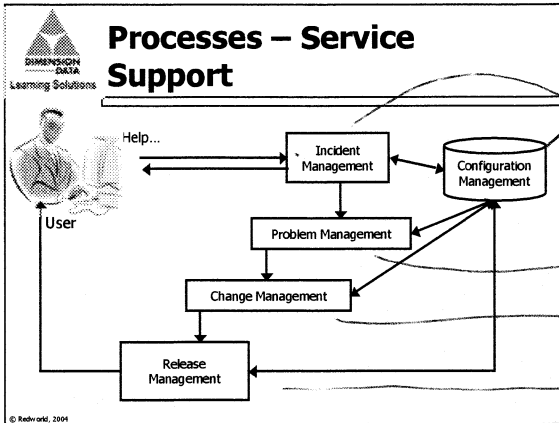
Procedures

 **The Processes**

ITIL Foundation Certificate

operational

- customer = user



software
CMDB - Asset database, what is in the comp what accesses etc

Get user going asap

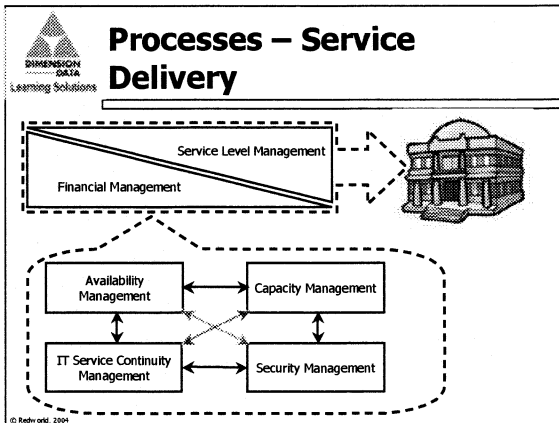
Determine underlying reason

Decide if a change is needed

Implement change and update CMDB

Tactical

- customer = business



Service Levels

Process Structure

- Goal
- Definitions
- Activities
- Benefits
- Possible Problems
- Metrics
- Tools

Things being measurement for reports

ITIL Foundation Certificate



CONFIGURATION MANAGEMENT



Goal

Configuration Management

- To account for all IT assets and configurations in the organisation, to ensure that this information is accurate, and to make this information available to support other Service Management processes

© Redworld, 2004

Asset management

What is of value ^{to} ~~of~~ I.T.

computers, servers, printers, software
databases, procedures, documentation, licence

Config management

How things are set up
plus plus



Definitions

Configuration Management

- Configuration Item (CI)
 - Any item of the IT infrastructure which will fall under the control of Configuration Management
 - Examples are: hardware, software, physical databases, baselines, change documentation, Service Level Agreements, procedures
- Configuration Management Database (CMDB)
 - a database that contains all relevant detail and relationship information about CIs.

© Redworld, 2004

ITIL Foundation Certificate

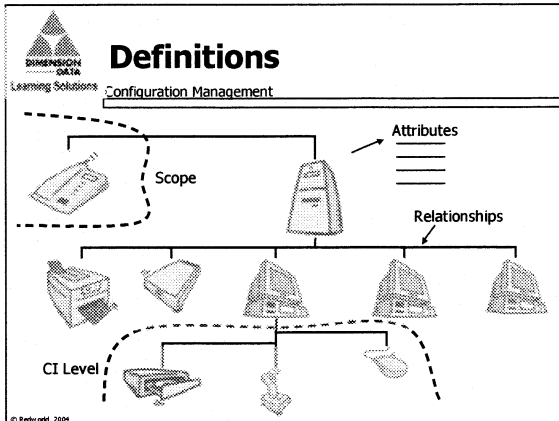
Definitions
Configuration Management

- Configuration baseline
 - The configuration of a product or system established at a specific point in time which captures both the structure and the details of a configuration.
 - Serves as a reference for further activities
 - Provides the opportunity to change or rebuild SOE

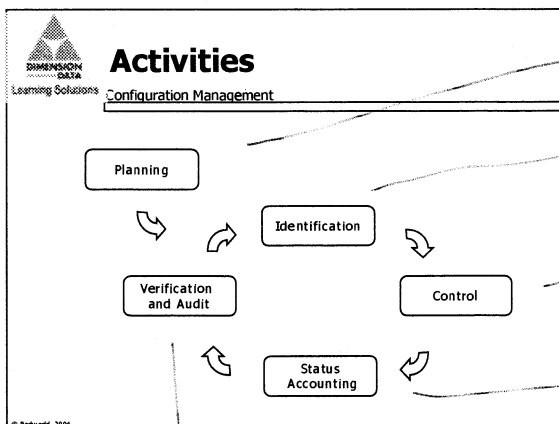
© Redworld, 2004

Snapshot in time

Can use it for a history of changes
or an audit trail



which levels of assets will we track.



→ objectives


→ Entering the information for new items

→ Keep it up to date via change management

→ Live or dead or lost or under maintenance


↓ Stocktake

ITIL Foundation Certificate

**Activities**
Learning Solutions Configuration Management


- Planning
 - Strategy, policy, scope, and objectives
 - Current situation analysis
 - Understanding the organisational context
 - Change or Release Management procedures
 - Interfaces with projects, suppliers, support teams etc.
 - Location of storage areas

© Redworld, 2004

**Activities**
Learning Solutions Configuration Management

- Identification
 - Numbering and naming conventions
 - Labelling
 - Creating documentation
 - Identifying relationships (h/w–h/w, h/w–s/w)
 - Populating the CMDB
 - Register all new CIs


© Redworld, 2004

**Activities**
Learning Solutions Configuration Management

- Control
 - Update CI records
 - Update RFCs with related CIs
 - Protect the integrity of the configurations
 - Ensures no CI is added, modified, or removed without appropriate controlling documentation (e.g. an approved Change request)

© Redworld, 2004


ITIL Foundation Certificate

**Activities**

Learning Solutions Configuration Management

- Status accounting
 - Reporting current and historical data for each CI through its life cycle
 - Eg “under development”, “live”, “in testing” etc.
- Verification and audit
 - A series of reviews and audits which verify the physical existence of CIs


© Redworld, 2004

**Benefits**

Learning Solutions Configuration Management

- Control of valuable CIs
- Support for the change and release management processes
- Support for the incident and problem management processes
- Improving security because CIs are harder to change without authorisation
- Helping with financial and expenditure planning
- Legal adherence where relevant

© Redworld, 2004

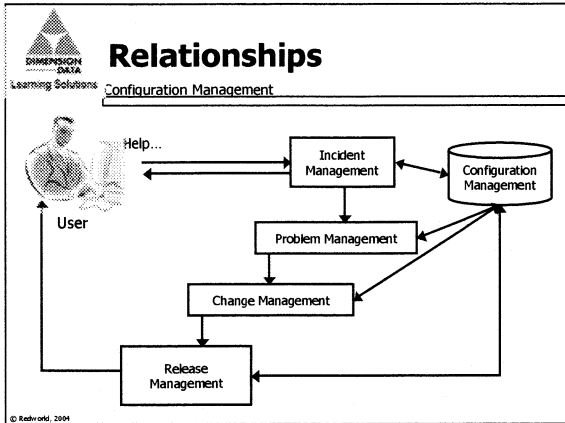
**Metrics**

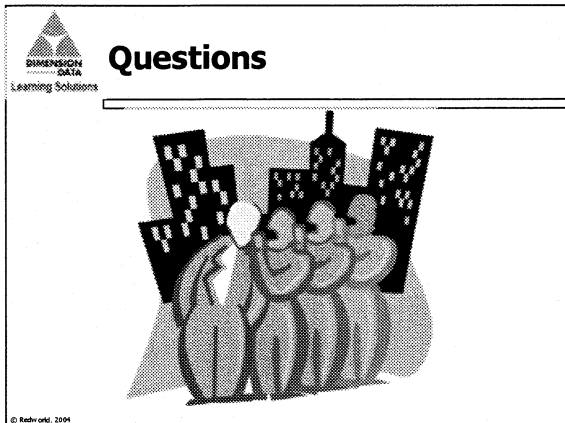
Learning Solutions Configuration Management

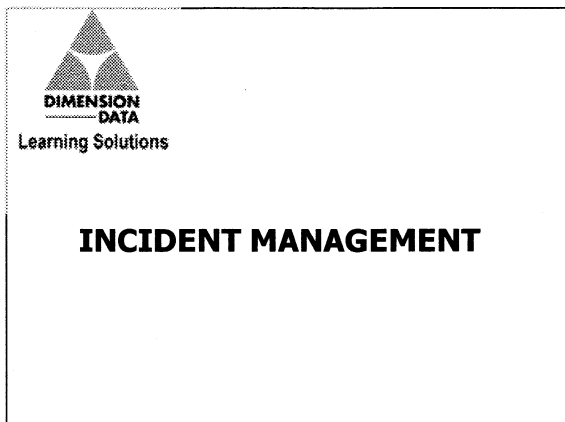
- Software licence usage and tracking
- Unauthorised components in use
- Exception reports on recorded vs. actual
- Unauthorised configurations in use
- Changes which failed as a result of poor Configuration Management Data

© Redworld, 2004


ITIL Foundation Certificate








ITIL Foundation Certificate



Goal

Incident Management

- To restore normal service operation as quickly as possible with minimum disruption to the business, thus ensuring that the best achievable levels of availability are maintained




Definitions

Incident Management

- Incident
 - Any event which is not part of the standard operation of a service and which causes, or may cause an interruption to, or a reduction in, the quality of that service
- Service Request
 - Requests for information

→ OR MAY CAUSE

→ THESE ARE INCIDENTS TOO



Definitions

Incident Management


- Escalation

Hierarchical escalation

```
graph TD; ITM[IT Manager] --> HDM[Help Desk Mgr]; ITM --> L2M[Level 2 Manager]; ITM --> L3M[Level 3 Manager]; HDM --> A1[Analyst]; HDM --> A2[Analyst]; L2M --> A3[Analyst]; L2M --> A4[Analyst]; L3M --> A5[Analyst]; L3M --> A6[Analyst];
```

Functional escalation

ITIL Foundation Certificate




Definitions

Incident Management

- Priority
 - Impact. A measure of the business criticality of an incident (often measured by number of people or systems affected)
 - Urgency. The necessary speed with which the incident needs to be addressed
 - Also:
 - Size, scope and incident complexity
 - Resources available to cope in the interim

© Redworld, 2004



Definitions

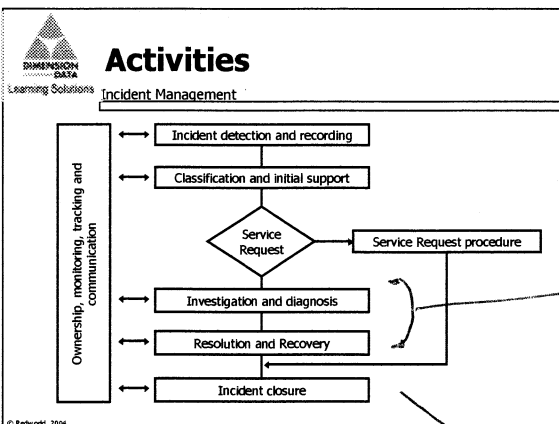
Incident Management

- Priority

Impact	High	3	2	1
	Med	4	3	2
	Low	5	4	3
		Low	Med	High

Urgency


© Redworld, 2004



→ Not a helpdesk function

→ by Service Desk


ITIL Foundation Certificate

**Activities**
Learning Solutions

Incident Management

- Incident Detection and Recording
 - System generated incidents
 - Record basic details of incidents
 - Alert support groups as necessary
 - Start procedures for Service Requests
- Classification and Initial Support
 - Classify incidents
 - Assess related configuration details
 - Assign Impact and Urgency (and therefore priority)
 - Match against Known Errors and Problems
 - Provide initial support
 - Close or re-route


© Redworld, 2004

**Activities**
Learning Solutions

Incident Management

- Investigation and Diagnosis
 - Assessment of incident details
 - Collection and analysis of all related information
 - Identification of a work around (if one exists)
 - Re-route to a further level of support if unresolved
- Resolution and Recovery
 - Resolve incident using work around or solution
 - Take recovery actions

© Redworld, 2004

**Activities**
Learning Solutions


Incident Management

- Incident closure
 - Closed by the Service Desk
 - Confirmed by the user prior to closure
 - Change to close category
- Ownership, Monitoring, Tracking and Communication
 - Monitor incidents
 - Escalate incidents
 - Inform user
- Reporting

© Redworld, 2004

→ SLA'S KPI'S

ITIL Foundation Certificate


**Benefits**

Learning Solutions

Incident Management

- Reduced business impact by timely incident resolution
- Availability of business focused management information related to the SLA
- Improved monitoring and reporting of IT efforts and resource usage
- Better staff utilisation
- Elimination of lost or incorrect incidents or service requests
- Improved user and customer satisfaction

© Redworld, 2004

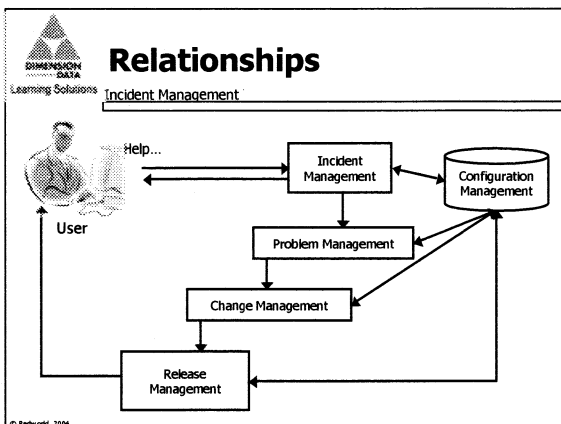
**Metrics**

Learning Solutions


Incident Management

- Total number of incidents
- Resolution time broken down by impact code and category
- Percentage of incidents handled within agreed timeframes
- Cost per incident
- Percentage of incidents solved without requiring reference to other levels of support
- Incidents per analyst
- Incidents resolved remotely without requiring a visit

© Redworld, 2004




ITIL Foundation Certificate

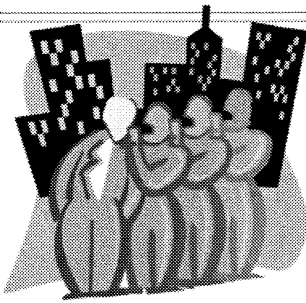
**Considerations**

- Incident management without Problem management can result in firefighting without the ability to eliminate root cause
- If you have the right kind of users, publicise the priority table


© Redworld, 2004

→ Fix it quick
→ Finding out why it happened


**Questions**



© Redworld, 2004

**PROBLEM MANAGEMENT**

ITIL Foundation Certificate


**Goal**

Learning Solutions

Problem Management

- To minimise the adverse impact of incidents and problems caused by errors in the infrastructure, and to proactively prevent the occurrence of incidents, problems and known errors

© Redworld, 2004

**Definitions**

Learning Solutions


Problem Management

- Problem
 - The unknown underlying cause of one or more incidents
- Known Error
 - A condition identified by successful diagnosis of the root cause of a problem - i.e. the identification of the CI responsible for the problem.

© Redworld, 2004

unknown cause of an incident

Now it's known

**Definitions**

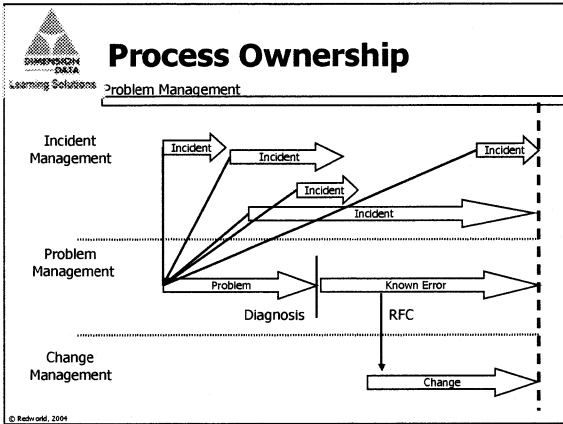
Learning Solutions

Problem Management

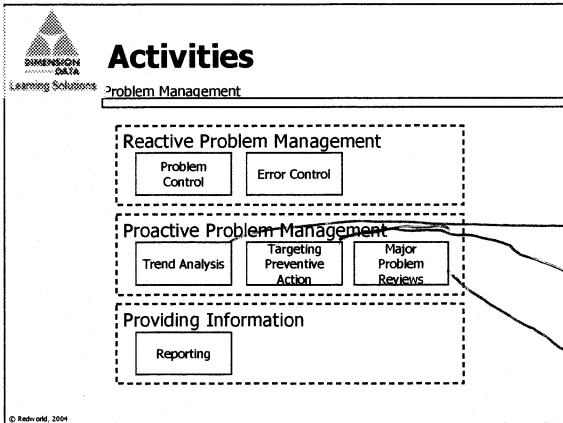
- Incident Matching:
 - Incidents should be linked to the associated Problem or Known error
 - The number of incidents caused by a specific Known Error or Problem can be tracked and reported over time

© Redworld, 2004

ITIL Foundation Certificate



A problem only gets created if it is a problem - not as soon as an incident is raised



The primary task of error control is to raise an RFC -> Request for change

2nd update known error database

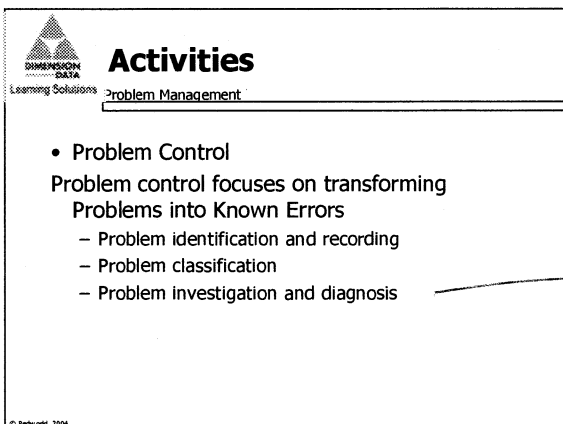
Secondary task

notice that something is going on

How to fix

How to stop it happening again

preventative action




what caused problem

↓

now its a known error

ITIL Foundation Certificate

**Activities**

Learning Solutions

Problem Management


- Error Control

Error Control focuses on resolving known errors through the change management process

- Error identification and recording
- Error assessment
- Recording error resolution (investigation of solution and raising of an RFC)
- Error closure
- Monitoring error resolution progress

© Redworld, 2004

→ when change successfully implemented


**Activities**

Learning Solutions

Problem Management

- Proactive Problem Management
 - Identifying and resolving Problems and Known Errors before Incidents occur.
- Tips:
 - Historical data is required
 - Reports from manufacturers can provide information on inherent Problems.
 - May be a part time role

© Redworld, 2004

**Activities**


Learning Solutions

Problem Management

- Trend Analysis
 - Identify 'fragile' components in the IT Infrastructure and investigate
 - Identify incipient or recurring faults of a particular type or with an individual item
 - Identify the need for more customer training or better documentation
- Targeting Preventive Action
 - Prioritise time spent and effort invested
 - Resolve the high impact issues

© Redworld, 2004

ITIL Foundation Certificate




Activities

Learning Solutions

Problem Management

- Major Problem Reviews
 - On resolution of every major problem, determine:
 - What was done right
 - What was done wrong
 - What could be done better next time
 - How to prevent the problem happening again
- Providing information
 - Reports on identified Problems, Known Errors and RFCs issued
 - Ad-hoc or periodically

© Redworld, 2004




Benefits

Learning Solutions

Problem Management

- Improved IT service quality
- Reduction in the volume of incidents
- Creation of permanent solutions
- Improved organisational learning
- Better first time fix rate at the Service Desk
- Right people doing the right jobs leading to greater job satisfaction

© Redworld, 2004



Metrics

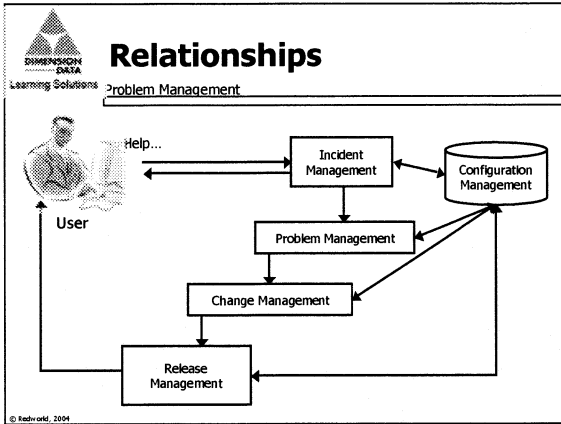
Learning Solutions

Problem Management

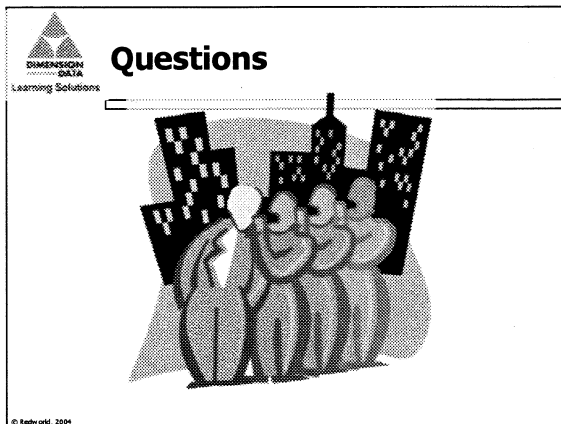
- Number of RFCs raised and their impact on availability
- Investigation time per organisational unit or supplier
- Number and impact of incidents occurring before the root problem is found
- Report of immediate effort to planned effort
- Number of incidents resolved at Service Desk
- Number of times a problem was solved from the knowledge base so not requiring research.

© Redworld, 2004

ITIL Foundation Certificate



- Principles to Apply**
- Manage the tension between Problem and Incident Management
 - Ensure that time is given to Problem management (this can be very difficult to justify)
 - Making known error information available to the other parts of IT
- © Redworld, 2004



ITIL Foundation Certificate



CHANGE MANAGEMENT



Goal

Change Management

- To ensure that standardised methods and techniques are used for efficient and prompt handling of all changes, in order to minimise the impact of any change related incidents upon the service



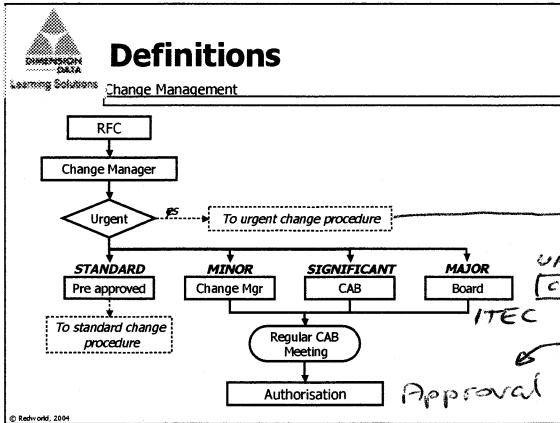
Definitions

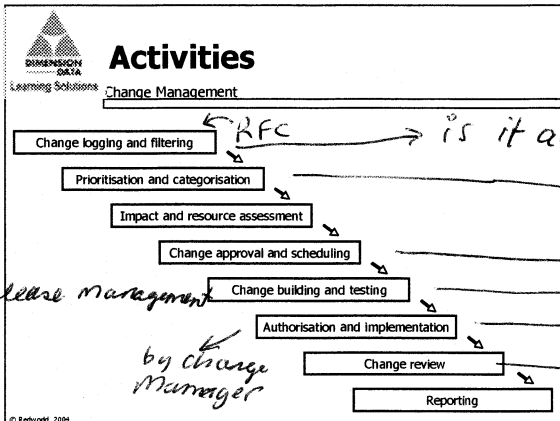
Change Management

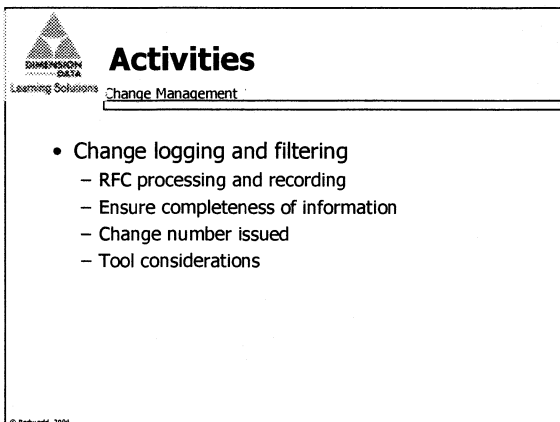
- RFC – Request for Change
- FSC – Forward Schedule of Changes
- PSA – Projected Service Availability
- CAB – Change Advisory Board
- CABEC – Change Advisory Board Emergency Committee
- ITEC – IT Executive Committee

- anyone can request a change
- Gant chart of resources needed when etc
- Planned outages, maintenance windows
- stakeholders decided by change Manager
- unplanned outage, emergency change
- major changes with senior execs pro-business


ITIL Foundation Certificate







ITIL Foundation Certificate




Activities

Change Management

- Allocation of priorities and categorisation
 - Use a priority matrix based on impact and urgency
 - Categorised into minor, significant, major, standard or urgent

© Redworld, 2004

→ sometimes called classification




Activities

Change Management

- Impact and resource assessment
 - Impact on customer's business
 - Impact on other services
 - Impact of non-implementation
 - Resources required
 - FSC and PSA considerations

© Redworld, 2004




Activities

Change Management

- Change approval and scheduling
 - Approval method determined by the organisation
 - Organise appropriate authorities
 - Schedule change
 - Consider other changes currently being scheduled
 - Release Management

© Redworld, 2004

ITIL Foundation Certificate


**Activities**

Learning Solutions

Change Management

- Change building and testing (1)
 - All RFCs should be passed to the relevant technical groups for building of Changes
 - Change Management coordinates
 - Supported by Release Management
 - Back-out procedures should be prepared and documented in advance

© Redworld, 2004


**Activities**

Learning Solutions

Change Management

- Building and Testing (2)
 - Testing should include:
 - Performance
 - Security
 - Maintainability
 - Supportability
 - Reliability/availability
 - Functionality
 - Regression
 - Testing may be retrospective

© Redworld, 2004

**Activities**

Learning Solutions


Change Management

- Change Authorisation and implementation
 - Final "green light" before implementation
- Change review
 - Desired effects
 - Individual change review
 - Process review
- Reporting

© Redworld, 2004

*Backup plan.
} it's fixed.
} nothing else is broken.*

ITIL Foundation Certificate


**Benefits**

Learning Solutions

Change Management

- Improved risk assessment
- Better alignment of IT services to business requirements
- Reduced adverse impact of changes on the quality of services
- Better assessment of impact prior to implementation
- Fewer backed out or failed changes
- Improved Availability Management
- Increased user productivity

© Redworld, 2004

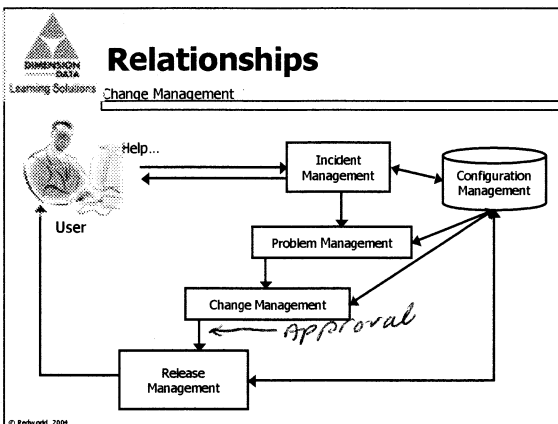
**Metrics**

Learning Solutions


Change Management

- Number of changes per period - successful and unsuccessful (together with the reason)
- Number of incidents caused by changes
- Number and outcome of change reviews
- Number of rejected RFCs
- Change backlogs by category
- Reasons for changes
- Sources of change requests
- Number of changes by category (urgent, standard, etc.)

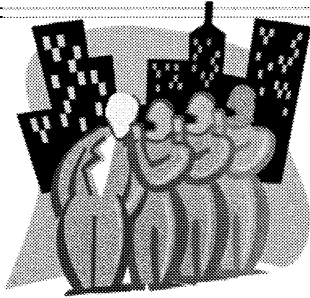
© Redworld, 2004



ITIL Foundation Certificate




Questions



© Redworld, 2004



SERVICE DESK




Goal

Service Desk

- To provide a single point of contact to offer advice, guidance and provide rapid restoration of services to customers and users

© Redworld, 2004

ITIL Foundation Certificate




Definitions

Service Desk

- Service Desk is a *function*, not a process
- Service Desk could be the customer's only window into IT
- The central point of contact called
 - Help Desk
 - Call Centre
 - Service Desk
 - Customer Support Group

© Redworld, 2004

→ note this!




Implementation

Service Desk

- Considerations
 - Resources
 - Targets
 - Follow the sun
 - Incident classification
 - Structure
 - Resolution / contact – phone? Email?

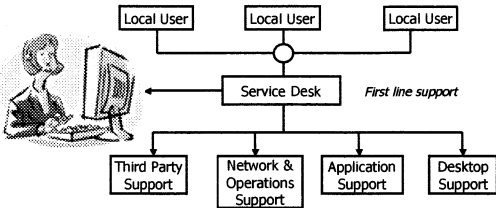
© Redworld, 2004



Implementation

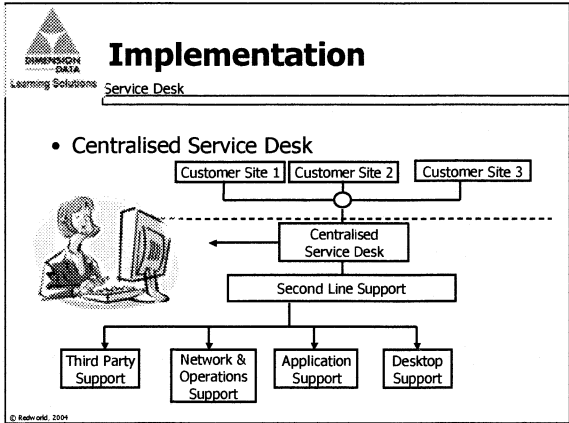
Service Desk

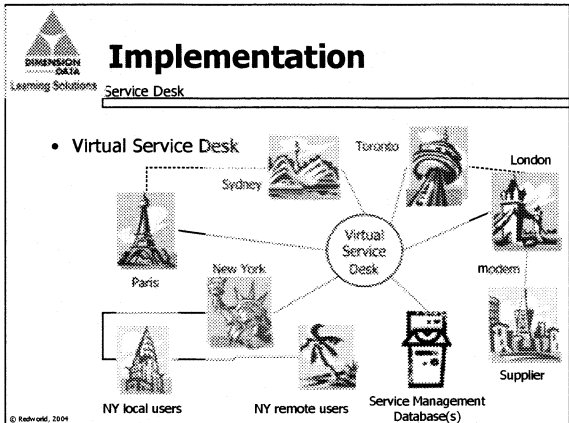
- Local Service Desk

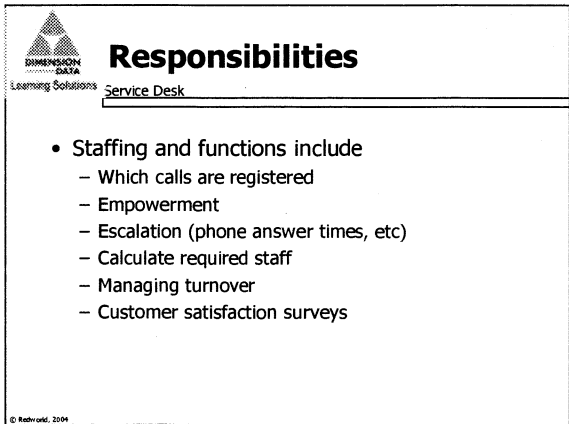


© Redworld, 2004


ITIL Foundation Certificate







ITIL Foundation Certificate




Skills Required

Learning Solutions Service Desk

- Service Desk staff need a different skill set to other parts of the IT organisation
 - Interpersonal skills are essential
 - Active listening
 - Troubleshooting
 - Teamwork
 - Multilingual

© Redworld, 2004




Benefits

Learning Solutions Service Desk

- Improved customer satisfaction and perception
- Increased accessibility
- Better quality and speedier turnaround of requests
- Improved teamwork and communication
- Enhanced focus and proactive approach to managing users
- Improved use of IT personnel and resources
- Reduced negative business impact

© Redworld, 2004



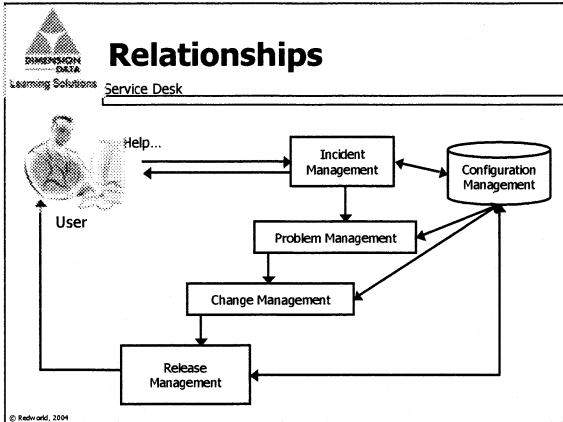
Metrics

Learning Solutions Service Desk

- Phone related statistics
 - Calls per analyst, call length, after call work time, etc.
- Incident management statistics
 - Incidents resolved without escalation, incidents resolved at first contact
- Customer satisfaction statistics
 - Percentage of satisfied customers

© Redworld, 2004

ITIL Foundation Certificate

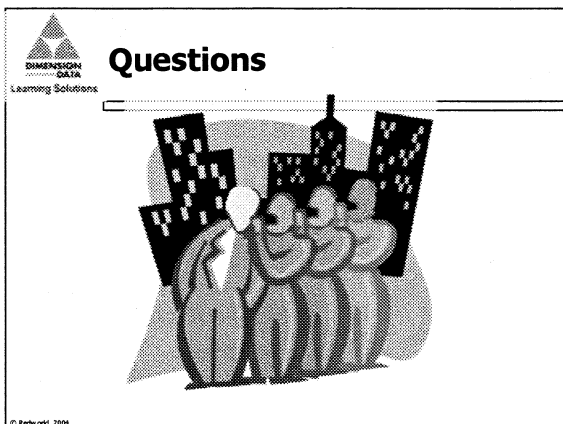


Principles to Apply

Service Desk

- Establish a single point of contact
- Be aware of the balance between technical skill and people skill
- Always imagine how the IT dept appears to a user
- Control expectations and perceptions at all times and whenever possible

© Redworld, 2004



ITIL Foundation Certificate



RELEASE MANAGEMENT



Goal

Release Management

- To take an holistic view of a change to an IT service and ensure that all aspects of a release, both technical and non-technical are considered together

© Redworld, 2004




Definitions

Release Management

- Release - "a collection of authorised changes to an IT Service"
- Release policy determined by the business need

© Redworld, 2004

ITIL Foundation Certificate




Definitions

Release Management

- Release Contents
 - Major s/w releases and h/w upgrades
 - Usually supersedes all preceding minor upgrades
 - Contains large areas of new functionality
 - Minor s/w releases and h/w upgrades
 - Usually supersedes all preceding emergency fixes
 - Contains small enhancements and fixes
 - Emergency s/w releases and h/w upgrades
 - Contains corrections to a small number of problems

© Redworld, 2004




Definitions

Release Management

- Release units
 - The portion of the IT infrastructure that is released together
 - Determine the most appropriate unit level
 - Considerations
 - Resources
 - Ease of implementation
 - Amount of change required
 - Complexity of the interfaces with the rest of IT

© Redworld, 2004



Definitions

Release Management

- Types of release
 - Delta (partial) release
 - Contains only the CIs that have changed
 - Full release
 - All components of the release built, tested, distributed and implemented together
 - Package release
 - Individual releases (Delta, Full, or both) grouped together

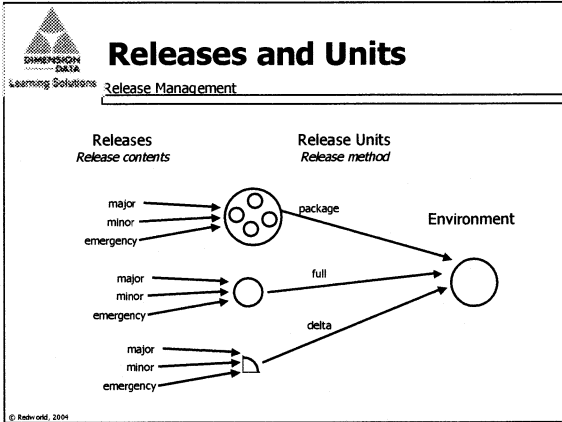
© Redworld, 2004

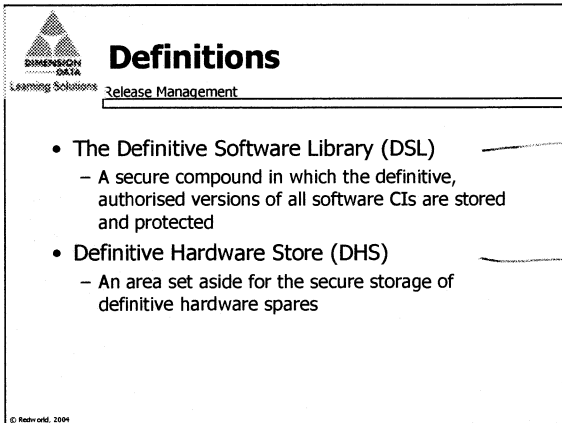
dot release

new version of word

new version of office

ITIL Foundation Certificate

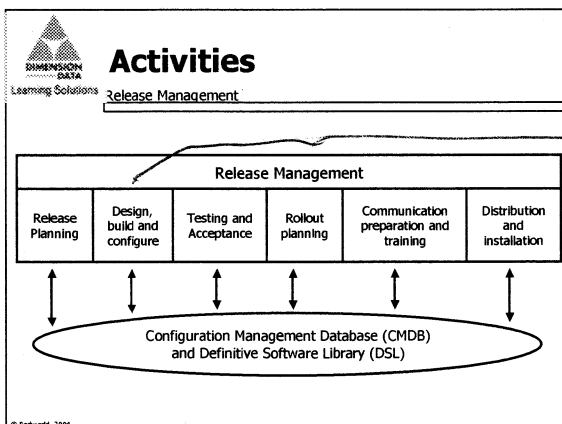




→ DSL a safe with all software

→ DHS a safe with spare keyboards


} owned by release mgt



→ Build or buy software

→ Actual rollout and security mgt

ITIL Foundation Certificate


**Activities**
Learning Solutions

Release Management

- Release Planning
 - Consensus on release contents
 - Agree on phasing
 - High-level release schedule
 - Site surveys to assess existing h/w and s/w
 - Resources available
 - Back-out plans

© Redworld, 2004


→ configuration and audit

**Activities**
Learning Solutions

Release Management

- Designing, building and configuring
 - Re-use standard procedures
 - Compile and link documents (from DSL)
 - Auto install routines
 - OH and S requirements

© Redworld, 2004


**Activities**
Learning Solutions

Release Management

- Release Acceptance
 - Test release (done by the business with IT involvement)
 - Includes back out, install and functional testing
 - Sign off for each stage

© Redworld, 2004

ITIL Foundation Certificate




Activities

Release Management

- Rollout planning

	Release 1	Release 2	Release 3					
Head Office								
Branch 1								
Branch 2								
Branch 3								
Month	1	2	3	4	5	6	7	8

© Redworld, 2004




Activities

Release Management

- Communication, preparation and training
 - Inform all customer liaison staff
 - Meetings/ workshops/ training sessions
 - PR of timing and any constraints
 - Vendor involvement (if not already considered)
 - Any links with other h/w, s/w, processes, etc

© Redworld, 2004




Activities

Release Management

- Distribution and installation
 - Build to test to live environment
 - Ensure procurement, dispatch, storage can deliver all components
 - Security
 - Ensure integrity of software during distribution
 - Check installation completeness
 - Ensure CMDB is informed

© Redworld, 2004

ITIL Foundation Certificate


**Benefits**

Learning Solutions

Release Management

- Greater success rate in the release of hardware and software
- Consistency in the delivery and make up of these releases
- Minimisation of business disruption
- Assurance of quality of hardware and software
- Better expectation setting
- Complete record of change made
- Ability to absorb high rate of change

© Redworld, 2004

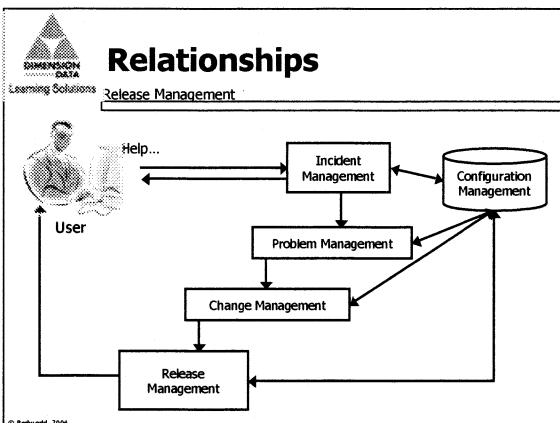
**Metrics**

Learning Solutions


Release Management

- Releases built and released on schedule
- Compliance with legal and licencing restrictions
- Accuracy of distributed materials to remote locations
- Number of unauthorised software and releases
- Timeliness of building, distribution and installation
- IT resources required

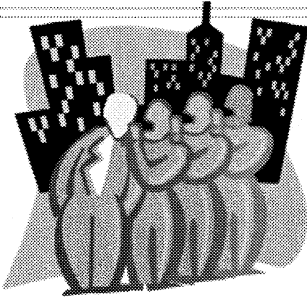
© Redworld, 2004



ITIL Foundation Certificate

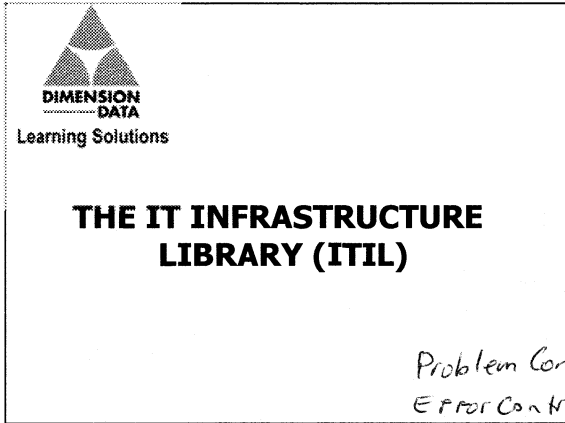


Questions



© Redworld, 2004

ITIL Foundation Certificate



Problem Control → Problem → unknown cause of an incident
Error Control → Known error → known - - - ✓
↓
raise a RFC

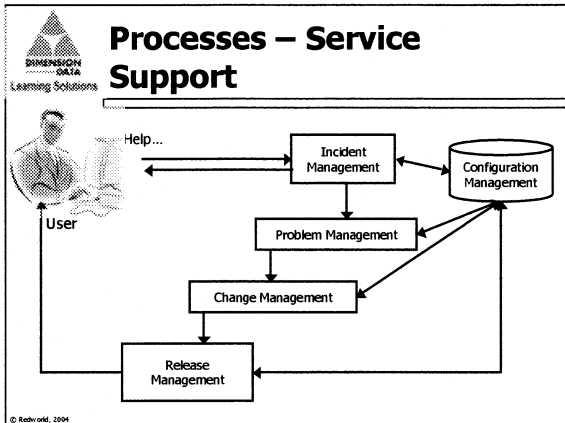
Recording

classification / Initial Support Help

Investigation / Diagnosis 2nd
3rd

Resolution and Recovery now clock stop

Confirm with user before closing



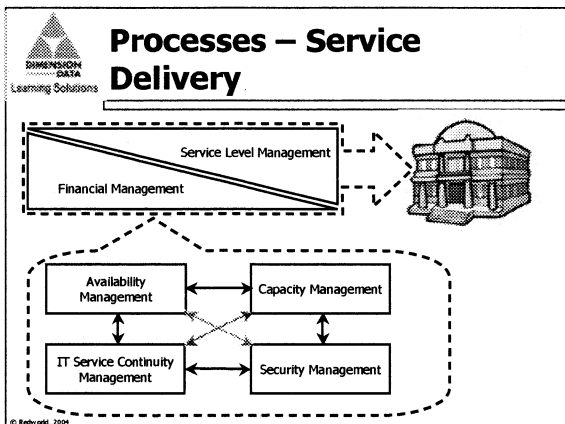
Trend Analysis

Target Preventative Action

major Problem Review

Projected Service Availability

CABEC includes oncall people



ITIL Foundation Certificate



Learning Solutions

SERVICE LEVEL MANAGEMENT



Goal

Service Level Management

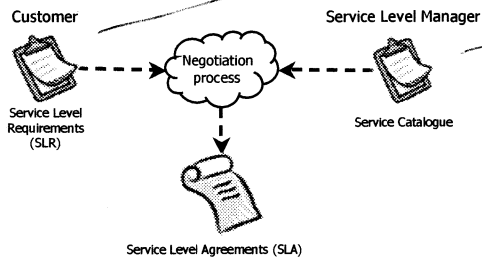
- To maintain and gradually improve business aligned IT service quality through a constant cycle of agreeing, monitoring, reporting and reviewing IT service achievements

© Redworld, 2004



Definitions

Service Level Management



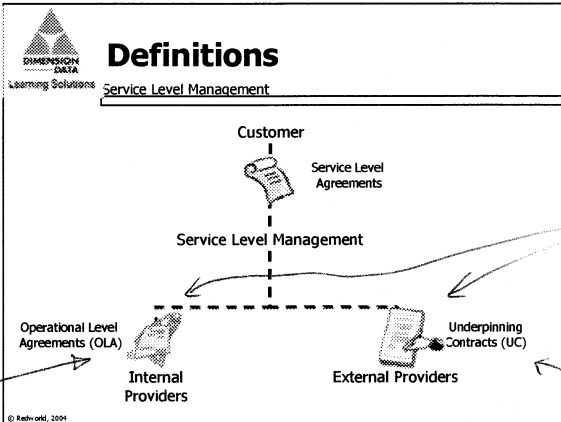
© Redworld, 2004

→ What the customer thinks the ^{need}

→ What I.T. provides and capable of

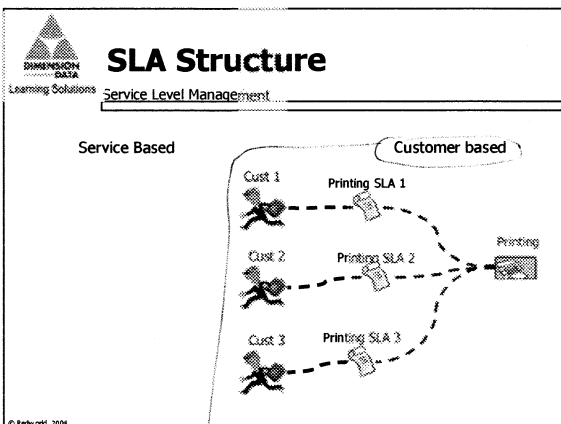
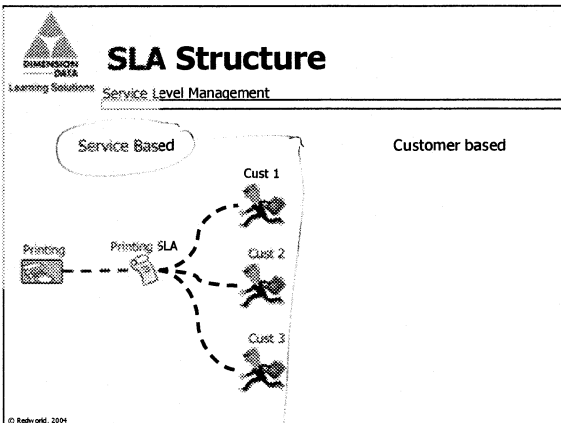
must be agreed
meet all
SMART

ITIL Foundation Certificate



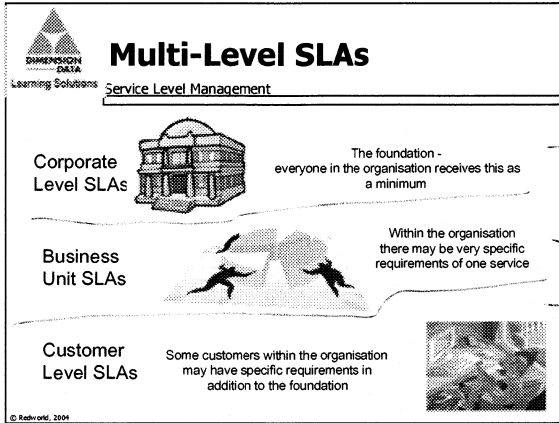
- These must be decided before working on the SLA

Agreement between Funi and IT



A different SLA for each Business Unit

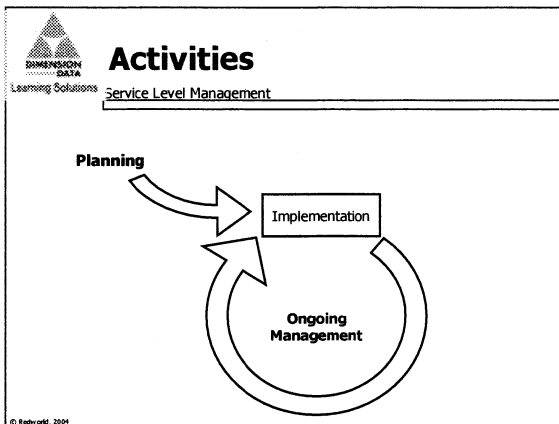
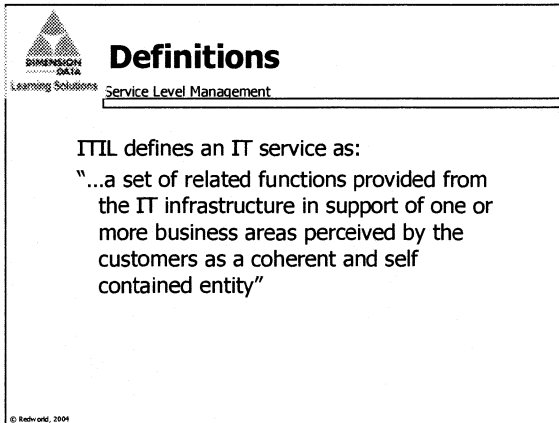
ITIL Foundation Certificate




→ Usual SLA for most people

→ Business or Dept specific

→ VIP's



ITIL Foundation Certificate




Activities

Service Level Management

- Planning
 - Scope, Objective and Mission statement
 - Awareness Campaign
 - Plan monitoring capabilities
 - Establish initial perceptions
 - Review existing UCs and OLAs

© Redworld, 2004




Activities

Service Level Management

- Implementation
 - Establish SLR
 - Produce the Service Catalogue
 - Implement/review UCs and OLAs
 - Draft SLA
 - Choose words carefully and define them clearly
 - Seek agreement (with the right person!)

© Redworld, 2004



Activities

Service Level Management


- Implementation
 - Manage expectations
 - Pilot (in an easy area)
 - Establish monitoring capabilities
 - Define reporting and review periods
 - Publicise the existence of the SLA

© Redworld, 2004

SIP = Service Improvement Program
Coordinated by Service Level Management

SRM = Service Review Meeting

ITIL Foundation Certificate


**Activities**

Learning Solutions Service Level Management

- Ongoing Management
 - Monitoring and reporting (eg RAG charts, Dashboard)
 - Service review meetings
 - Service Improvement Program (SIP)
 - May target user training, systems, or documentation
 - Designed to address any specific issues which are impacting service quality
 - Maintain SLA, OLA, and UC
- Reporting

© Redworld, 2004


Red
orange } indications of status
green }

**Sample SLA Contents**

Learning Solutions Service Level Management

- As a minimum should include:
 - A simple description of the service and the deliverables
 - The agreed service hours
 - User response times, Incident response times and resolution times and response time for changes
 - Service availability, security and continuity targets
 - Customer and provider responsibilities
 - Critical business periods and exceptions

© Redworld, 2004


**Benefits**

Learning Solutions Service Level Management

- IT services designed to meet business requirements
- Improved relationship with business
- Specific targets
- Service monitoring allows weaknesses to be identified
- Clearer understanding of roles and responsibilities
- Better supplier management
- Can provide a basis for charging for services

© Redworld, 2004

ITIL Foundation Certificate




Metrics

Service Level Management

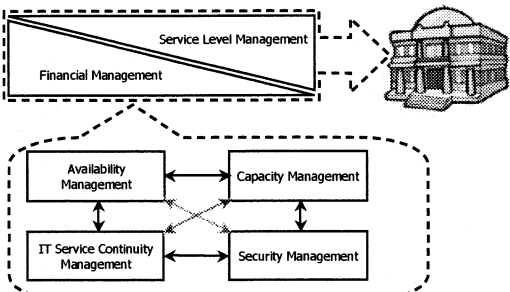
- Percentage of services covered by SLAs
- Percentage of suppliers/ providers covered by SLAs
- Timeliness of review meetings
- Currency of all agreements
- Whether Service Levels are improving
- Whether customer perception stats are improving

© Redworld, 2004




Relationships

Service Level Management




© Redworld, 2004




Questions

Service Level Management




© Redworld, 2004

ITIL Foundation Certificate



**DIMENSION
DATA**
Learning Solutions


FINANCIAL MANAGEMENT



Goal
Financial Management

- To provide cost effective stewardship of the IT assets and resources used in providing IT Services
- In a commercial environment there may also be a statement reflecting the need to make a profit

© Redworld, 2004



Activities
Financial Management

- Budgeting
 - Predicting and controlling the spending of money
- IT Accounting
 - The processes which enable the IT organisations to account fully for the way money is spent
- Charging
 - Processes required to bill customers
- Reporting

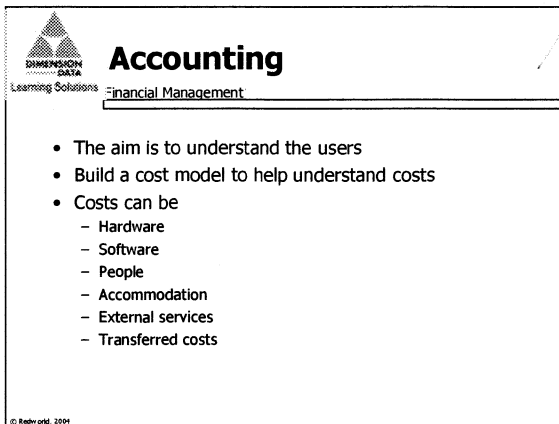
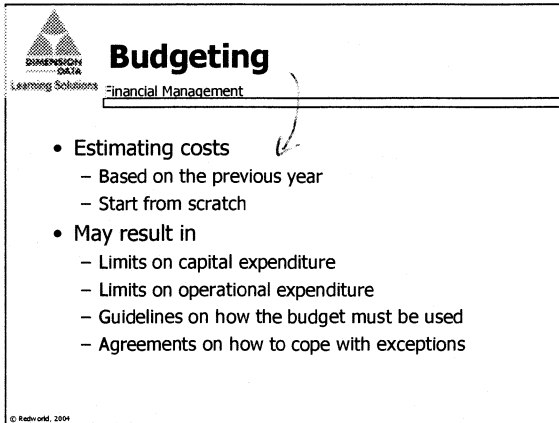
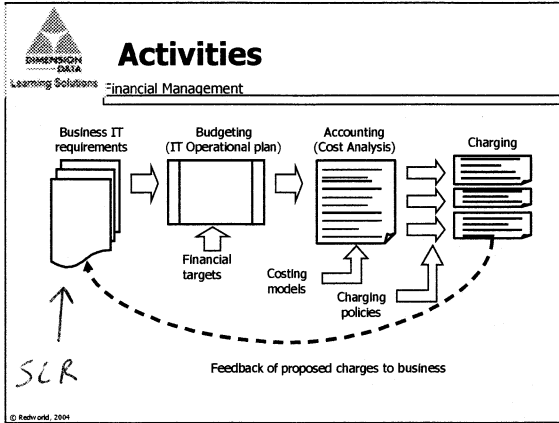
© Redworld, 2004

→ A budget

→ where did the money go

→ optional

ITIL Foundation Certificate



Hardware → Cost Items

Software

People

Accommodation etc

Capital OR Operational → for a sector


Direct OR Indirect → overheads

Fixed OR Variable → fixed costs

Variable → based on usage

stuff that depreciates

ITIL Foundation Certificate




Considerations

Learning Solutions Financial Management

- Depreciation
- Cost units - how do you understand what the users are doing?
 - Activity Based Costing vs. Cost Centre Accounting
- Investment appraisals (ROI - Return on Investment analyses)
- Total cost of Ownership (TCO)

© Redworld, 2004

→ all costs of a charge




Charging

Learning Solutions Financial Management

- Developing the IT Charging policy and scope
- Chargeable items should be
 - Measurable
 - Understandable
- Pricing policy
 - Cost
 - Cost Plus
 - Going rate
 - Market Rate
 - Fixed price
- Billing

© Redworld, 2004

→ recoup costs / plus a fixed profit



Comments


Learning Solutions Financial Management

- Do customers only value what they have to pay for?
- How important is fairness in charging?
- Changes may affect underlying costs
- The responsibility for the processes and tasks may lie with the Finance department
- Costing costs

© Redworld, 2004

→ Very

ITIL Foundation Certificate


**Benefits**

Learning Solutions

Financial Management

- Increased confidence in setting and managing budgets
- Accurate cost information to support IT investment decisions
- A more efficient use of IT resource throughout the organisation
- Increased professionalism of staff within IT

© Redworld, 2004


**Metrics**

Learning Solutions

Financial Management

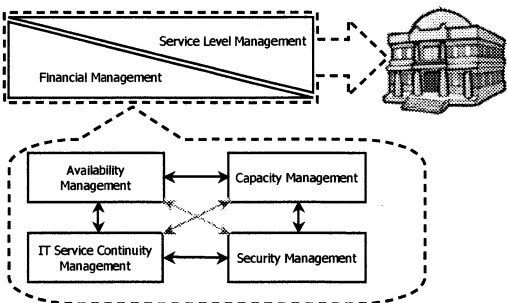
- Accuracy of forecasts
- IT operating within expected budgets
- Reporting produced on time
- Reduction in the number of variances

© Redworld, 2004

**Relationships**


Learning Solutions

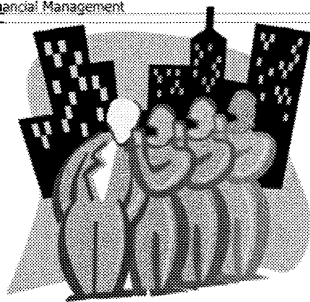
Financial Management




© Redworld, 2004


ITIL Foundation Certificate

 **Questions**
Financial Management



© Redworld, 2004


 **AVAILABILITY MANAGEMENT**

 **Goal**
Availability Management

To optimise the capability of the IT infrastructure, services and supporting organisation to deliver a cost effective and sustained level of availability that enables the business to satisfy its business objectives

© Redworld, 2004

ITIL Foundation Certificate

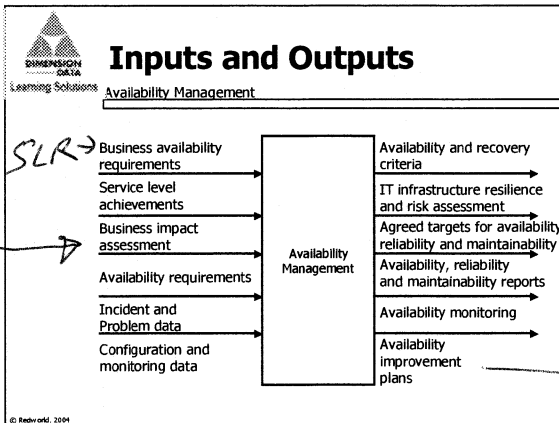
 **Guiding Principles**
Learning Solutions Availability Management

- Availability is at the core of customer satisfaction
- Recognising that when things go wrong, it is still possible to achieve business and User satisfaction
- Improving Availability can only begin after understanding how the IT Services support the business


"The customer doesn't always expect everything will go right all the time, the big test is what you do when things go wrong...occasional service failure is unavoidable"
Sir Colin Marshall - CEO, British Airways

© Redworld, 2004

Business Impact Statement is needed before working on availability



→ For next 12-18 months

 **Definitions**
Learning Solutions Availability Management

- Availability
- Reliability
- Maintainability
- Serviceability
- Security
 - Confidentiality
 - Integrity
 - Availability
- Vital Business Function (VBF)

© Redworld, 2004

→ ability to perform function in the stated time

→ degree of freedom from failure

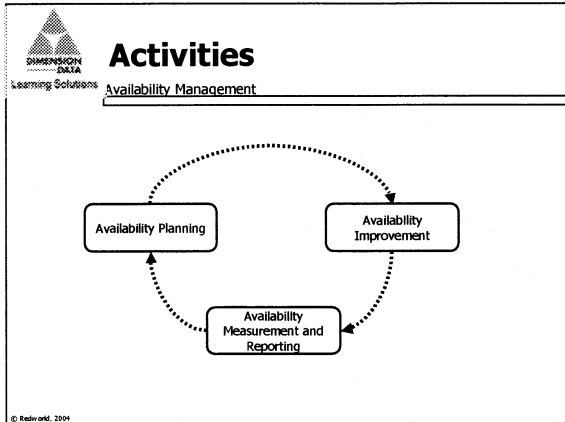
→ internal } ability to retain or restore
→ third party } to operational state

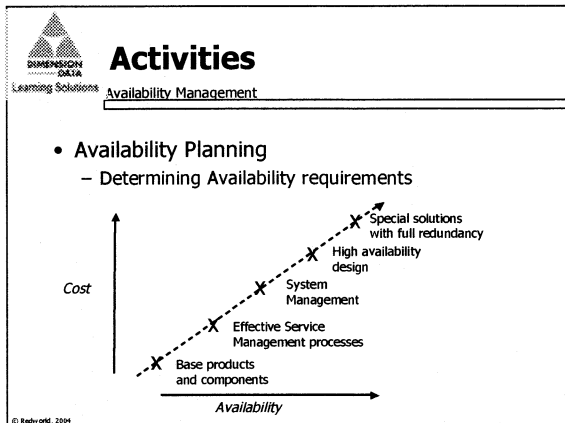
→ confidential - only available to those allowed

→ file is entire

→ information is, virus protection, firewall is there when needed


ITIL Foundation Certificate





- Activities**
Availability Management
- Availability Planning
 - Determining requirements
 - Defining downtime and required service hours
 - Understanding VBF and business impact
 - The cost of unavailability
 - Monetary impact
 - Non-financial impact (reputation, goodwill)
 - Understanding the importance of different work periods
 - Designing for Availability
 - Designing for Recovery
- © Redworld, 2004

ITIL Foundation Certificate


**Activities**

Learning Solutions

Availability Management

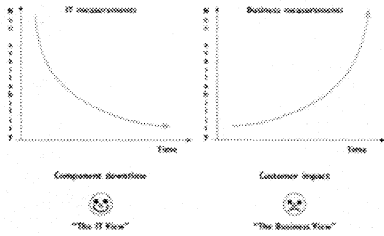
- Availability Improvement
 - Reviewing measurements
 - Availability Management needs to consider availability from an IT Service perspective and from an IT component perspective. These are entirely different aspects. While the underlying concept is similar, the measurement, focus and impact are entirely different

© Redworld, 2004


**Impacts of non-Availability**

Learning Solutions

Availability Management



© Redworld, 2004

**Activities**


Learning Solutions

Availability Management

- Availability Improvement
 - Reviewing unavailability periods
 - Compiling the availability plan
 - Actual vs. agreed
 - Actions taken to address this
 - Details of any changing requirements
 - Forward looking schedule
 - Technology assessment (current and future)

© Redworld, 2004

ITIL Foundation Certificate




Learning Solutions

Activities

Availability Management

- Availability Measurement and Reporting
 - User view influenced by
 - The frequency of the downtime
 - The duration of the downtime
 - The scope of the impact
 - Two approaches possible
 - Impact by user minutes lost
 - Impact by business transaction

© Redworld, 2004



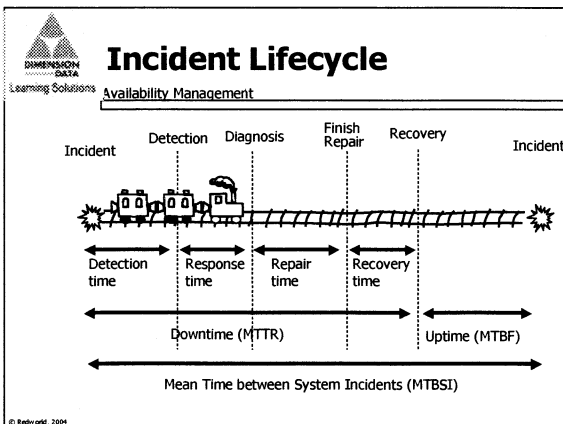
Learning Solutions

Activities

Availability Management

- Availability Measurement and Reporting
 - Some techniques are:
 - Component Failure Impact analysis (CFIA)
 - Fault Tree Analysis (FTA)
 - CRAMM
 - Calculating Availability
 - Calculating the cost of unavailability
 - Systems Outage analysis (SOA)
 - The Incident Lifecycle
 - Technical Observation Post

© Redworld, 2004




Mean Time ^{To} Between Repairs

Between Failures

system Incident

ITIL Foundation Certificate




Incident Lifecycle

Learning Solutions Availability Management

- Mean Time To Repair (MTTR)
Average Downtime
- Mean Time Between Failures (MTBF)
Average Uptime
- Mean Time Between System Incidents (MTBSI)
Average Incident Lifecycle

© Redworld, 2004




Benefits

Learning Solutions Availability Management

- IT Services designed to meet business needs
- Cost justifiable levels of availability
- Ownership and single point of accountability for availability
- Agreed, measured and monitored levels of availability
- Business and User perspective on outages

© Redworld, 2004



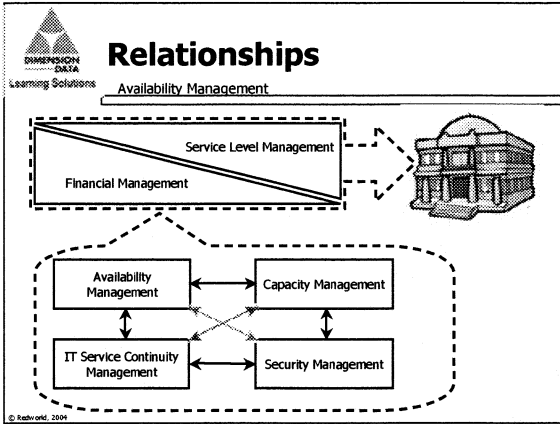
Metrics

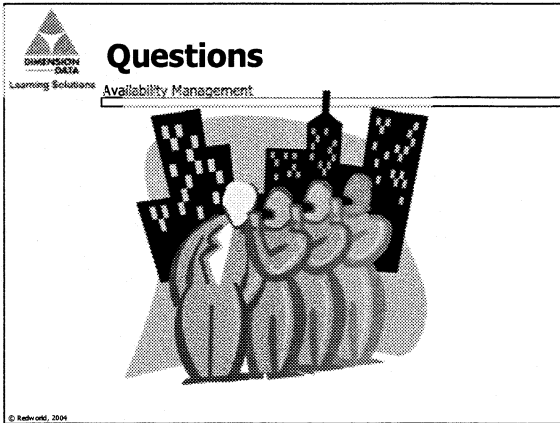
Learning Solutions Availability Management

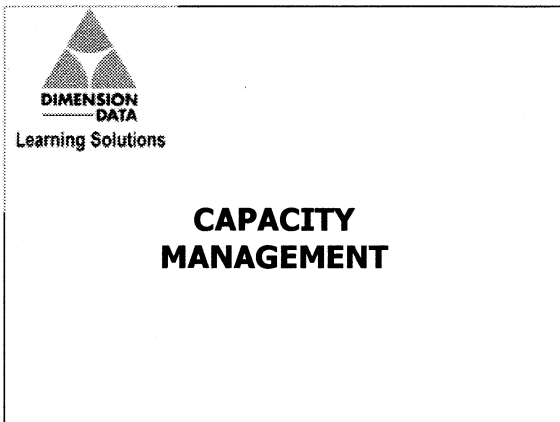
- Cost of unavailability
- Unproductive time
- System outage time
- Reduction or increase over weeks, months or years in availability impact
- Cost to provide availability

© Redworld, 2004


ITIL Foundation Certificate







ITIL Foundation Certificate


**Goal**

Learning Solutions

Capacity Management

To ensure that cost justifiable IT Capacity always exists and that it is matched to the current and future needs of the business

© Redworld, 2004


**Scope**

Learning Solutions

Capacity Management

- Determined by the process, but could include
 - All hardware
 - All networking equipment
 - All peripherals
 - All software → ALL STAFF
- Ultimately driven by the needs of the business

© Redworld, 2004

**Sub-Process Overview**

Learning Solutions

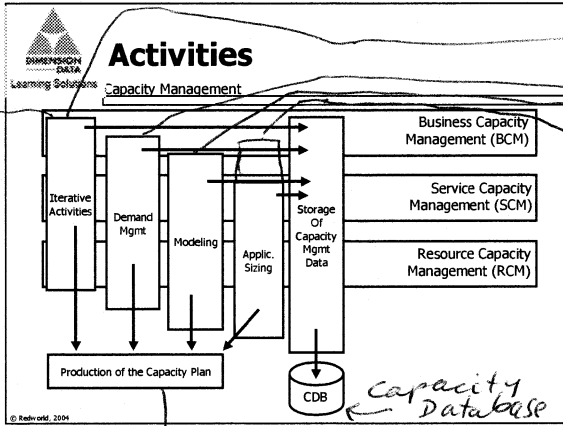
Capacity Management

- Business Capacity Management
 - Future business needs are considered, planned and implemented in a timely manner → Future
- Service Capacity Management → Live
- Resource Capacity Management → Individual bits

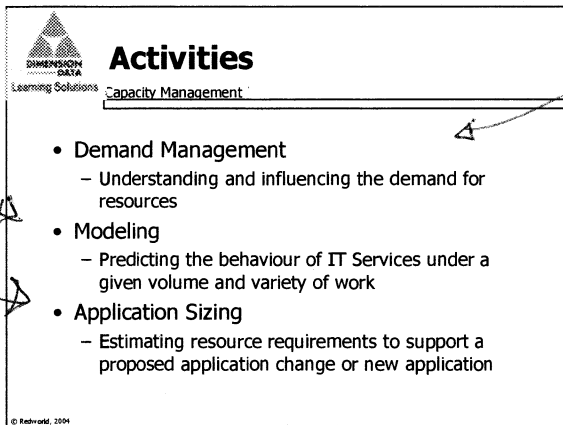
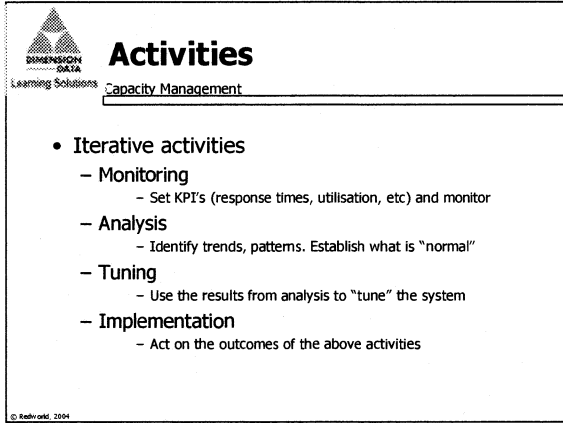
© Redworld, 2004

strategic tactical operational

ITIL Foundation Certificate



↓ How things are now
and in 12-18 months




→ Monitoring, tuning - things that happen

→ Time-based impact on systems

→ what-if 9 to 5 peak times

➤ If a new app, what does it need?


ITIL Foundation Certificate

**Activities**

Learning Solutions
Capacity Management

- Production of Capacity Plan
 - Document current resource usage
 - Forecast the future requirements for the resources based on the analysis of the three sub processes


© Redworld, 2004

**Benefits**

Learning Solutions
Capacity Management

- Increased efficiency and cost savings
- Reduced risk
- More confident forecasts
- Value to applications lifecycle

© Redworld, 2004

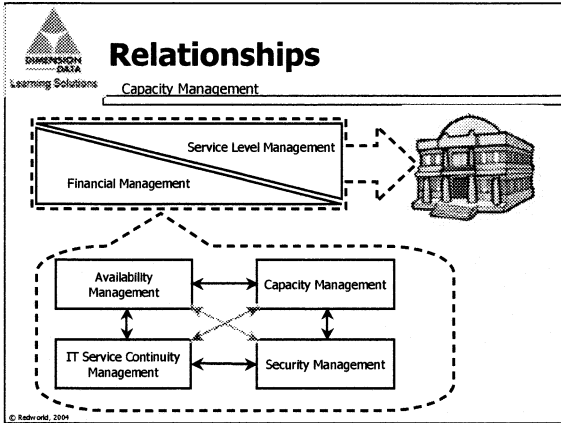
**Metrics**

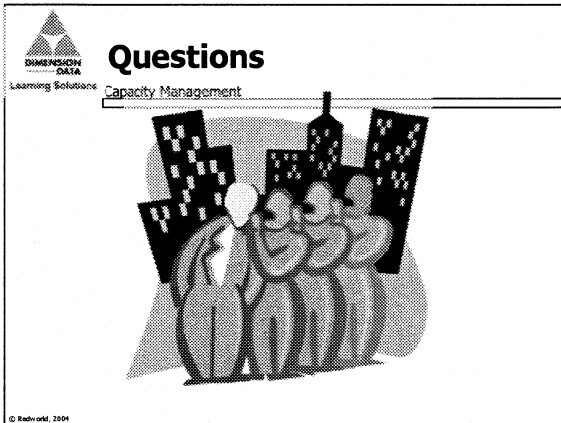
Learning Solutions
Capacity Management

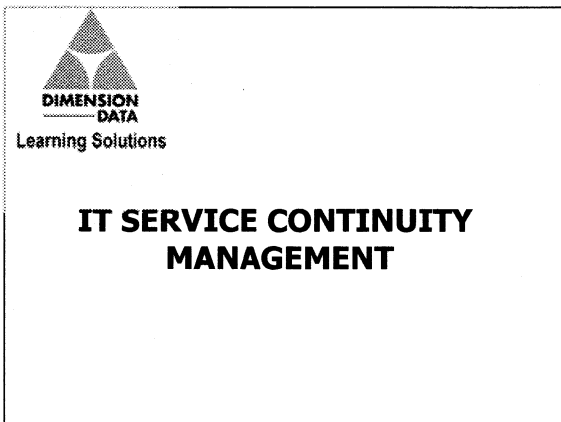
- Production of workload forecasts on time
- Accuracy of business trends
- Timeliness of technology implementation
- Reduction in over capacity
- Reduction in business disruption caused by lack of capacity
- Reduction in incidents due to poor performance

© Redworld, 2004


ITIL Foundation Certificate







ITIL Foundation Certificate


**Goal**

Learning Solutions

TSCM

To support the overall Business Continuity Management process by ensuring that the required IT technical and services facilities can be recovered within required, agreed business timescales

© Redworld, 2004


**Scope**

Learning Solutions

TSCM

- Determined by organisation structure, culture, strategic direction...
 - Organisational dependence on technology
 - Number and location of offices
 - Number of critical business processes
 - Level of services required to support the critical business processes
 - Attitude to risk

© Redworld, 2004

**Activities**

Learning Solutions

TSCM

- Stage 1 Initiation
- Stage 2 Requirements and Strategy
- Stage 3 Implementation
- Stage 4 Operational Management

© Redworld, 2004

Business Continuity Management initiates
I.T. ✓ ✓

Testing and keeping up to date

ITIL Foundation Certificate

Activities

ITSCM

Stage 1
Initiation

Initiate BCM

- IT is *one* of the services on which the business depends - BCM initiates
- Initiation involves
 - Defining a project organisation structure
 - Specifying scope and terms of reference
 - Policy setting
 - Allocating resources

© Redworld, 2004

→ Business Continuity Management

Activities

ITSCM

Stage 2
Requirements and Strategy

Business Impact Analysis

- How much does the organisation stand to lose?
 - Identifying critical business processes
 - Understanding potential damage

© Redworld, 2004

→ same thing as BCM

when a disaster happens the SLA is suspended
The recovery plan will be part of SLA

Activities

ITSCM


Stage 2
Requirements and Strategy

Risk Assessment

- Risk Assessment in terms of
 - Assets
 - Threats – likelihood of the service disruption
 - Vulnerabilities – impact of threat materialisation

© Redworld, 2004

ITIL Foundation Certificate

 **Activities**
Learning Solutions

ITSCM

Stage 2
Requirements
and Strategy

Business Continuity Strategy

- Risk reduction measures
 - Eliminate the SPOFs
 - Stability
 - Security
- Recovery Options
 - See guide

© Redworld, 2004


→ Single Points of Failure

→ Problem Mgt
↳ Availability

Cold = empty room, no gear

Warm = just need to restore

hot = ready to switch to


 **Activities**
Learning Solutions

ITSCM

Stage 3
Implementation

Organisation and Implementation Planning		
Implement Stand-by arrangements	Develop Recovery Plans	Implement Risk Reduction measures
Develop Procedures		
Initial Testing		

© Redworld, 2004

 **Activities**
Learning Solutions


ITSCM

- Organisation and Implementation Planning
 - Who does what and in what order
- Implement Stand-by Arrangements
 - Negotiate with third parties (accommodation, facilities)
 - Purchasing stand by systems
- Develop ITSCM Plan
 - Ensure all activities are performed and so all systems are covered
 - Manage plan distribution

→ for all to see

© Redworld, 2004

ITIL Foundation Certificate

**Activities**


Learning Solutions

ITSCM

- Implement Risk Reduction measures
 - For example UPS, back up power, offsite storage, installation of fault tolerant systems, RAID arrays
- Develop Procedures
 - Documentation of tasks so that any IT literate person is able to undertake the recovery
- Initial testing
 - It is the only way to ensure that the plan really works
 - Partial/ departmental/ phased/ total testing

© Redworld, 2004

training

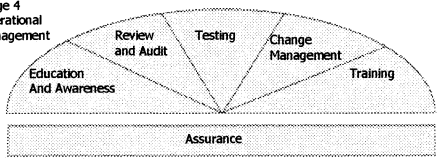
**Activities**

Learning Solutions

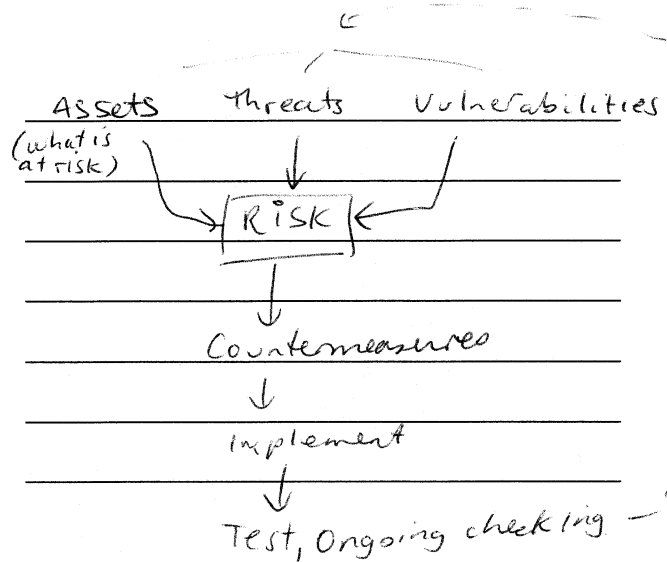
ITSCM


- Ensuring that the ITSCM plan is embedded and maintained

Stage 4 Operational Management



© Redworld, 2004



**Invocation**


Learning Solutions

ITSCM

- Make plans available at home and in the office
- Set deadlines to follow during a disaster
- Decision to invoke should consider
 - Any specific requirements due to current work being undertaken by the business
 - The potential business impact due to the time of the year
 - The extent of the damage
 - The likely length of the outage


© Redworld, 2004

ITIL Foundation Certificate

**Benefits**
ITSCM

- Competitive advantage
- Business relationship
- Organisational credibility
- Regulatory requirements


© Redworld, 2004

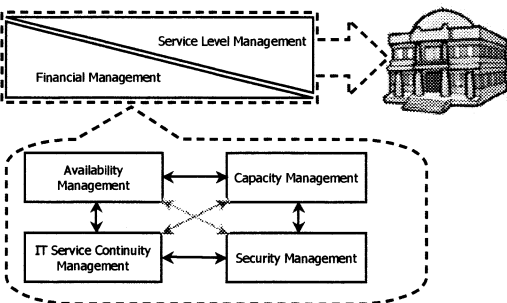
**Metrics**
ITSCM

- Regularity of audits to ensure business can be recovered in agreed timeframes
- Regularity testing
- All agreed targets can be met in a disaster
- Training and awareness of staff
- Regularity of communication with staff
- Results of tests

© Redworld, 2004


> This is the main thing

**Relationships**
ITSCM

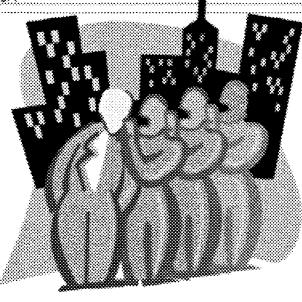


© Redworld, 2004


ITIL Foundation Certificate




Questions



© Redworld, 2004



SECURITY MANAGEMENT




Goal

Security Management

- 1 - To meet external security requirements as stipulated in SLAs
- 2 - To meet internal security requirements to assure the IT service provider's own continuity

© Redworld, 2004

ITIL Foundation Certificate

 **Definition**
Security Management

Information Security Incidents are those events that can cause damage to confidentiality, integrity, or availability of information or information processing. A Security Incident is the materialisation of a threat.


Information security is not a goal in itself but a means of achieving the business objectives

© Redworld, 2004

_____ → and availability


_____ some info is more valuable

_____ than other info

 **Definition** CIA
Security Management

- Confidentiality
 - Protecting sensitive information from unauthorised disclosure or intelligible interception
- Integrity
 - Safeguarding the accuracy and completeness of information and software
- Availability
 - Ensuring that information and vital IT services are available when required

© Redworld, 2004

 **Security Measures**
Security Management

- Physical security measures
- Technical security measures
 - AusCERT report 2003: 42% of Australian organisations suffered hacking attacks. 95% of these had firewalls, 93% had access control technology
- Procedural security measures

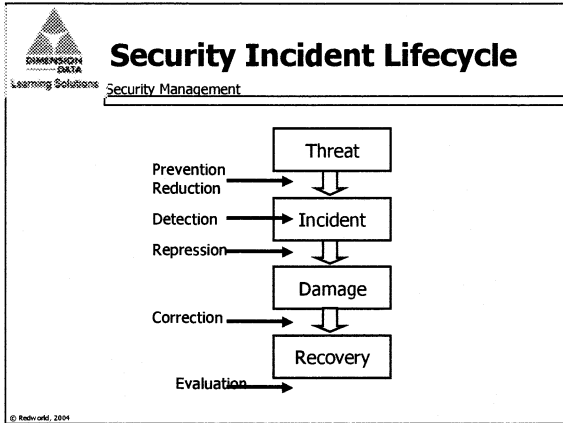
© Redworld, 2004

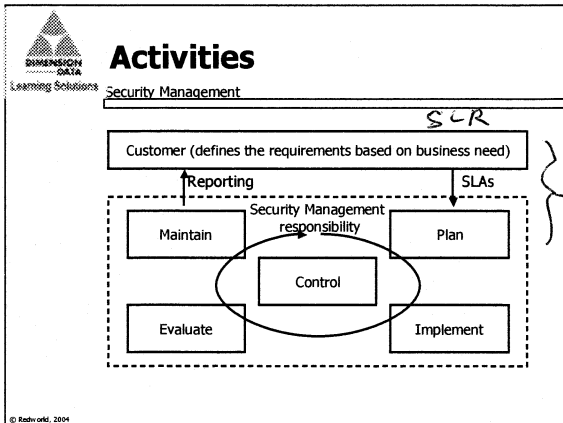
_____ → Doors, guards, cameras etc

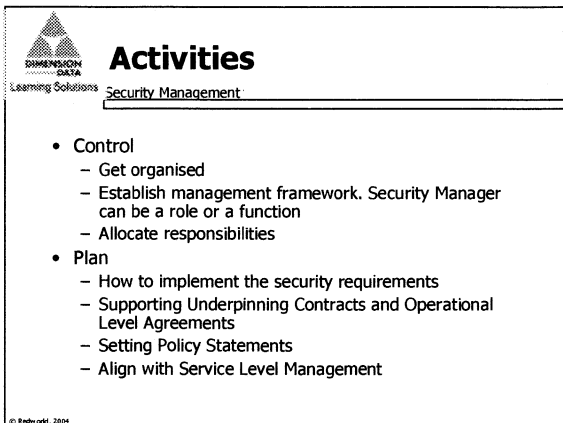
_____ → Firewalls, Encryption, passwords

_____ → Procedures


ITIL Foundation Certificate







ITIL Foundation Certificate




Activities

Learning Solutions

Security Management

- Implement
 - Create awareness
 - Classification and registration
 - Personnel security
 - Physical security
 - Security management of infrastructure components
 - Control and management of access rights
 - Security incident handling and registration

© Redworld, 2004




Activities

Learning Solutions

Security Management

- Evaluate
 - Internal audits
 - External audits
 - Self assessments
 - Based on reported Security incidents
- Maintain
 - Keep security measures up to date
 - Keep security handbook up to date
 - Learn
 - Improve

© Redworld, 2004



Benefits


Learning Solutions

Security Management

- Security level set to meet business requirements
- Possible regulatory requirements
- Assurance to the business
- Confidence in Services provided by IT
- Increased IT credibility

© Redworld, 2004

ITIL Foundation Certificate

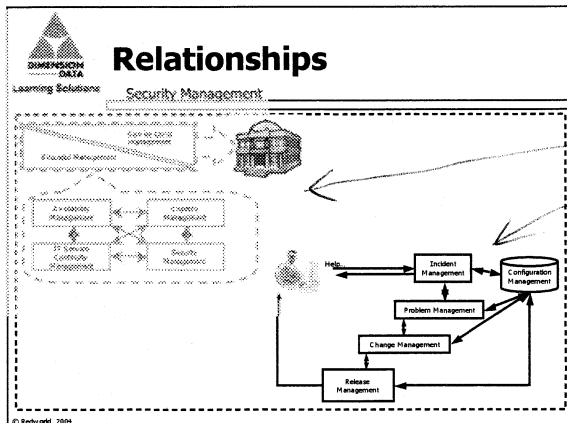


Metrics

Security Management


- Number of security incidents broken down by:
 - Source
 - Reason
 - Resolution
- Number of reviews
- Security issues identified by Problem Management
- Decrease over time in security incidents

© Redworld, 2004



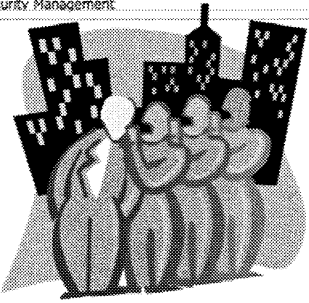
Tactical

operational




Questions

Security Management




© Redworld, 2004

ITIL Foundation Certificate




**THE IT INFRASTRUCTURE
LIBRARY (ITIL)**

Day 3



TOOLS



What are tools about?

"Good people, good process descriptions
and good procedures and working
instructions are the basis for successful
service management"

© Redworld, 2004

ITIL Foundation Certificate



What is available?

- IVR/ VRU /ACD
- Remote control
- System monitoring
- Asset Management
- Service Management
- Change Management
- Voicemail
- Intranet/ internet
- Knowledge bases
- Release and distribution software

© Redworld, 2004



Why might you need tools?

- More sophisticated customer demands
- A shortage of IT skills
- The need to manage a number of vendors
- Company merges
- A change in corporate priorities which rely more heavily on IT
- International standards within the organisation

© Redworld, 2004



Considerations

- The size of your organisation
- Budget
- The level of knowledge of the customer
- The demands of the customer
- The type of support
- The location of the customer

© Redworld, 2004

ITIL Foundation Certificate



Where do we start?

- What is the real business need?
 - "To have great software" is not a business need
 - Would an in house developed tool fit the bill?
 - There are free ones on the internet
- Gather and rate the requirements on the tool (would likes, must haves, etc.)
- Send this information to vendors
- Qualify/ quantify the responses
- Weight each category on the responses to assess value. (Objectivity is vital!)

© Redworld, 2004

What must the tool do?

What extra would you like?

Rate the extras 1 to 10 (most wanted)

Each person rates them, add totals

the specs
Send to vendors, How well?

← more



Tips to remember

- The credibility, history and ongoing viability of the vendor (including market satisfaction)
- Cost - be aware of upfront vs. ongoing costs including the cost for upgrades and support
- Be aware of the issues relating to flexibility, scalability and interoperability (i.e. how well will the new tool work with your existing tools)

© Redworld, 2004




Some notes

- Be aware that a match of >80% between your processes and the product's functionality is very high
- ITIL compliance
- Business driven rather than technology driven
- Budgeting considerations (OPEX vs. CAPEX)
- Training

© Redworld, 2004


ITIL Foundation Certificate




Reference

- www.toolselector.com
- ITIL software support or delivery books
- Service Delivery Tools - an ITIL publication

© Redworld, 2004



IMPLEMENTATION

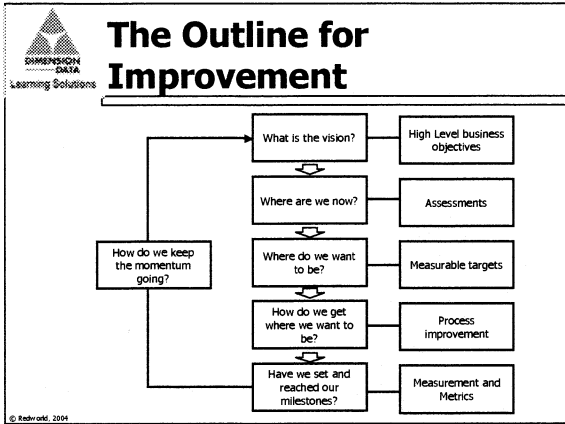



Why

- Justification
- Benefits:
 - Business
 - Financial
 - Employee
 - Innovation
 - Internal

© Redworld, 2004


ITIL Foundation Certificate




Learning Solutions

Step 1 The Vision

"Why are we doing this?"


Learning Solutions

Creating a Vision

- The vision should:
 - Clarify direction
 - Motivate people in the right direction
 - Coordinate actions of different people
 - Outline the view of senior management
- Two questions to help frame the vision
 - Can I explain this in 30 seconds to each stakeholder?
 - Can I answer "WIIFM" to each stakeholder?

© Redworld, 2004

ITIL Foundation Certificate



Step 2 Current State

"Where are we now?"

Vision statement : To be the best ...

IT mission statement : To enable/support
the business to be the best ...

Gap analysis



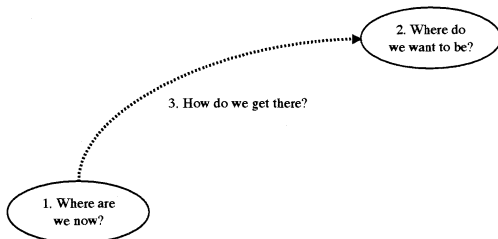
Current State

- The following need to be considered
 - Gap between current and required state
 - Appropriateness of IT goals
 - Current processes and procedures
 - Skill sets and competencies
 - Technology
 - Attitudes and behaviour

→ Gap analysis



Three Questions



ITIL Foundation Certificate

DIMENSION DATA
Learning Solutions

Assessing Current State

example

Configuration Management

Activity: Identification

Providing unique id:	80%
Collecting attributes:	40%
Determining relationships:	0%
Updating CMDB	80%
Total:	50%

Maturity level: 1.5

1. Where are we now?

© Redworld, 2004

DIMENSION DATA
Learning Solutions

Current State: Result

example

1. Where are we now?

© Redworld, 2004

DIMENSION DATA
Learning Solutions

Step 3 Future State

"Where do we want to be?"

ITIL Foundation Certificate



Future State

- Understand stakeholders
- Quick wins
- Measurement
 - Goals
 - Questions
 - Metrics

© Redworld, 2004



Step 4 The Plan

How do we get to where we want to be?




Moving forward

- Start point depends on
 - Outcome of assessments
 - Organisational goals
- Awareness
- Managing organisational change
- Managing cultural change
- Roles and responsibilities
- Training


© Redworld, 2004

ITIL Foundation Certificate

**Implementation Time**
Learning Solutions


- Depends on
 - Process
 - Organisation size, geographic spread, culture, structure, etc.
 - Readiness for change
 - Resources available

© Redworld, 2004

**Phased Introduction**
Learning Solutions

- Never implement all processes simultaneously
- Quick ways to score wins with users
 - Service Desk / Problem Management
 - Service Level Management (e.g. especially Service Catalogue; SLA's)
- Integration - transfer each process to line/ process manager


© Redworld, 2004

**Possible Clustering**
Learning Solutions

- Configuration Management, Incident Management and Problem Management
- Configuration Management, Change Management and Release Management
- Availability and Capacity Management
- Financial and Service Level Management


© Redworld, 2004

ITIL Foundation Certificate

**Implementation Times**
Learning Solutions


- Configuration Management
 - 4 - 12 months from inception to completion
- Incident Management
 - 3 - 9 months
- Problem Management
 - 2 - 4 months for product evaluation and system design
- Change Management
 - 2 - 4 months including the procurement of support tools
- Release Management
 - 1 - 3 months depending on the status and quality of configuration management

© Redworld, 2004

**Implementation Times**
Learning Solutions

- Availability Management
 - 6 - 9 months (for a full implementation)
- Capacity Management
 - 9 - 12 months (for a full implementation)
- ITSCM Planning
 - 6 - 12 months including test
- Financial Management
 - 3 - 6 months depends on the maturity of Service Level Management and Configuration Management
- Service Level Management
 - 2 - 12 months for existing services


© Redworld, 2004

**Process Work Groups**
Learning Solutions

- Translation of ITIL to the organisation
 - Objective and scope
 - Identification of procedures, working out the activities, positioning within organisation
 - Communication with intended worker and clients/users
 - Documentation of results
- Transfer to the operational working level


© Redworld, 2004

ITIL Foundation Certificate



Step 5
Metrics

Are we there yet?




Metrics

- Critical Success Factors and KPIs
- Change Management examples

CSF (one)	KPI (many)
Quick, Accurate change process	- % of backed out changes - % urgent changes
Protection of services	- unscheduled service outages - % changes causing incidents

© Redworld, 2004



Step 6
Looking Ahead

How do we keep the momentum going?

ITIL Foundation Certificate



Continuous Improvement

- Consolidate changes and produce more change
- Institutionalise changes
- Monitoring and reviews
- Reinforce business and IT alignment continuously
- Knowledge management

© Redworld, 2004

The Hitchhiker's Guide to ITIL



It Depends!

The most comprehensive ITIL Foundation Exam preparation guide in
3,567,852,985,562.752 pages

Table of Contents

1	PREFACE	5
2	INTRODUCTION.....	9
3	CONFIGURATION MANAGEMENT	15
3.1	GOAL	15
3.2	TERMINOLOGY AND DEFINITIONS	15
3.3	ACTIVITIES	16
3.4	BENEFITS.....	18
3.5	PROBLEMS	19
4	SERVICE DESK	20
4.1	GOAL	20
4.2	TERMINOLOGY AND DEFINITIONS	21
4.3	ACTIVITIES	22
4.4	BENEFITS.....	23
4.5	PROBLEMS	24
5	INCIDENT MANAGEMENT.....	25
5.1	GOAL	25
5.2	TERMINOLOGY AND DEFINITIONS	25
5.3	ACTIVITIES	27
5.4	BENEFITS.....	29
5.5	PROBLEMS	30
6	PROBLEM MANAGEMENT	31
6.1	GOAL	31
6.2	TERMINOLOGY AND DEFINITIONS	31
6.3	ACTIVITIES	33
6.4	BENEFITS.....	35
6.5	PROBLEMS	36
7	CHANGE MANAGEMENT	37
7.1	GOAL	37
7.2	TERMINOLOGY AND DEFINITIONS	37
7.3	ACTIVITIES	38
7.4	BENEFITS.....	42
7.5	PROBLEMS	43
8	RELEASE MANAGEMENT	44
8.1	GOAL	44
8.2	TERMINOLOGY AND DEFINITIONS	44
8.3	ACTIVITIES	46

8.4	BENEFITS.....	49
8.5	PROBLEMS	50
9	SERVICE LEVEL MANAGEMENT	51
9.1	GOAL	51
9.2	TERMINOLOGY AND DEFINITIONS	51
9.3	ACTIVITIES	55
9.4	BENEFITS.....	60
9.5	PROBLEMS	61
10	FINANCIAL MANAGEMENT FOR IT SERVICES	62
10.1	GOAL.....	62
10.2	TERMINOLOGY AND DEFINITIONS	62
10.3	ACTIVITIES	66
10.4	BENEFITS	68
10.5	PROBLEMS.....	69
11	AVAILABILITY MANAGEMENT.....	70
11.1	GOAL.....	70
11.2	TERMINOLOGY AND DEFINITIONS	70
11.3	ACTIVITIES	73
11.4	BENEFITS	75
11.5	PROBLEMS.....	76
12	CAPACITY MANAGEMENT	77
12.1	GOAL.....	77
12.2	TERMINOLOGY AND DEFINITIONS	77
12.3	ACTIVITIES	78
12.4	BENEFITS	82
12.5	PROBLEMS.....	83
13	IT SERVICE CONTINUITY MANAGEMENT	84
13.1	GOAL.....	84
13.2	TERMINOLOGY AND DEFINITIONS	84
13.3	ACTIVITIES	86
13.4	BENEFITS	89
13.5	PROBLEMS.....	90
14	SECURITY MANAGEMENT.....	91
14.1	GOAL.....	91
14.2	TERMINOLOGY AND DEFINITIONS	91
14.3	ACTIVITIES	94
14.4	BENEFITS	96
14.5	PROBLEMS.....	97

15	ACRONYMS USED	98
-----------	----------------------------	-----------

1 PREFACE

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

It is not the strongest of the species that survive, or the most intelligent, but the one most responsive to Change.

Charles Darwin

It Depends!

This document can be used as a reference guide or study tool when preparing for the Information Technology Infrastructure Library (**ITIL**) Foundation Exam. It can also be used as paperweight, wall-paper, campfire fuel, and I'm sure all the secrets of the Multiverse will be hidden in the text in some sort of alien language – you just have to look long enough – I mean really, really l... o... n... g...

Some organisations also refer to the ITIL Foundation Exam as ITIL Essentials Exam or ITIL Fundamentals Exam. Fortunately you will not need to stick a Babel-fish in your ear to understand the ITIL language, although they are very nice creatures, just a bit temperament-full¹. This document will be clear, concise and mainly in English. Translations in Martian, Venusian, and other more Earth like languages will be available on request. Translation time is exactly 10^{google} years and all requests for translation will need to be submitted in tenfold.

This document is not intended to cover the ITIL Foundation course as provided by DIGANO or any of its partners, although it is getting pretty close and better each time it is revised (also a bit longer each time – and hopefully also funnier). You will need to follow the classroom based course to reap the full benefits that such a training session has to offer. ITIL is about People, Processes and Products (the **triple-P balance**) and you won't meet other people or hear the stories of their products by reading this document only.

A full description of ITIL is described within the ITIL Service Support book, the ITIL Service Delivery book and the ITIL Security Management book as provided by the Office of Government Commerce (**OGC**). Other ITIL volumes (there are 9 volumes in total) are also available, but fall outside the scope of the Foundation course and therefore also outside the scope of this document.

¹ The Babel fish is explained in the Hitchhiker's Guide to the Galaxy by Douglas Adams

In the not too distant future a more comprehensive summary of ITIL will be provided for those self-masochists following the full ITIL Master's course. This document is due to be released mid 2006, although we keep all rights to delay this release date. Restaurants, lots of wine, beer and fancy dinners are also mighty important!

Please realise that DIGANO is a relatively new organisation, has only one crazy employee (the author), and can only work 24 hours a day. Occasionally where holes in the space-time continuum allow this 24¼, but not a minute more! A request to clone the author has been submitted, but unfortunately was denied due to a prematurely discovered ITIL-insanity syndrome. That is what too much ITIL does to people nowadays! Ouch!

This document contains tips, tricks, resources and templates that can be studied in more detail at a place and time convenient to the reader – preferably on or near the beach. It can be used as a study-tool or future reference. At some stage this document, used together with DIGANO's other online resources should be sufficient to pass the ITIL Foundation Exam. More and more feedback proves this is already the case. As the author, I do not think there is enough online material available as yet, but with your support and feedback I am sure this will be possible to accomplish in the not too distant future (early 20006, oops I meant to say 2006). This document is a "blarticle" and as such dynamic – it seems to grow continuously and sometimes even makes spontaneous genetic changes.

All templates in this document that are labelled 'template' are freeware and can be used, changed and reproduced by any person or organisation free of charge. Applications to reuse, reproduce or republish any other material in this publication should be addressed to DIGANO.

Please also note that the ITIL-brand is owned by the Office of Government Commerce. I have no intention to copy what has already been written in their manuals, but I would like to enable you to learn, understand and adopt ITIL in less than a 1000 pages, and using a less formal (sleep-inducing) language. As such, I still acknowledge OGC for their incredible effort to get the ITIL knowledge and experience together in a relatively small library of books.

This document will use shaded boxes (see example below) to provide tips, tricks, resources and references to the reader. Readers are invited to send DIGANO additional information that can be used in future releases of this document. Its intention is to become an up-to-date resource for all those that are interested in the topic of ITIL or more generically in the topic (IT) Service Management with the main purpose passing the Foundation Exam. This version is available in PDF format from DIGANO's website and questions and/or suggestions can be addressed to the author marco.cattaneo@digano.com.au. This document must not be used by training organisations other than DIGANO, unless they have received written approval from DIGANO.

Please check the website regularly for updated, even more surrealistic, versions of the Hitchhiker's Guide to ITIL, dubbed H₂I. This document will be fully revised when ITIL v3

(nicknamed ITIL PBNR) will become available. Oh sorry, ITIL PBNR that stands for "ITIL Point Beyond No Return". That's how good it will be – according to some!

The following resources can, and should, be used as additional literature when studying for the ITIL Foundation or other ITIL related exams:

Resource: Best Practice for Service Support – ISBN 0 11 330015 8

Resource: Best Practice for Service Delivery – ISBN 0 11 330017 4

Resource: Security Management - ISBN 011330014X

All books can be purchased directly from the itSMF (IT Service Management Forum) website with a nice discount if you're/become a member. You must become a member of the itSMF and join the dark-side. DIGANO is also a member and uses a lot of the ITIL Force.

In the next sections we will introduce ITIL. The remainder of the document will then discuss the individual process areas into more detail, although not as detailed as the original ITIL books (or CD-Roms).

When the author, who is currently brushing his teeth, and dripping toothpaste, over his keyboard, finds some extra spare time, more paragraphs will be added on topics such as Costs, Inputs, Outputs, Vision, Mission, Cultural Change, Tools, ITIL Implementation, Leadership, Managing a Successful ITIL project, Maturity Assessments, and little green bugs that crawl under your bed at night.

When you follow training with DIGANO or any of its partners, you also create more opportunity for DIGANO to add more contents to the online library, and indirectly you're supporting the World Wildlife Fund for Nature (WWF) at the same time (see DIGANO's website). Those little green bugs need to be preserved forever!

I'm very grateful to the little ants that are crawling over my desk right now, although I'm not quite sure why and would also like to express my gratitude to **Marcus Binet**, **Don McEwan**, and **Erin Casteel** for their enormous effort deciphering and quality assessing my cryptic sometimes even alien language and for adding their mega-trillions of years of IT Service Management knowledge, skills and attitude to this guide.

Happy reading and don't forget:

ITIL is VITIL (doh – I meant VITAL)!

You will be ITIL-ised², resistance is utterly and completely futile.

You will be infected with the highly contagious ITIL-itis virus.

Life is too short as it is, so let's make it a bit of fun whilst we can!

Again many happy (or not so happy, as after all, this is a management course) reading hours,

Marco Cattaneo

DIGANO
Accredited ITILiser!

² Also read the author's article: "To ITILise: Managing your Infrastructure Effectively & Efficiently.

2 INTRODUCTION

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

The **Information Technology Infrastructure Library (ITIL)** is a set of books (hence library) that focuses on the management of an IT infrastructure (bits and pieces that process zeros and ones). It is not more and it is not less than a big, mind-boggling big set of books, hence library.

Definition of a *Library*: “A place in which literary and artistic materials, such as **books**, periodicals, newspapers, pamphlets, prints, records, and tapes, are kept for reading, reference, or lending.”³

The initial library (ITIL v1) that consisted of dozens of books was published late 80s, with a lot of support from large IT companies. The newer revised library (ITIL v2) was released late 90s and currently has 9 volumes in it, although volume 9, the 2nd Business Perspective volume, still hasn't come out of print. The target release date for ITIL v3 is set to late 00s (2007/2008) and will hopefully only contain one volume, although it's everyone's guess on how many pages this volume will end up with. Hopefully ITIL v3 will fit on three DVDs (blue-laser), maybe two if we're lucky. The new ITIL library will be published online/electronically before it will be released in hardcopy – this to ensure that the hardcopies will end-up in the highest (read error-free/typo free) quality possible.

It seems that ITIL revisions have a 10 year refreshment cycle, which means that studying and certifying in ITIL creates long term business and personal benefits, whereas studying for an MCSE or similar technical certification scheme has a lifetime of roughly 18 months (if not superseded earlier). This makes answering the question: “ITIL **WIIFM** (What's In It For Me)?” relatively easy.

ITIL is developed and maintained by the Office of Government Commerce (**OGC**), located in the United Kingdom. Initially it was developed as a guidance/framework to support UK government in doing their business more successfully using fewer resources. It was such a success in government that it was soon to become adopted by private organisations and is currently used worldwide as the most successful *guidance* to setup and maintain IT infrastructures. Before OGC was known as OGC it was known as **CCTA**; the Central Computing and Telecommunications Agency. Therefore the older ITIL books will carry the CCTA name and not the OGC name. Please realise it is the same organisation!

ITIL is a **framework**; it is not and will never become a methodology. It is a flexible, tailorable, twistable, bendable, tweak-able, customisable (I ran out of words here) set of

³ <http://www.dictionary.com>

guidelines. It is based upon proven **world best practices**. Even if you decide to use only one third of a page of one of the many ITIL volumes to make a small Business or IT improvement, than you are still using ITIL. ITIL is not about quantity, ITIL is about quality! It's not a bible; it's a tool to success!

There is no such thing as *the* ITIL implementation! An ITIL implementation will depend on many factors such as politics, stakeholders, support, complexity, size, attitude, geography, technology, people, goals, time, commitment, vision, involvement, quick wins, roadblocks, resources available and much more within an organisation. In other words: **It depends!** Where Douglas Adam[†] uses the words "DON'T PANIC!" on his Hitchhiker's Guide to the Galaxy, I would like to print or at least you, the reader, to visualise the words "**IT DEPENDS!**" on a sparkling cover of this Hitchhiker's Guide to ITIL. Don't expect ITIL to be your own personal Oracle, as it will not give you all the answers you'll be looking for. ITIL is relatively high-level – the detailed design and implementation is your own challenge!

Just like a house needs sewerage, foundation, walls and a roof. Information Technology (IT) needs planning, support and proper understanding of services that are delivered to the customers and users. Although all houses need a front-door (Service Desk), you can still decide on the colour, material and size of that door. In other words, ITIL gives you the framework/skeleton and you fill in the details based upon your own specific requirements and preferences. Some organisations like Microsoft have already filled in many of these details for a specific Microsoft Windows environment and have called their specific ITIL interpretation the Microsoft Operations Framework (MOF). Nowadays most large IT organisations offer their tailored version of ITIL as one of their products. Please realise that these tailored versions will not always match your specific needs and may not be suitable in multiplatform environments.

ITIL puts a lot of emphasis on using the right **terminology** and **definitions**. It makes it a lot easier if we all speak the same language. There is a huge difference between Customers and Users, and Incidents and Problems. We do need to get the terminology and definitions right in order to prevent Babylonian speech. We don't have a universal translation device, such as the Babylon fish you can stick in your ear, or some high tech Star Trek device that will translate from Martian into Venusian language, so we must somehow agree on the language we use within IT management space. This is exactly one of the many spots where ITIL fits in, and it might be the very reason why you are reading this manual at this very moment in space and time. This guide will contain the most important ITIL terminology and definitions you will need to know of to pass your ITIL Foundation Exam. Let's all start to communicate more effectively and efficiently by using the same language: the ITIL language.

A clear distinction is made in ITIL between Customers and Users.

- ☉ **Customers** are typically the people who will be funding the IT Services and often they will be signing off the agreements with IT on the delivery of those services.
- ☉ **Users** are typically the people using the services to support their daily business

activities. The terminology End-Users can be used interchangeably with Users.

ITIL is process based, not functional. Processes are by definition **cross-functional**. When establishing processes people in various functions (business units) will have to come down from their ivory towers and will have to start working together to make something happen (I.e. manufacturing an airplane).

Definition: A process is a set of interrelated activities, sub-processes (**or stages**)⁴ to achieve a common goal.

⁴ Stages are added by the author to accommodate for the process IT Service Continuity Management, as this is the terminology used under this specific process – it is not part of the official ITIL definition, but it should be!

The following ITIL processes will be discussed in this summary:

Service Support (operational) processes:	Service Delivery (tactical) processes:
Incident Management	Service Level Management
Problem Management	Financial Management for IT Services
Change Management	Availability Management
Release Management	Capacity Management
Configuration Management	IT Service Continuity Management

The Service Desk is a function, not a process, and typically performs activities for one or more Service Support processes. In most organisations the Service Desk will have the responsibility to log and record all Incidents (calls from Users). The Incident Manager, who is the process owner of the Incident Management process, will ensure that the Service Desk logs and records the Incidents with the right amount of detail and the right data.

The Security Management process has interfaces with both Service Support processes (the operational processes) and Service Delivery processes (the tactical processes). Security Incidents will need to be recorded (operational), but Security also needs to be planned properly to ensure that the right level of Security is provided to protect the business' assets (tactical). In other words: "Security Management exists everywhere!"

Resource: The ITIL Rocket. DIGANO's model visualising a hierarchy of the ITIL processes.

All ITIL processes have strong relationships with all the other ITIL processes. Synergy will occur when these relationships are fine-tuned to the specific conditions of the organisation where ITIL is implemented. None of the ITIL processes will perform optimally in isolation: the sum of all processes integrated is larger than the all individual processes implemented in isolation. So, ITIL is about creating **synergy**!

The ITIL processes are like tectonic plates. Sometimes they nicely connect with each other, sometimes they overlap without too much friction and sometimes they collide with much friction, and cause an organisational earthquake. By assigning the proper roles and responsibilities to the appropriate people and exercising monitoring and control, friction can be kept to a minimum. However an organisation without friction doesn't exist – that's for fantasy stories! It is the ability to recognise friction and dealing accordingly with it that separates an effective and efficient organisation from a non-effective and inefficient organisation.

Effectiveness: The ability to achieve outcome! **Doing the right things!** Selling a blue car to someone who is actually after a pushbike is not very effective.

Efficiency: Achieving an outcome using minimal resources (time, money, and people)! **Doing things right!** Sending an email to someone is typically a lot more efficient (faster) than using the manual and labour intensive postal services (hence the terminology snail-mail).

ITIL is all about **increasing quality of services, decreasing the costs of delivering these services and ensuring that the services are aligned with the business needs and (future) business direction.** Why so many words in bold? Well, this is in a nutshell what ITIL all comes back to, it is fundamental, it is core to ITIL, and written between all the lines in the ITIL books! It is also the reason why so many organisations worldwide have embraced ITIL and are currently reaping the benefits.

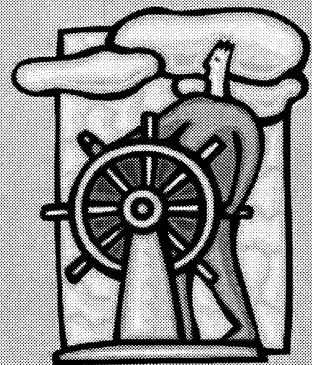
IT Service Management



Increasing
Quality



Reducing
Costs



Aligning IT and
the Business

© DIGANO 2006

Can you afford not managing your IT infrastructure?

The continuous improvement of quality of services is safeguarded when Dr. W. Edwards Deming's model of continuous quality improvement or total quality management (TQM) is followed. Dr. W. Edwards Deming[‡] (<http://www.deming.org>) tells us we should **Plan** first, **Do** the things we have planned, **Check** (monitor/measure) whether or not we're doing the right things (effective), and things right (efficient), and if not take appropriate corrective action (**Act**). These four key activities (Plan, Do, Check and Act) should be carefully monitored by internal (self-assessments) or external quality reviews (**Quality Assurance**). Formalised QA for ITIL is known as BS15000 (UK), AS8018/BS15000 (Australia) and ISO20000 (Global).

Short-term, the road to "pure" ITIL can be perceived to be too time-consuming, expensive, bureaucratic, curved, filled with roadblocks and painful, but medium to long-term it will always turn into a success where all the painful obstacles will belong to history and real benefits will be visible, measurable and tangible, to all involved. When embarking on an ITIL journey, it is not the cobbled road we travel, but the divine destination that should drive our motivation and passion. Sounds a bit heavy doesn't it? Just start to use ITIL and you will see what's meant with this statement.

3 CONFIGURATION MANAGEMENT

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

3.1 GOAL

The **goal** of Configuration Management is to **track** and **control** all IT related infrastructure components and to **provide information** on these components to the other parts of IT and the business.

3.2 TERMINOLOGY AND DEFINITIONS

The Configuration Management process manages the *logical* informational aspects of all components whereas Release Management manages the *physical* components. Information about all of all these components, referred to as **Configuration Items** (CIs) within ITIL, will be stored in the **Configuration Management Database** (CMDB).

Although the financial asset register might have an overlap with the CMDB, in the form of financial data, the CMDB typically contains more detail and also contains relationships between all the CIs, whereas the financial asset register typically looks like a simple spreadsheet.

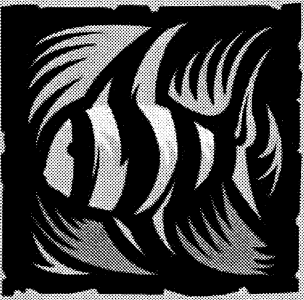

3.3 ACTIVITIES

There are basically six activities within Configuration Management that you will need to know of for the exam. These activities can be memorised using the mnemonic PICSAR.

Activities

- **P**lanning
- **I**dentification
- **C**ontrol
- **S**tatus Accounting
- **A**udit & Verification
- **R**eporting

From **P I X A R** To **P I C S A R**



© DIGANO 2006

The activities are:

- **Planning:** The activity of initialising the process. A process owner needs to be assigned, goals need to be agreed and measurements for success need to be set. Resources (time, people, and money) need to be allocated and a decision has to be made on which CIs need to be tracked (**scope**), how much detail we need to know for each item (**level of detail**), the types of relationships we need to identify (**relationships**) and the types of unique data that we are going to store on each CI (**attributes**). A CI can be seen as a record in a database, the attributes can be seen as the fields of a record.
- **Identification:** The CIs will need to be identified and attributes of the CIs stored into the CMDB. All CIs will also need to be labelled (tagged) in a consistent and logical manner. The use of Radio Frequency Identifiers (RFIDs) might be a nice new technology rather than using bar-codes. The use of automatic inventory tools could be

an efficient way to populate the network-attached devices, but realise that non-network-attached devices also represent value. Your warehouse might be filled with spare workstations and servers.

- ☯ **Control:** All CIs that are added, modified or deleted to and from the infrastructure need to be kept under strict control; otherwise the data kept in the CMDB becomes useless. It is recommended to use Change Management as the controlling process. In other words: Thou shall not make any change to a CI without a properly authorised Request for Change (RFC) form. Policies need to be in place to prevent (or at least minimise) unauthorised modification of the CMDB.
- ☯ **Status Accounting:** This activity will track where the CI is in its own specific lifecycle. The lifecycle of a CI starts when you formally place an order for the item, and ends the moment the item is formally disposed of. The item might be “on order”, “in test”, “operational”, “in archive”, “disposed of”, “in repair”, “under maintenance” etc. The status of a CI might tell you when the item will expire in its lease. This information can be used proactively to manage the infrastructure more efficiently, ensuring, for example, that items will be returned to the leasing company without exceeding return by dates and therefore avoiding expensive penalties. It also helps identify which types of CIs are too often “in repair”.
- ☯ **Audit and Verification:** Regularly the contents of the CMDB will need to be matched against the real world. This can be an automatic or manual process. Verification needs to be done at least once a year (during the annual stocktaking), after major changes or ad-hoc when mismatches are discovered (e.g. via the Service Desk).
- ☯ **Reporting:** Operational and management reports should be produced so that efficient and effective management and control of the infrastructure can be performed. All other ITIL processes, the business (Customers and Users) and even external vendors and suppliers will have an interest in data that is stored within the CMDB.

Activity reporting, more formally known as “Providing Management Information” is an important component of every ITIL process as it is part of the communication within any organisation. There is always a “reporting” activity that you can mention for each ITIL process.

3.4 BENEFITS

Benefits:

- ☯ Provides accurate and up-to-date infrastructure related information to all other IT Service Management processes. None of the other IT Service Management processes would be able to perform optimally without an up-to-date CMDB in place.
- ☯ Creates a better understanding of the resources in use, and resources available
- ☯ Creates a clear understanding of the relationships and the inherent dependencies of Configuration Items
- ☯ Creates, and maintains baselines and standards for the organisation
- ☯ Better information to make justified investment decisions
- ☯ Less unauthorised and illegal hardware- and/or software used in the organisation
- ☯ Cost savings by understanding when, and how resources should be replaced, or disposed of
- ☯ Puts IT back in end-to-end control of valuable Configuration Items (IT related assets)
- ☯ Allows adherence to legal obligations, thus avoiding painful penalties, or loss of image
- ☯ Improves security, and locks down critical Configuration Items
- ☯ Puts unauthorised Changes back into daylight
- ☯ Creates operational, and improves operational knowledge of IT Configuration Items, by tracking, and acting upon lifecycle related data

3.5 PROBLEMS

Problems:

- ☯ Configuration Items (CIs) are defined at the wrong level causing too much or not enough data to work with
- ☯ Implementation is attempted at the wrong level with too much detail making the process inefficient to run
- ☯ Schedules for implementation and populating the configuration management database are too/over ambitious
- ☯ Senior commitment and involvement is lacking
- ☯ The process is perceived to be too bureaucratic and time consuming
- ☯ The process is routinely circumvented which results in a CMDB that is out-of-date
- ☯ Processes are inefficient and ineffective/error-prone
- ☯ Expectations of what the tool can do (automatically) are unrealistic
- ☯ The chosen tool may lack flexibility (e.g. importing and exporting of data)
- ☯ The process has been implemented in isolation not integrated with Change Management and Release Management
- ☯ Expectations of what the process can do are unrealistic and not achievable
- ☯ Proper configuration control is not in place, often because of a lack of Change Management
- ☯ The scope of the database hasn't been set properly which results in a lack of information
- ☯ The process is implemented as a function (or a number of functions), instead of a cross-functional process
- ☯ Clear CI guidelines are not created or communicated/enforced

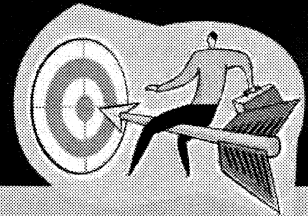
4 SERVICE DESK

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

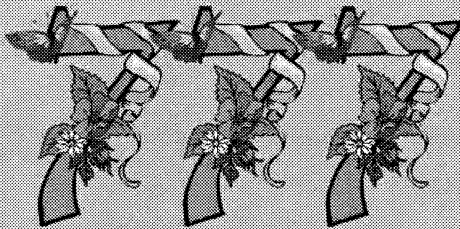
4.1 GOAL

The **goal** of the Service Desk is to provide a **single point of contact** (SPOC) for Users and Customers and to facilitate the **restoration of normal operational service** with minimal business impact on the Customer within agreed service levels and business priorities.

Goal



- To provide a single point of contact for Users and Customers
- To facilitate the restoration of normal operational service with minimal business impact on the Customer within agreed service levels and business priorities



Often the Service Desk will be the only window into IT for Users and Customers. As such the **accessibility** of the Service Desk, **responsiveness** and **attitude** (user-friendliness) of the Service Desk will be key factors to its success. When the Service Desk does not or can not respond efficiently and effectively to the calls being submitted to her, her credibility will quickly diminish and Users and Customers will start to bypass this function altogether.

4.2 TERMINOLOGY AND DEFINITIONS

There are three recognised Service Desk structures in ITIL:

- ☉ **Local Service Desk:** In this scenario each site or business unit will have its own Service Desk. This structure provides for local support and knowledge, will not be hindered by time zones, language or cultural differences, but is typically not optimal when it comes to resource usage.
- ☉ **Central Service Desk:** In this scenario all Service Desk activities are centralised and the Users and Customers will be supported from only one location. In the case of issues the Indian business-unit might have to call the Service Desk located in Ireland. This scenario typically asks for working in shifts when multiple time-zones are supported. However it becomes easier to share knowledge and to ensure adherence to policies and procedures.
- ☉ **Virtual Service Desk:** The Virtual Service Desk uses the follow-the-sun concept and typically partitions regions into various time-zones. All regions are open for a predefined number of hours and when one region closes the next region opens up. In this way Customers and Users are “always” supported with their Incidents, Queries and Service Requests.

As single point of contact, the Service Desk staff members will need excellent people-skills. Good communication, listening and empathy skills are vital for good support. Technical skills will be secondary and are a nice to have. It is a lot easier to send someone on a technical Microsoft or Cisco course than teaching someone telephone manners, patience and empathy.

4.3 ACTIVITIES

The Service Desk is a function, not a process and hence has no identified process activities, but merely functions. Some of the identified functions are:

- ☯ Receiving calls, as first-line customer liaison reference point;
- ☯ Recording and tracking of all Incidents;
- ☯ Recording and tracking complaints and compliments;
- ☯ Keeping customers informed on request status and progress of Incidents;
- ☯ Making an initial assessment of requests, attempting to resolve them or refer them to someone who can, based on agreed service levels
- ☯ Escalation Incidents, Problems and other events as per established escalation procedures;
- ☯ Monitoring Incidents, Problems, and other events relative to the appropriate SLA;
- ☯ Managing the request life-cycle, including closing and verification of Incidents, Problems, and other events;
- ☯ Contributing to Problem identification by picking up trends in Incidents;
- ☯ Communicating planned and short-term changes of service levels to customers;
- ☯ Coordinating second-line and third-party support groups, so Incidents and Problems can be resolved appropriately;
- ☯ Providing management information and recommendations for service improvement;
- ☯ Identifying Problems based upon significant or repetitive occurrence of Incidents;
- ☯ Highlighting customer training and education needs; and
- ☯ Closing Incidents and confirmation with the customer.

4.4 BENEFITS

Benefits:

- ☯ Creates a single point of contact between the Business and IT, hence improves the accessibility of the IT organisation
- ☯ Improved customer services, and typically higher customer satisfaction
- ☯ Improved communication, and feedback and events closure mechanisms
- ☯ Right escalation of events to the appropriate staff
- ☯ Business aligned response, and feedback targets
- ☯ Improved quality, and continuity of services (more uptime by rapid and effective restoration of services)
- ☯ Improved usage of resources, skills, and staff (also predicting required staff and resources to cope with the various peaks and troughs)
- ☯ Formalised and agreed performance targets for 1st level support
- ☯ Improved skills, and team-effort supporting by formalised procedures, work instructions and job descriptions
- ☯ Enhanced focus on proactive activities, rather than only focusing on reactive fire-fighting related activities
- ☯ Reduced burnouts and stress by proper management of 1st level support staff
- ☯ Improved information, and documentation (reports) for (Incident) management to control, and manage the 1st level support organisation

4.5 PROBLEMS

Problems:

- ☹ No visible commitment and/or involvement from senior management
- ☹ Lack of resources to implement and maintain the function
- ☹ No agreed service targets in place for the Service Desk
- ☹ The scope of what needs to be supported has not been set and/or agreed unambiguously
- ☹ Users and Customers bypassing the Service Desk for various reasons
- ☹ No adequate induction and/or ongoing training for first level support staff
- ☹ Not clear where the Service Desk is to support the other ITIL processes
- ☹ Service Desk staff not empowered to make decisions themselves
- ☹ High turnover of staff due to the repetitive nature of the workload
- ☹ High stress-levels and burn-out of staff, and no staff rotation used
- ☹ No code-of-conduct in place on how to deal with abusive Users
- ☹ No integrated IT Service Management solution (tool-wise)
- ☹ Tools not properly aligned with the function (e.g. event recording takes relatively too long compared to event resolution)
- ☹ No adequate reporting functionality for the function
- ☹ Not enough resources assigned to the Service Desk and workloads not understood

5 INCIDENT MANAGEMENT

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

5.1 GOAL

The **goal** of Incident Management is to restore normal service operation as quickly as possible and minimise the adverse impact on business operations, thus ensuring that the best possible levels of service quality and availability are maintained.

Rebooting a machine, control-alt-deleting an application in Windows, resetting someone's password, re-imaging someone's workstation, re-setting someone's connection, restarting a printer-session are all common examples of Incidents. These types of Incidents typically do not take a very long time to resolve (maybe a couple of hours up to a few days) and are by nature very **reactive**.

Normal service operation is defined here as service operation within Service Level Agreements (SLA) limits.

5.2 TERMINOLOGY AND DEFINITIONS

Definition: An Incident is **any** event which is not part of the standard operation of a service and which causes, or may cause, an interruption to, or a reduction in, the quality of that service. All Incidents need to be registered, even those that only take a couple of minutes to resolve. Some Incidents will mean that the service no longer works properly (the "real" Incidents – something is broken), some Incidents will mean that the User is after some information (Queries) and some Incidents will mean that the User wants something added, modified or deleted (Request for Change or Service Request).

Definition of **Priority**: All Incidents will need to be prioritised so it is possible to allocate the right amount of resources. Priority is always a function of **Impact** and **Urgency**! Impact meaning the affect the Incident has on the business and urgency meaning the time you have to find a fix. Some Incidents might affect all people in the organisation, but this doesn't always mean that it needs to be fixed immediately. Some Incidents might only affect one person, but if it doesn't get resolved immediately the person can not continue with his or her work and we are losing productivity/business. Often a **Priority-Matrix** will be created where you will find impact on the vertical axis and urgency on the horizontal axis.

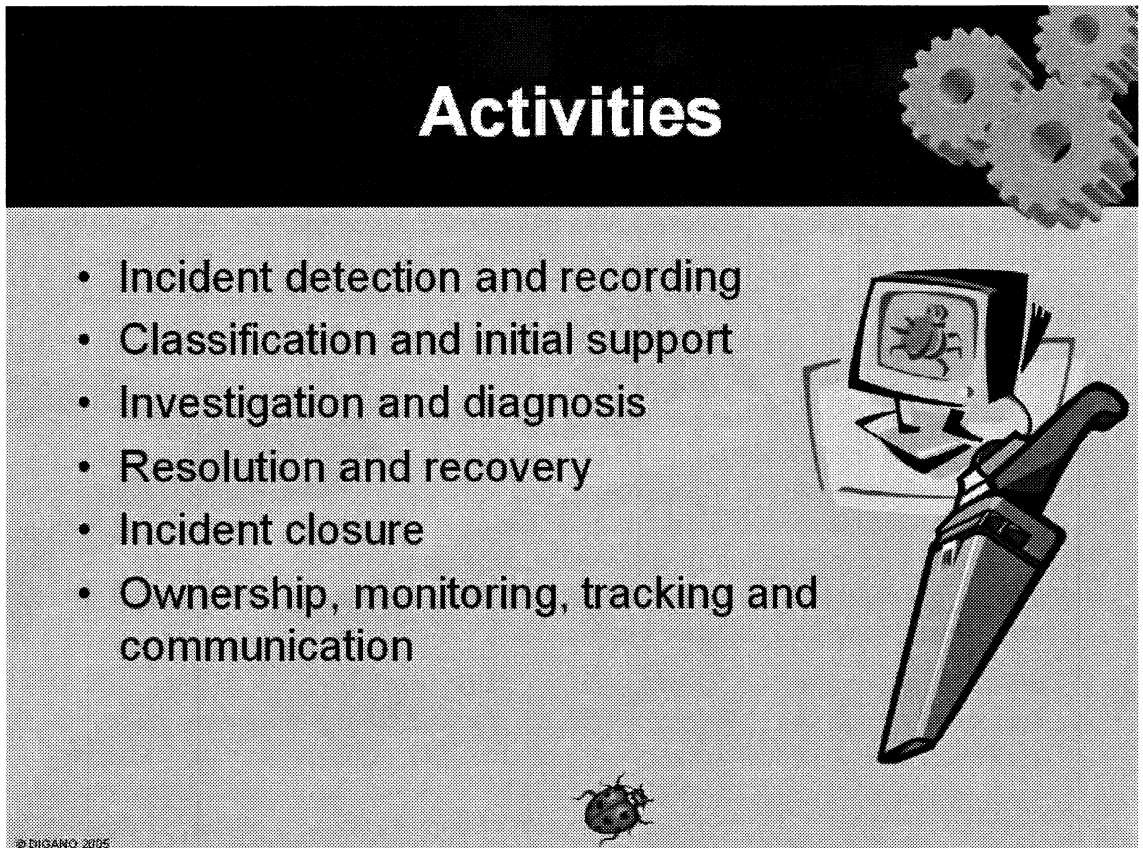
Definition of **Escalation**: ITIL recognises **functional** and **hierarchical** escalation.

Functional or horizontal escalation is used where skills, knowledge or experience are scarce within one business unit and therefore the Incident will be escalated to another business unit that typically operates on the same business level. Hierarchical escalation is used where a decision from management is required or certain triggers have been met that requires

notification to management (e.g. the Incident has exceeded its resolution target).

5.3 ACTIVITIES

There are basically six activities within Incident Management that you will need to know of for the exam.



Activities

- Incident detection and recording
- Classification and initial support
- Investigation and diagnosis
- Resolution and recovery
- Incident closure
- Ownership, monitoring, tracking and communication

© DIGANO 2005

The activities are:

- ☉ **Incident detection and recording:** All Incidents need to be recorded using a consistent approach to capture the necessary data, such as initiator details, date and time details, description of the Incident and CIs affected. Nowadays many Incidents will be automatically logged into the Incident Management system by tools like Openview, Patrol, Tivoli and other monitoring systems.
- ☉ **Classification and initial support:** All Incidents need to be classified – in other words – what type of Incident we are dealing with. Some Incidents will have a standard solution; other Incidents need more investigation and diagnosis. Password resets typically follow a standard procedure – ITIL uses the terminology “Service Request” to deal with these types of Incidents. Incidents will also receive a category like hardware, software, network, etc. and they need to be prioritised properly (using impact and urgency quantifiers) so the right amount of resources can be allocated

towards them.

- ☯ **Investigation and diagnosis:** The Incident Matching activity will tell the analyst whether or not a similar Incident has occurred in the past and whether or not a Workaround or Permanent Solution is available. Diagnostic scripts like the Windows Wizards can be used to standardise the diagnostic process. Diagnostic scripts typically guide the analyst (doctor) towards the solution (cure).
- ☯ **Resolution and recovery:** When a proper Workaround (quick fix) or Permanent Solution has been identified the Incident record needs to be updated with the appropriate amount of detail (actions and time taken to resolve). Communication procedures between higher level support teams (2nd and 3rd level) and 1st-level support teams (the Service Desk) need to be established to ensure efficient and effective communication back to the initiator of the Incident. A response from the initiator (Customer Satisfaction Survey) may be required before the Incident can be closed.
- ☯ **Incident closure:** After confirming with the initiator that the Incident has been successfully resolved the Incident can be closed after all data is updated and a proper closure category has been assigned to the Incident. Mismatches between opening category (e.g. hardware) and closure category (e.g., software) should be examined as they will impact on the effectiveness and efficiency of the Incident Management process. ITIL recommends the use of Customer Satisfaction Surveys to measure perception and satisfaction of the service delivered. The **RAG** approach, using the traffic-light colours **Red**, **Amber** and **Green**, is a simple though efficient and effective way of measuring the quality of a service.
- ☯ **Ownership, monitoring, tracking and communication:** This activity will ensure that Incidents do not get lost within the organisation and enough resources are available to deal with Incidents in an efficient and effective manner. The Incident Manager as process owner carefully needs to track whether or not service targets as agreed with the Customers will be met. Where necessary, resources need to be rescheduled and reallocated between the various support levels. This activity will also ensure that proper information is relayed back to the organisation in the form of reports. The Incident Management process will always take full ownership of all Incidents until closed – the phrase: “It’s no longer my problem!” can not be tolerated within professional organisations.

5.4 BENEFITS

Benefits:

- ☯ Being in control of all Incidents
- ☯ No more lost, and inaccurate Incidents
- ☯ A single point of accountability for all Incidents
- ☯ Understanding the weaknesses of systems and services
- ☯ Clear formalised communication between support groups
- ☯ Making optimal use of the staff and resources dealing with Incidents
- ☯ Less interruptions to business and technical staff
- ☯ Improved business, and IT satisfaction
- ☯ Improved continuity (by rapid restoration) of business services
- ☯ Better understanding of performance and resources used
- ☯ Formalised reporting and monitoring
- ☯ Consistency of data-collection, and service provision
- ☯ Faster response times on Incidents
- ☯ Reduced downtime per Incident

5.5 PROBLEMS

Problems:

- ☹ No visible commitment and/or involvement from senior management
- ☹ Lack of resources to implement and maintain the process
- ☹ No agreed “end-to-end” service targets in place for Incident Management
- ☹ No accurate and complete capturing of data
- ☹ Users and Customers bypassing the process for various reasons
- ☹ No adequate induction and/or ongoing training for staff
- ☹ No full integration with the other processes, in particular Problem Management
- ☹ No clear distinction made between Incidents and Problems
- ☹ Not enough build up of knowledge that can be re-used
- ☹ Unclear or no escalation paths set for Incidents
- ☹ No clear classification in place (e.g. Incidents, Service Requests and Queries)
- ☹ Priorities constantly overrules by business managers
- ☹ No integrated IT Service Management solution (tool-wise)
- ☹ Tools not properly aligned with the process (e.g. Incident recording takes relatively too long compared to Incident resolution)
- ☹ No adequate reporting functionality for the process

6 PROBLEM MANAGEMENT

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

6.1 GOAL

The **goal** of Problem Management is to minimise the adverse impact of Incidents and Problems on the business that are caused by errors within the IT Infrastructure, and to prevent recurrence of Incidents related to these errors. Problem Management seeks to get to the root cause of Incidents and then initiate actions to improve or correct the situation.

6.2 TERMINOLOGY AND DEFINITIONS

Problems are the reasons why so many machines need to be rebooted, why “control-alt-deleting” an application in Windows is necessary, why people are forgetting their passwords, why machines lose their standard configurations, why connections are failing, and why printer sessions are lost . Understanding the **underlying root cause** is the key activity within Problem Management. Rebooting a workstation might take 10 minutes, but the investigation into why it is necessary and how to prevent it from happening in the future might take weeks, months or sometimes even years! So Problem Management is by nature very **proactive**.

Example: There is a crack in the ceiling, there is another crack in the floor, there is another crack in the wall, there are cracks everywhere – let's identify a Problem – we need to get rid of all these cracks before the building collapses or we all lose our jobs!

Definition: A **Problem** is the unknown underlying cause of one or more incidents. Problems are typically identified based upon frequency, regularity or significance of Incidents.

Definition: A **Root Cause/Error** is a Problem that is successfully diagnosed and for which the Configuration Item (CI) at fault has been identified.

Definition: A **Known Error** is a Problem that is successfully diagnosed (the Root Cause has been identified) and for which a Work-around (or permanent solution) has been identified.

Definition of **Priority**: All Problems need to be prioritised so it is possible to allocate the right amount of resources. Priority is always a function of **Impact** and **Urgency**! Impact meaning the affect the Problem has on the business and urgency meaning the time you have to find a fix. Some Problems might affect all people in the organisation, but this doesn't always mean that it needs to be fixed immediately – a Workaround might be available already. Some Problems might only affect one person or system, but if it doesn't get resolved immediately the business can start to lose money or their good image. Often a **Priority-Matrix** will be created where you find impact on the vertical axis and urgency on the horizontal axis.

Definition of **Escalation**: ITIL recognises **functional** and **hierarchical** escalation. Functional or horizontal escalation are used where skills, knowledge or experience are scarce within one business unit and therefore the Problem needs to be escalated into another business unit that typically operates on the same business level. Hierarchical escalation is used where a decision from management is required or certain triggers have been met that requires notification to management (e.g. the Problem has exceeded its internal (to the IT organisation) resolution target).

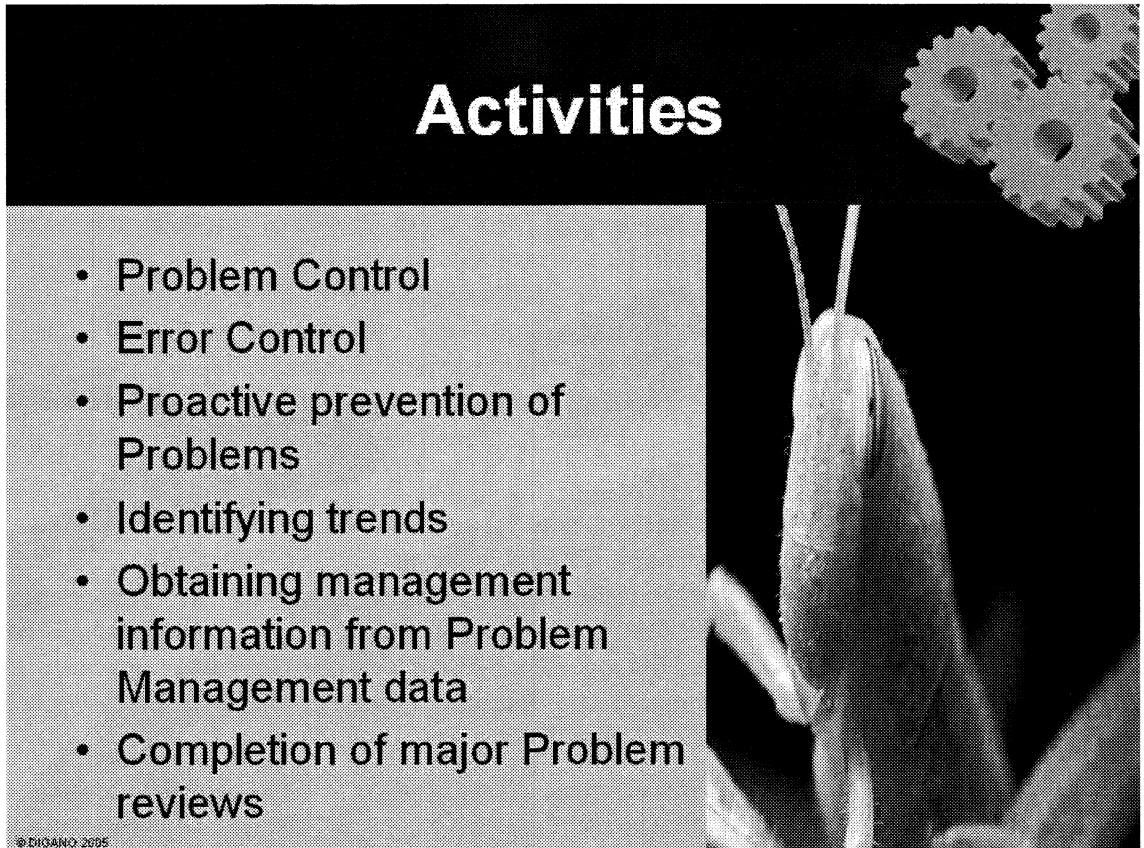
Incidents **never** turn into Problems! They can co-exist, but Incidents are business focused (restoring services as soon as possible) whereas Problems are IT focused (creating a reliable and stable IT infrastructure). If Incident Management can't find proper resolutions to certain types of Incidents they can ask Problem Management for assistance, but Problem Management will not become accountable for the Incidents.

According to the ITIL framework many Incidents can be related to the same Problem (many-to-one) or one significant Incident can be related to one Problem (one-to-one), but it is not allowed to link one Incident to multiple Problems (one-to-many).

Many Known Errors with Workarounds or permanent structural solutions will come from developers, external system houses or from vendors and suppliers. These Known Errors could immediately progress into Request for Changes (not always), and fall under control of Problem Management. There may be the need to convert Known Errors from the vendor's format (e.g. Microsoft Technet) into a format that is used within the internal organisation.

6.3 ACTIVITIES

There are basically six activities within Problem Management that you will need to know for the exam.



Activities

- Problem Control
- Error Control
- Proactive prevention of Problems
- Identifying trends
- Obtaining management information from Problem Management data
- Completion of major Problem reviews

© DIGANO, 2005

The activities are:

- ☉ **Problem Control:** This activity identifies new Problems, prioritises the Problems, allocates resources and looks for the Root Cause of the Problem. In other words, Problem Control is about finding the source of the Problem. Once the source has been identified the next activity Error Control kicks in. This activity also tries to match new Incidents to existing Problems (**Incident Matching**). Resources can be allocated to the Problem depending on the number of Incidents matched to that Problem
- ☉ **Error Control:** This activity is geared to minimise the negative affect of the Problem on the business by establishing a Work-around. Furthermore, Error Control is about finding a permanent structural solution (or where more than one solution is available Problem Management will typically provide a recommendation) and will submit Requests for Changes (RFCs) to Change Management for approval and implementation of the solution(s). The Known Errors (Known Error Records

“KERs”) will be maintained in the Known Error database (knowledgebase). The Problem can only be closed after successful implementation of the Change.

- ☯ **Proactive prevention of Problems:** Whereas Problem Control and Error Control typically focus on Incidents that have already happened (Reactive Problem Management), Proactive Problem Management focuses on prevention of Incidents so they won't happen at all. Proper maintenance schedules, replacing old equipment, software patch-level management and keeping virus-definition files up-to-date are all examples of Proactive Problem Management. It is typically cheaper to prevent Incidents than to fix them afterwards.
- ☯ **Identifying trends:** This activity keeps track of where and when Incidents and Problems occur. Some problems start very small (embryonic faults), but could quickly grow larger with sometimes disastrous consequences if not detected early enough. The number of Incidents or Problems relating to a certain business unit, system (CI) or service needs to be tracked and variations on the norm need to be dealt with effectively and efficiently to guarantee a smooth running service environment. Where a certain number of Incidents exceeds a predefined norm (pain-factor) a Problem could potentially be generated automatically thus ensuring resources and attention.
- ☯ **Obtaining management information from Problem Management data:** Management will need information on new, work-in-progress, pending and resolved Problems in order to allocate the right amount of resources (money, time and people) towards the process. Where Problems were not resolved successfully through the Problem, Change and Release Management processes corrective actions will need to be taken to ensure smooth running and optimal co-operation between these Service Support processes.
- ☯ **Completion of major Problem reviews:** Where the Problem has been diagnosed and a solution identified and implemented (through Change and Release Management), a lessons-learnt activity must be performed. Did everything work according to plan? Did you stay within predicted resources? Has the full Problem been resolved or are there still some outstanding issues or side-effects? Were the proper resolution techniques adhered to? Was the documentation properly updated and were stakeholders properly informed?

6.4 BENEFITS

Benefits:

- ☯ Reduced number of (repetitive) Incidents
- ☯ More reliable infrastructure environment
- ☯ Providing permanent structural long-term solutions
- ☯ Allocating Problem solution resources where, and when they are necessary to reduce the pain felt by the business, and/or IT
- ☯ Improved quality and continuity of services
- ☯ More professional attitude towards IT
- ☯ Capturing business- and IT related knowledge in the knowledge database
- ☯ Improved first-time solution rate for the staff providing services at 1st level support (as workarounds and permanent solutions will be provided by Problem Management)
- ☯ Overall increasing the quality of services provided
- ☯ Separating stress (short-term pressure) from rationality (long-term pain-relief)
- ☯ Improved relationships with external vendors/suppliers
- ☯ Formalised reporting and monitoring

6.5 PROBLEMS

Problems:

- ☯ No visible commitment and/or involvement from senior management
- ☯ Lack of resources to implement and maintain the process
- ☯ No Incident Management process/data in place, therefore prohibiting Problem Control and Error Control
- ☯ No full integration with the other processes, in particular Incident Management (e.g. no ability to link the various records)
- ☯ Problem Management used to escalate Incidents, thus becoming a second Incident Management process
- ☯ Problem Management taking over the role of the Service Desk and undermining their existence
- ☯ Not enough time provided to build up of knowledge (knowledge base)
- ☯ Unclear or no escalation paths set for Problems
- ☯ No clear classification in place (e.g. Incidents, Service Requests, Queries, Work Arounds, Problems and Known Errors)
- ☯ Resources not properly allocated to deal with Problems (organisation prefers reactive mode, rather than proactive mode)
- ☯ No integrated IT Service Management solution (tool-wise)
- ☯ Tools not properly aligned with the process (e.g. Problem Management investigation and diagnosis tasks can not be properly assigned to the various resolvers)
- ☯ No adequate reporting functionality for the process
- ☯ No clear priorities, impacts and urgencies set and/or committed too
- ☯ No Known-Error data provided by other teams (development, external suppliers, etc), and as such reinventing wheels

7 CHANGE MANAGEMENT

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

7.1 GOAL

The **goal** of Change Management is to ensure that standardised methods and procedures are used for efficient and prompt handling of **all** Changes, in order to **minimise the impact of Change-related Incidents** upon service quality, and consequently to improve day-to-day operations of the organisation.

7.2 TERMINOLOGY AND DEFINITIONS

Definition: A **Change** is moving from one defined state to another. An authorised Change typically changes the fit, form or function of a Service.

Definition: A Request for Change (**RFC**) is the paper-based or electronic form that contains all change related data needed to assess the Change on its value to the business or IT.

Definition: The Forward Schedule of Change (**FSC**) is a schedule (Gantt-chart) that allows IT (and the business) to schedule its changes. The FSC is typically distributed by the Service Desk and where possible the business will use the same schedule to inform IT of business-vital activities that might delay or postpone IT related change.

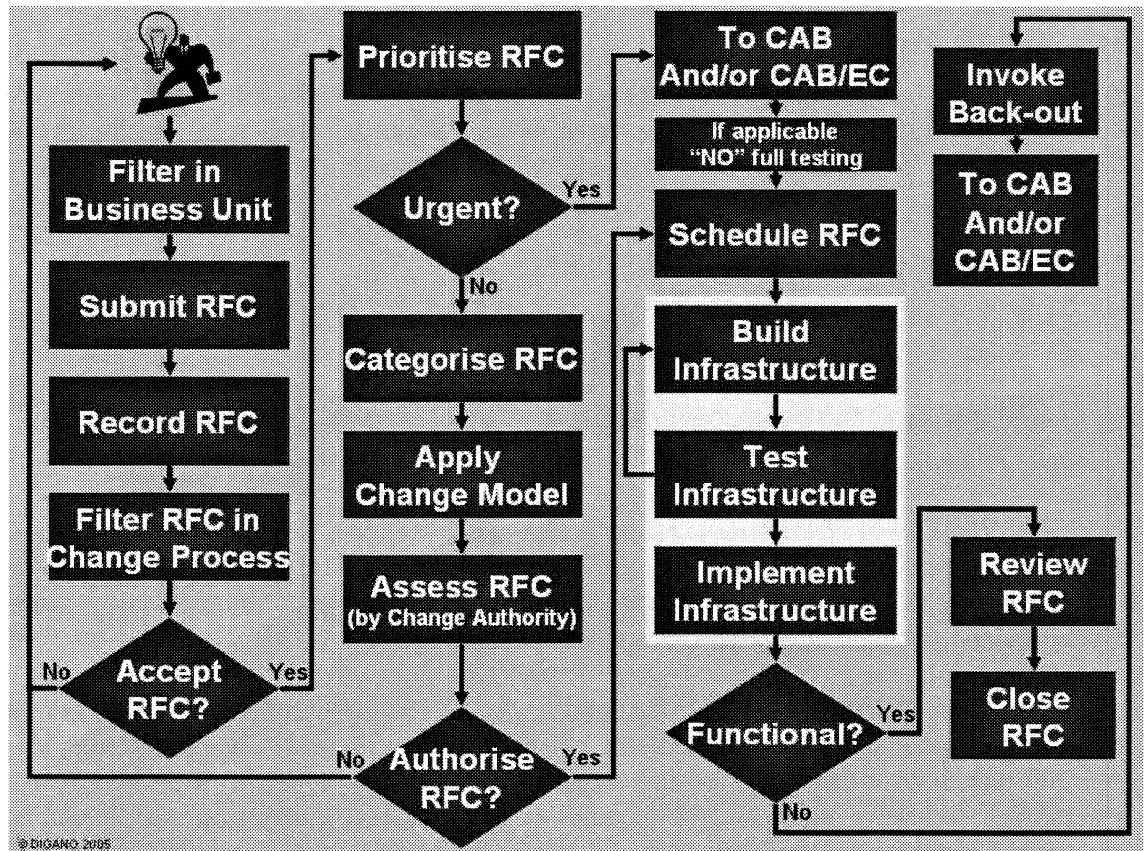
Definition: The Projected Services Availability (**PSA**) document outlines the impact of scheduled and unscheduled maintenance and changes on the (agreed) availability targets as set within the Service Level Agreements (see Service Level Management) and maintenance agreements. Where maintenance or changes impact business performance it should be investigated how this can be avoided in the future, hence there is a clear relationship with Availability Management.

One of the biggest mistakes made by organisations today is to implement Change Management in silos! Change Management is a process and can not be implemented using a silo approach as Changes in one area (e.g. network) often affect other areas (e.g. desktops and servers). As such only a holistic approach to Change will work effectively.

It is vital for Change Management to start with the right level of commitment and involvement from top senior management. All too often it is exactly the senior managers (and sometimes IT themselves) who start bypassing the defined and agreed Change Management process. If one person sets the bad example and gets away with it, others will follow swiftly!

7.3 ACTIVITIES

There are fourteen key activities within Change Management that you will need to know for the exam.



The activities are:

- ☉ **Change Recording:** All Changes need to be recorded. Any actions taken or approvals given need to be added to the Change record. It is vital that a proper history (audit trail) of the Change is maintained for future reference. Information about Changes that are subsequently rejected is still useful and can sometimes lead to the identification of new services and/or products.
- ☉ **Change Filtering:** Where the RFC is not fully completed or doesn't enter into the Change Management process because of possible conflicts with company policies the Change needs to be formally rejected and feedback given to the initiator of the Change. Where the Change is accepted into the Change Management process the initiator should receive a unique Change number for future reference.
- ☉ **Change Prioritising:** Changes will follow one of two possible scenarios: they are either **urgent** or **non-urgent**. Urgent Changes typically increase the risk to the

organisation and should be kept to an absolute minimum. Testing of non-urgent Changes is always a must-perform in ITIL; however, urgent Changes don't have to follow this rule and can be implemented after partial testing or even with no-testing at all. This of course increases the risk to the organisation. If time allows urgent Changes should be tested.

- ☉ **Change Categorising:** Non-urgent Changes need to be further categorised so the optimal process can be followed to allow for fast yet accurate progress of the Changes. Each Change category will follow its own **Change Model** outlining the **Change Authority** (who will authorise the Change), the steps to take and the time and resources allowed to perform the other Change related activities such as assessing, authorising and scheduling of the Change. The number of Change Models will vary from one organisation to another, but basically you will need to understand the following five Change Models for your exam: Urgent, Standard, Minor, Significant and Major. Urgent Changes will be approved by the Change Advisory Board Emergency Committee (**CAB/EC**), Standard Changes are typically pre-approved by the Change Management process, Minor Changes can be approved by the Change Manager, Significant Changes need to be approved by the Change Advisory Board (**CAB**) and Major Changes need to be approved by the Information Technology Executive Committee (**IT/EC**).
- ☉ **Change Assessment:** The assessment of the Change should be performed by the appropriate assessment committee. The Change should be assessed against the impact on technology (**technical assessment**), the impact on finances (**financial impact**) and the impact on the business (**business impact**). Where applicable representatives from the business, the users and the suppliers (**BUS**) should be invited. The **short-term**, **medium-term** and **long-term consequences** and risks of both implementing and not implementing the Change should be considered.
- ☉ **Change Approval:** The Change must be approved by the appropriate Change Authority (pre-approved, Change Manager, CAB, IT/EC or CAB/EC), before any further actions can be initiated. A clear approval mechanism should be in place to approve the changes (e.g. consensus, voting, etc.) to avoid unnecessary delays and to assign clear accountability. Where the Change cannot be authorised proper feedback must be given to the initiator. Be aware that the Change Manager does not authorise all Changes by default, but “merely” manages the Change Management process and collect the ticks-in-boxes and sign-offs from the various stakeholders. Although the statement “The Change Manager doesn't know anything, and the Change Manager doesn't do anything”, sounds extremely harsh, it is not too far from reality.
- ☉ **Change Scheduling:** When the Change is authorised it needs to be scheduled and the Forward Schedule of Changes (**FSC**) and the Projected Services Availability (**PSA**) documents need to be updated. Changes can often be scheduled together with the Release Manager as a large number of the Changes will become the work of Release Management. When more critical Changes are submitted it might be necessary to reschedule all other Changes - this makes automation under a high volume of Changes

almost a prerequisite.

- ☯ **Co-ordinating Change Building:** Change Management co-ordinates the building stage of the Change while Release Management typically performs the work. Work packages need to be assigned to the various build-teams and clear agreements must be made on deliverables and milestones. Change Management as a process must ensure that not only the new environment is properly built according to specifications, but also that a test plan and back-out plan are prepared by the builders.
- ☯ **Co-ordinating Change Testing:** Change Management co-ordinates the testing stage of the Change while Release Management will typically perform the work. Testing should not be performed by the same builder, but should be performed by an **independent tester**. A writer can't proofread his or her own work! Tests such as performance tests, functional tests, regression tests, integration tests, back-out tests and operational tests are just a few examples of tests that will be performed in this activity.
- ☯ **Change Implementation Approval:** As the *gatekeepers of the live environment* nothing should be introduced into the live environment without the knowledge and approval of Change Management (and Release Management). A clear interface in the form of a programme/project office needs to be in place to ensure proper handover and communication from the build and test environments. The programme/project office acts as a functional unit between the Change Management process and the various programmes and projects running within and outside of the organisation.
- ☯ **Co-ordinating Change Implementation:** Change Management co-ordinates the implementation stage of the Change while Release Management will typically perform the work. As a process, Change Management will have to keep a close eye on the implementation of a Change and take appropriate corrective actions where the implementation has the potential to fail and damage the IT organisation or the business. Clear triggers must be set on how and when to invoke the back-out plan for a particular Change to minimise negative impact on the business and to ensure continuity of business.
- ☯ **Change Review:** After implementation of the Change, either successful or unsuccessful, Change Management performs a Post Implementation Review (**PIR**) of the Change. A clear lesson learned needs to be taken from all the successes and mistakes during implementation - What went well? What went wrong? How can we do it better next time? Did the Change achieve its desired outcome? (Was it effective?) Was the Change implemented within agreed time and resources? (Was it efficient)? Clearly the Change needs to be reviewed against the success criteria as set by the initial requestor of the Change. If, according to the success criteria, the Change met all its objectives the Change can be successfully closed (see next activity). If the Change was successful but the requestor has additional requirements for more Change, a new Change record should be submitted and this new Change record should be linked back to the original Change record. Such a chain of Change records provides information on the organisation's ability to specify its requirements upfront -

clearly and completely.

- ☯ **Change Closure:** When the Change has been reviewed (PIR) and the success criteria met, the Change record can be closed. Proper feedback needs to be provided to the requestor and other involved stakeholders. Documentation needs to be stored or archived in line with company procedures and where applicable the Problem Management process (Problem Manager) needs to be notified of the successful implementation of one of their recommendations.
- ☯ **Reporting (Providing Management Information):** As the Change Management process 'indirectly' provides stability and reliability for the IT Infrastructure it is of vital importance that the right information is made available to management to control this process so the necessary corrective actions can be taken on time. Metrics such as number of Changes per category, number of urgent Changes, failed and successful Changes and resources used are just a few of the examples that can be reported.

7.4 BENEFITS

Benefits:

- ☯ Formalised process for approving all Changes
- ☯ Proper test- and back-out plans
- ☯ Involvement of the right business-, and IT stakeholders
- ☯ Understanding the risks of implementing, and not implementing Changes
- ☯ Reduced in the number of failed Changes
- ☯ Involvement of stakeholders at the right levels, and at the right times (different Change authorities)
- ☯ Improved selection of Changes that enable (align to) the business (understanding the full impact of a Change)
- ☯ Improved visibility of all Changes
- ☯ Being able to work smarter, rather than harder (e.g. implementing more Changes at the same time that do not negatively affect each other)
- ☯ Full accountability and audit trail of all decisions made, and by whom
- ☯ Improved perception of IT Services delivered by IT, as Change Management typically creates a more stable, reliable, and consistent infrastructure environment
- ☯ Better assessment of the full financial, business, and technical impact of Changes
- ☯ Full control of Changes during the entire life-cycle; from submission to review
- ☯ Appropriate assessment of all Changes
- ☯ Increased awareness at the Service Desk of upcoming Changes

7.5 PROBLEMS

Problems:

- ☹ No visible commitment and/or involvement from senior management
- ☹ Lack of resources to implement and maintain the process
- ☹ No (or no up-to-date, or no accurate) Configuration Management process/data in place, therefore prohibiting efficient and effective Change Management
- ☹ No full integration with the other processes, in particular Configuration Management and Release Management
- ☹ No clear scope on the type of Changes that is to be managed
- ☹ The process is perceived too bureaucratic by Business and IT and hence frequently bypassed, or not used at all
- ☹ The process doesn't deal effectively with urgent/emergency Changes
- ☹ Unclear or no escalation paths set for Changes, in particular failed Changes or Changes that need to be backed out
- ☹ No clear prioritisation and impact scheme in place for Changes
- ☹ No supporting Change Management tools in place (e.g. recording, assigning tasks, authorisation, scheduling, and project management)
- ☹ Not enough authority given to the Change Manager to say "No"
- ☹ No adequate reporting functionality for the process
- ☹ Right stakeholders, those who can actually make some decisions, not attending the various committees
- ☹ No buy-in from areas like development
- ☹ Multiple Change Management processes in place especially in an outsourced environment

8 RELEASE MANAGEMENT

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

8.1 GOAL

The **goal** of Release Management is to package, distribute and implement hardware and/or software covering the technical and also the non-technical aspects, ensuring a smooth transition from the 'old' infrastructure to the new one. The focus is the protection of the 'live' environment.

8.2 TERMINOLOGY AND DEFINITIONS

Definition: A **Release** is a collection of new and/or changed Configuration Items (CIs) which are tested and introduced into the live environment together.

Definition: A **Release Unit** is the portion of the IT infrastructure that is normally released together. The unit may vary, depending on the type(s) or item(s) of software and hardware.

Definition: A **Release Identification**: Releases should be uniquely identified according to a scheme defined in the Release policy, e.g. Major Releases: Payroll v1, v2, Minor Releases: Payroll v1.1, v1.2, Emergency fix Releases Payroll v1.1.1, v1.1.2.

Definition: **Release Type**. There are basically three recognised Release Types in ITIL. They are known as **Delta Release**, **Full Release** and **Package Release**. A Delta Release will only contain the modified CIs (as compared to the original) of an application or system (e.g. patches and bug-fixes). A Full Release will contain both the modified CIs, but also the original CIs of an application or system (e.g. Windows98SE). A Package Release is a combination of two or more Delta and/or Full Release for two or more applications or systems (e.g. a new Standard Operating Environment).

Definition: The **Definitive Software Library (DSL)**: The library in which the definitive authorised versions of all software CIs (all relevant current and previous versions) are stored and protected. This repository will contain all physical software-related CIs, such as CD-ROMs, DVDs, source-code, license documents, user manuals, installation instructions, baseline assembly instructions, etc. Only authorised CIs should end-up in the DSL.

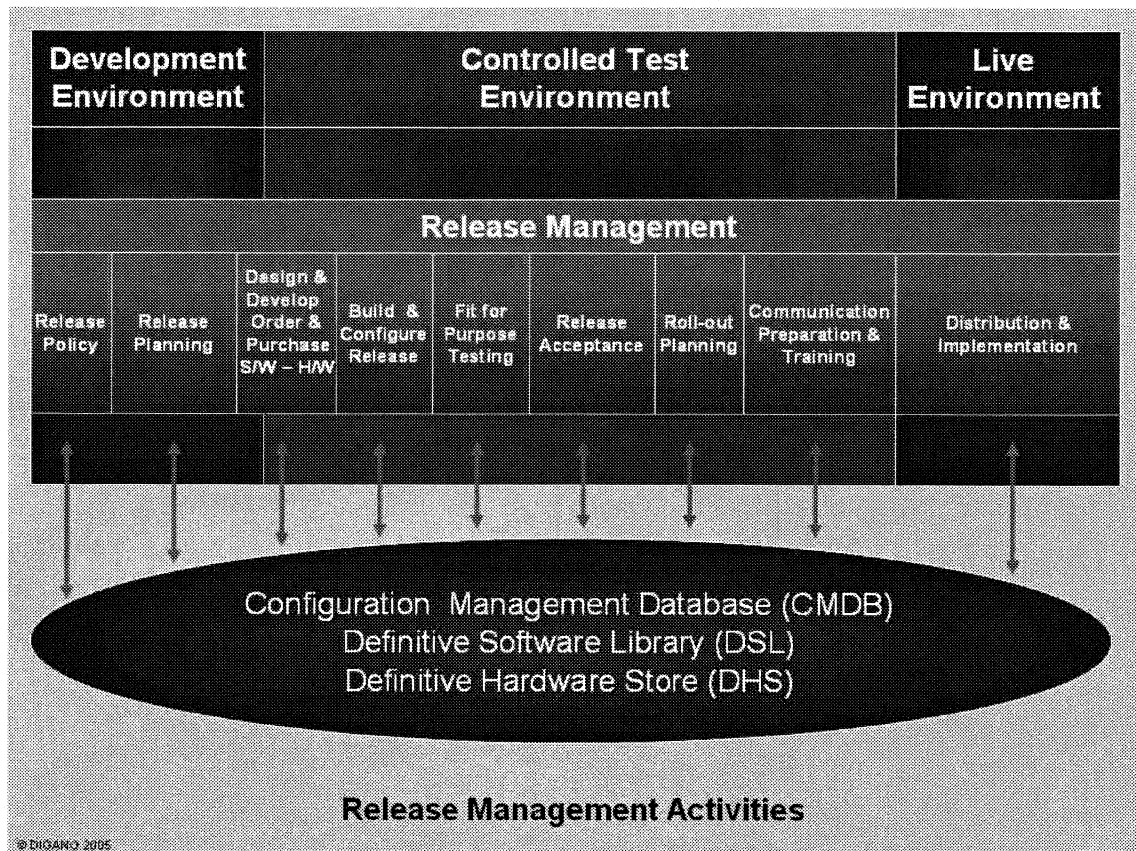
Definition: The **Definitive Hardware Store (DHS)**: The store in which the definitive authorised versions of all spare hardware CIs are stored and protected. This repository will typically contain those hardware CIs for which the status accounting field will have the value "In Stock" or "In Spare".

Please realise that development is not normally managed using the ITIL framework. A

methodology like the Structured Systems Analysis Development Methodology (SSADM) can be used to manage the development of a new application or system. Only the Build, Test and Implementation areas are managed by ITIL.

8.3 ACTIVITIES

There are basically 9 key activities within Release Management. The exam rarely goes into the details of any of these activities.



The activities are:

- 🕒 **Release policy:** A formalised Release policy will set the guidelines for the rights and obligations towards software and hardware usage. Release Management will create documentation with input from Service Level Management. The Release policy sets the scene for Release Management and answers questions like: “What do we Release, how often do we Release and what happens if a Release goes haywire?”
- 🕒 **Release planning:** This activity ensures the quality of the Release. The Release needs to be scheduled, back-out plans need to be produced and roles and responsibilities need to be assigned. Where the Forward Schedule of Change (FSC) is at a high-level the Release schedule will typically need to go into more detail. Of course these “two” schedules need to be closely aligned.
- 🕒 **Design, develop, order and purchase hardware and software:** This activity focuses on acquiring the necessary software and hardware items. These items may come from

the Definitive Software Library (DSL) and Definitive Hardware Store (DHS) but could also be purchased externally. Close alignment with the procurement process is a must where software and hardware needs to be ordered. The necessary checklists will need to be produced to minimise the chance of installing unauthorised software and/or hardware items.

- ☯ **Build and configure Release:** This activity creates the assembly instructions and compile and link application modules, generates databases and populates these with data, writes automated installation routines and caters for licensing and training of central Release Management staff. Where necessary this activity negotiates changes to support contracts. Last but not least the high-level test plans need to be expanded into more detailed test plans.
- ☯ **Fit for purpose testing:** This activity focuses on testing: testing the final functionality by independent business staff, testing installation procedures, testing back-out procedures and testing functional integrity of the resulting system. For accountability purposes sign-off for each stage needs to be part of this activity. Rejected Releases should be treated as failed Changes and need to be reviewed as such.
- ☯ **Release acceptance:** When all tests have been performed a final green-light needs to be provided by the Business and Change Management before Release Management can start with the actual implementation of the Release.
- ☯ **Roll-out planning:** This activity focuses on getting ready to implement. An exact detailed timetable of events needs to be produced including new CIs to be installed and old CIs to be decommissioned. The overall action plan should identify any site-specific implications such as different time zones. Release notes and communications to end Users should be produced with the help of internal specialists in communicating with the business. Finally, detailed purchasing plans to acquire hardware and software (not forgetting secure storage) need to be produced and meetings scheduled for staff and any other groups involved with the Release.
- ☯ **Communication, preparation and training:** In this activity a series of rollout planning meetings are scheduled and training conducted for Customer liaison staff, Customers and support staff. Stakeholders are informed and expectations set. Regular status updates should be provided and Release mechanisms and any related constraints publicised. Health and safety requirements must be taken into consideration and any changes made to support contracts should be communicated.
- ☯ **Distribution and implementation:** This activity manages the distribution of software into the build, controlled test and live environment and ensures that equipment is delivered safely to its destination in its expected state. Procedures for procurement, storage, dispatch, receipt and disposal of goods are created and used as well as procedures for installation, environmental and electrical checks. Release Management will also have to maintain the integrity of software during handling, packaging and delivery and where applicable has to check for complete delivery over networks, if possible using automatic checks. Finally, the relevant data has to be provided to

Configuration Management to update the CMDB and where applicable Release Management should also perform the Customer satisfaction surveys where the Release relates to the installation of the new or modified Infrastructure.

8.4 BENEFITS

Benefits:

- ☯ Ability to work smarter, rather than harder, by making optimal use of resources (e.g. combining multiple Releases into packages)
- ☯ Reduced interruption to the Business as a result of formalised build, test, and implementation procedures
- ☯ Reduced number of unauthorised hardware- and/or software components in the organisation, and faster detection of these unauthorised components
- ☯ Reduced likelihood of introducing viruses into the organisation as all software will be controlled and authorised before it will be put into the definitive software library, build, test or operational environment
- ☯ Controlled access to hardware and software repositories and hence increased security
- ☯ Creating a repeatable, and consistent process of rolling out new hardware and software, as all assembly and installation instruction will be documented within the Release record
- ☯ Clear version control of software components
- ☯ Adhering to software copyrights and cost savings by ensuring that the right number of licenses is available
- ☯ Proper management of the transition from the 'old' infrastructure environment towards the 'new' infrastructure environment
- ☯ Clear separation of duties, and awareness why these duties need to be separated (build, test, implementation, and review)
- ☯ Non-technical aspects of a Release are properly managed (e.g. communication, induction and training, documentation, health and safety, and sign-offs)
- ☯ Improved feedback mechanism with the customers as a result of using customer satisfaction surveys
- ☯ Stronger buy in for Changes as a result of Users and Customers being formally informed beforehand and involved in the testing

8.5 PROBLEMS

Problems:

- ☹ No visible commitment and/or involvement from senior management
- ☹ Lack of resources to implement and maintain the process
- ☹ No Change Management or Configuration Management processes in place therefore prohibiting effective and efficient Change Management
- ☹ No full integration with the other processes (e.g. no ability to link the various Release related data to RFCs, CIs, Problem records and Incident records)
- ☹ Unclear what the Release entails (includes) and who is doing what
- ☹ Business pressure to roll-out a Release before it is properly documented/tested
- ☹ Unclear or no escalation paths set for failed Releases
- ☹ No adequate reporting functionality for the process
- ☹ Resistance from staff to follow the new procedures and work instructions
- ☹ Process not being followed for urgent/emergency Releases
- ☹ Gray area between what is development and what is operational Release Management
- ☹ No representative build and test environments (e.g. the equipment is of a different brand)
- ☹ Inability to recreate all live environments (e.g. due to geographical dispersion)
- ☹ Reluctance to back out after a failed Change (often under pressure from the Business or IT)
- ☹ No sign-off between the various stages of building, testing and implementing the Release, thus no accountability and no audit-trail available

9 SERVICE LEVEL MANAGEMENT

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

9.1 GOAL

The **goal** of Service Level Management is to maintain and improve IT Service quality through a constant cycle of agreeing, monitoring and reporting upon IT Service achievements and instigation of actions to eradicate poor service – in line with business or cost justification.

Although the above mentioned goal comes straight out of the ITIL books it's a bit vague and seems to summarise a large number of activities rather than the actual goal of this process. The goal should really emphasise: increasing quality, decreasing costs, and aligning business with IT.

Leaving out the mumbo jumbo of the original ITIL goal, the goal suddenly turns into a shorter, more to the point goal. Thus, the goal we recommend to learn for the exam: To maintain and improve IT Service quality in line with business or cost justification.

9.2 TERMINOLOGY AND DEFINITIONS

The Service Management chapter in the ITIL book also refers to three recognised Service Level Agreement structures (**SLA structures**). A structured approach is highly recommended. With 12 business units and 12 identified services, you may soon end up with 144 SLAs that need to be managed – 1 SLA per service per business unit (12x12). The SLAs themselves might also include nested-service levels, such as delivering services on a bronze, silver, gold, platinum and diamond level. That would make the number of permutations 12x12x5. Have fun!

The recognised structures are:

- ☉ **Corporate:** It would be ideal if a large number of Services could be covered for a large number of Customers at the same time. It's almost like establishing a baseline of services for the organisation. Everyone needs access to a workstation, a telephone connection, email, virus-scanning, support from the Service Desk from 9am until 5pm etc. The corporate SLA is like finding a coat that fits most people comfortably, and at the same isn't too expensive. This corporate SLA is typically signed off by the General Manager (CEO) and the Manager of IT (CIO) representing the Business and IT as a whole. If you're lucky the corporate SLA may cover 80% or more of all services you're providing (Pareto's 80/20 rule).
- ☉ **Customer based SLAs:** Where specific Customers have their own unique needs for additional products and services or service levels that are not covered by the corporate SLA, it may be necessary to create a number of Customer-based SLAs. A Customer-based SLA covers all the products and services used by an individual Customer

(Business Unit). When the Customer signs a Customer-based SLA they will receive all the products and services as outlined in that agreement. The corporate and customer based SLAs typically cover the majority of products and services provided by IT. These SLAs are typically Customer driven!

- ☹ **Service based SLA:** Left, are those services that are neither used by everyone in the business, nor by individual customers (business units). These are the services that should be covered on an on-demand basis. The Service-based SLA will describe a number of products and services, and anyone who wants to use them can sign-off on these Service based SLAs. These SLAs are typically IT-provider driven!

All text used in SLAs should be written in a business language; text used in OLAs and UCs may contain some technical language as well, although that should be kept to a minimum when possible. Statements used within the agreements and contracts must be written in a 'SMART' context:

- ☹ **Specific:** The statements must be specific enough so they leave no room for ambiguity. For example the statement "we are open during normal business hours" is not considered to be very specific. A statement like "we are open from Monday to Friday, 9am-5pm excluding the following public holidays" leaves a lot less room for interpretation.
- ☹ **Measurable:** The statements used must be measurable. If it can't be measured it's probably not worthwhile putting it in! A statement like "we will respond to your Incidents swiftly" is meaningless. The statement "we will answer the phone within 5 rings and respond to your call within 30 minutes" starts to become more measurable.
- ☹ **Agreed:** All statements used within the agreement must be agreed to by both parties. Where service targets are set by only side and forced upon the other, the results will be sub-optimal and potential friction is likely to occur. Many articles use Achievable as terminology for the letter 'A', but as the author I'm of the opinion that Achievable and Realistic lie too closely together.
- ☹ **Realistic:** Setting unrealistic targets that can never be met should be avoided at all costs. Promising 100% uptime of systems, where the current availability is less than 50% is committing Service Management suicide. All trust will be lost and may never be regained. For this reason a period of due diligence is recommended, so proper data can be collected and feasible targets can be set. Creating SLAs is creating mutual agreement between IT and the Business and not promising "Heaven on Earth".
- ☹ **Timely:** The targets set should be time-based and monitoring and reporting should occur according to the times set. Promising availability of 99.99% is easy, but are you monitoring the availability over a time-interval of 30 minutes or over a time-interval of 5 billion years?

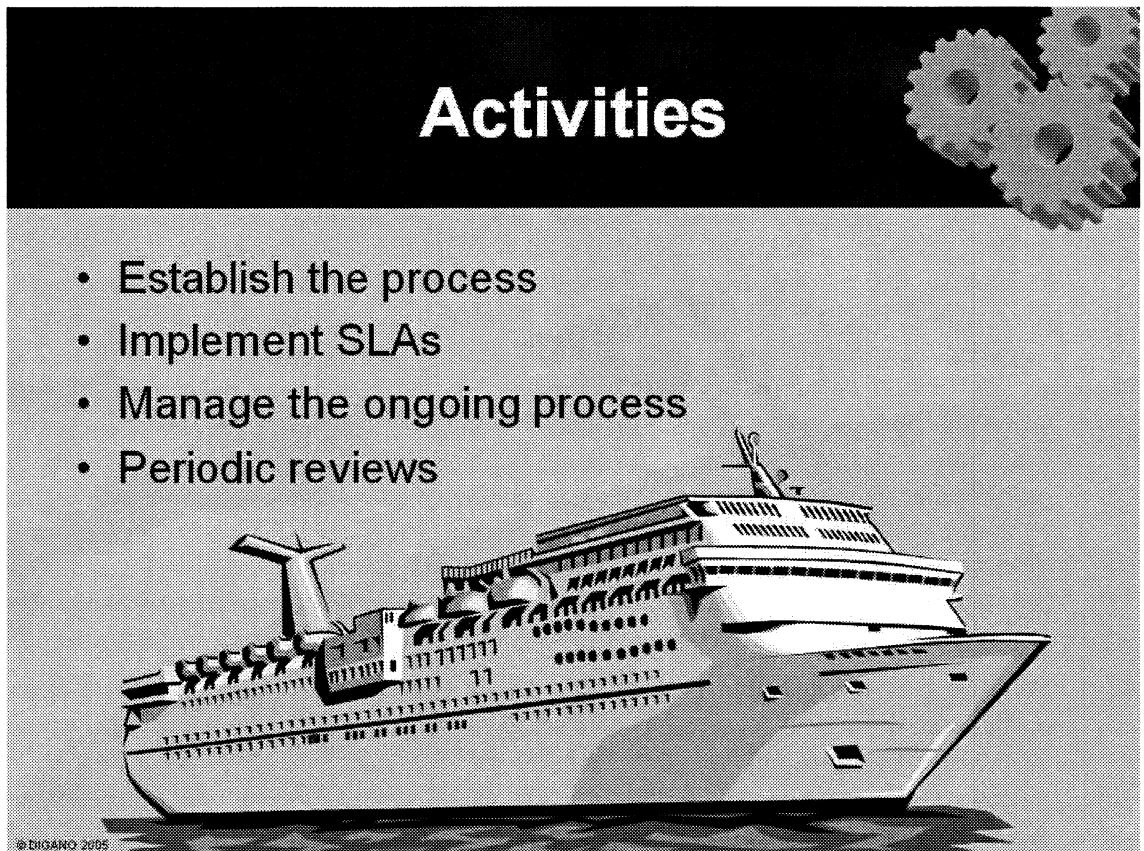
The following list contains a number of items/sections that are typically covered in Service Level Agreements (note the items below are placed in alphabetical order – use any order that suits your organisation best):

- ☉ **Availability targets:** The availability targets states the percentage of the agreed opening times that the Service will be available to the Customer. Different targets can be used for peak hours, off-peak hours, critical business times and less critical business times (e.g. from 6am – 6pm: 98.5%, from 6pm – 10pm: 92.5%, from 10pm – 6am: 0%).
- ☉ **Change statements:** This section describes the process of submitting Changes that affect this Service. Typically a reference will be made the Corporate Change policies and procedures.
- ☉ **Change and maintenance windows:** This section covers any specific time-windows where Changes will or will not be allowed to the Service or where maintenance can or cannot be performed by IT.
- ☉ **Charging targets:** Where charging for the Service is used this section should explain how the charges will be calculated and how often the Customer will be charged.
- ☉ **Continuity targets:** A statement should be included that covers continuity of Service, especially in the case of unexpected outages (e.g. (natural) disasters). Where there is no IT Service Continuity Management Plan available, than this should be clearly stated in the SLA.
- ☉ **Critical business periods:** This section states the Business Critical periods related to the Service (e.g. student enrolment systems during student enrolment time).
- ☉ **Glossary of Terms:** All text used must be unambiguous and where applicable unclear terminology must be explained in the Glossary of Terms.
- ☉ **Incentives:** Incentives (penalties and bonuses) can be used to influence (penalise/reward) the Customer's and IT's performance. Care must be taken not to use too many penalties in internal SLAs. Internal SLAs are about mutual understanding and creating a professional environment. Beating your own colleagues around with a big stick (SLA) is not likely to create an environment that will stimulate continuous improvement.
- ☉ **Maintenance windows:** This section states the maintenance periods relating to the Service (e.g. regular defragging of hard disks).
- ☉ **Page with sign-offs and validity dates:** At least sign-off by IT and the Business. The agreement should also state a start and termination date of the agreement.
- ☉ **Performance targets:** These targets are typically speed related and indicate the time it takes to process a certain job, query or transaction.
- ☉ **Possible amendments to the Agreement:** Any changes to the SLAs should be reflected (and signed-off) in the amendments.
- ☉ **Reliability targets:** The reliability target will set a maximum number of outages allowed within a certain timeframe, and may also reflect the minimum time between outages.

- ☯ **Reporting targets:** This section outlines the frequency and contents of reports to be generated by Service Level Management. Any triggers that initiate the creation of exception reports should be mentioned under this section.
- ☯ **Restrictions:** Restrictions are setting the scope for the SLA and often indicate under what conditions the SLA is active and under what conditions the SLA is deemed to be inactive (e.g. the SLA has a lower threshold of 500 users and an upper threshold of 1000 users).
- ☯ **Reviewing targets:** This section outlines when and by whom the SLA will be reviewed and triggers that may initiate the reviewing activity (e.g. number of Users exceeding a certain threshold).
- ☯ **Right and obligations:** This section states the rights and obligations for both IT and the Business. Today, it is no longer only IT supporting the Business, but equally the Business supporting IT (e.g. IT will deliver the Customer with a desktop Service, but this means to the Customer that they can no longer make their own changes, but will have to fill in a Request-for-Change form).
- ☯ **Scope:** The scope identifies those areas and products and services covered by the SLA. It should be clearly stated what and who is excluded from the Service (e.g. the Desktop Service only covers desktop equipment purchased by centralised procurement).
- ☯ **Security targets:** Any specific Security targets/actions, not covered by the corporate Security Policy and that affect or could affect the Service should be stated in the Security section of the SLA.
- ☯ **Service/system response targets:** The service/system response targets typically specify the time it takes before the Customers receives response, feedback or updates from a system (e.g. after pressing the enter-key on the keyboard the full Intranet web-pages will be delivered within 8 seconds).
- ☯ **Short description of the Service:** A short description of the functionality of the Service should be provided and where applicable functionality that is not included must be mentioned.
- ☯ **Support targets:** The support targets will set a number of performance indicators for support (e.g. from Service Desk) and will typically also state from where and when this support will be delivered. Targets for response time, resolution time, escalation time and feedback times based upon the various priorities should be stated in the SLA.
- ☯ **Table of Contents:** Where the number of pages exceeds 10 a Table of Contents should be considered.

9.3 ACTIVITIES

There are basically sixteen key activities within Service Level Management that you will need to know of for the exam.



- Establish the process
- Implement SLAs
- Manage the ongoing process
- Periodic reviews

The activities are:

- ☉ **Creating a Services Catalogue:** The Services Catalogue is basically a shopping list of all the products and services (the Services) that IT is providing to the Customers. The Customers are those people funding or using the Services and signing off the agreements. The Services Catalogue will contain a short description of the Services, and where applicable some high level service targets and services prices can be mentioned. This document is often published on the Intranet (by the Service Desk), so any Customer can see what type of products and services IT has to offer. This Services Catalogue is referred to by some as the “holy grail” of ITIL as it is the key to understanding your own products and services. If you don’t know what you are selling to your own Customers how can you manage it at all?
- ☉ **Identifying the Service Level Requirements:** Based upon an understanding of what type of Services are currently provided to the various Customers of the organisation, a

beginning can be made to identifying the actual Service Level Requirements (SLRs). These requirements specify the needs (and wants) of the organisation. Where previously it might have been unclear what the Customer's requirements were, this activity will determine and formalise these requirements and capture them in some type of template. Items like opening times, support levels, security targets, critical service times, availability targets, response targets and disaster recovery requirements will be collected and documented in the initial Service Level Agreements (SLAs) – see next activity.

- ☉ **Drafting the initial Service Level Agreement:** The initial Service Level Agreement (SLA) is a statement that formalises the rights and obligations for both IT and the Business. It should be written in clear and concise business language and, where necessary, ambiguous terminology should be explained in a glossary of terms. By definition, this document is an agreement between IT and the internal Business and should not be confused with an actual contract. A contract is a legal document between two organisations and is often written in legal language; whereas an agreement is a document used for internal understanding of quality of service provision and should be written in business language applicable to the organisation introducing the agreement. Contracts typically contain some form of legally enforceable incentives like penalties and bonuses that minimise the financial risk or potential damage to the image of the organisations involved. Of course an SLA could also contain incentives, but this document should not be used to slap each other around the ears; on the contrary, it should be used as an instrument to measure quality and quantity of service provision and where applicable lead the improvement actions.
- ☉ **Assessing the capability to deliver:** Many organisations make the often-lethal mistake of signing off the SLA without performing proper due diligence, only to discover inability to deliver when “push comes to shove”. This and the next three activities (negotiating, establishing UCs and establishing OLAs) should be performed in parallel but in no particular sequence to ensure services can be delivered at a sustainable and consistent level to the Customers. Questions like: “Do we have the right people, the right processes and the right products in place to deliver, support and maintain the new service(s)?” should be asked and the answers verified before signing any SLAs or contracts. Remember, SLAs are with other internal business units, and contracts are with other external organisations to which you, as IT, are delivering services.
- ☉ **Negotiating the contents:** Where additional investment in infrastructure and support is deemed necessary, or delivering against service targets (e.g. 24x7, 100% uptime) is too expensive, unrealistic or unfeasible (e.g. technically not possible), service targets will have to be renegotiated and often downgraded until both parties in the agreement are fully satisfied with the service targets and are fully confident they can be met. Often negotiating will be a painstaking process of finding this fragile balance of what IT can deliver and what the Customer wants. Negotiating is all about creating a win-win situation for both parties involved in the negotiation process.

- ☉ **Establishing Underpinning Contracts:** Where the service to be delivered to the Customer depends on underpinning services delivered by external vendors or suppliers, the appropriate Underpinning Contracts (UCs) will have to be established between the IT organisation and the vendors/suppliers. For example, if the link with your ISP is only up and running for 50% of the agreed time it will not be possible to deliver more than 50% available to the Customer. Most likely the Customer will end up with even less (see Availability Management summary for the explanation). The various UCs will also have to be aligned with the various OLAs (see next paragraph) to guarantee back-to-back coverage of the SLA. An UC is a legally binding contract between two organisations and therefore the wording used should be carefully examined for legal implication before signing off.
- ☉ **Establishing Operational Level Agreements:** Where the service to be delivered to the Customer depends on underpinning services delivered by internal business units, the appropriate Operational Level Agreements (OLAs) will have to be established between the IT organisation and the other internal business units. If Incidents are to be resolved successfully by 1st, 2nd and 3rd level support (assumed to be all internal for the sake of this example) within agreed time, then the right internal agreements must be in place between these support areas before committing to any targets, such as response, escalation, feedback, and resolution time. All involved stakeholders (business unit managers) will have to sign the OLA and commit to the targets set and resources such as time, people and funds that will be made available to deal with the Incidents accordingly. Where multiple internal business units are working together to deliver a service or part of a service it may be necessary for all stakeholders to sign off the OLA to ensure full accountability is taken and responsibilities are clear.
- ☉ **Sign-off:** When the capability is assessed properly, the necessary UCs and OLAs established and all SLA details successfully negotiated, it is time for official sign-off of the SLA. All statements of the SLA should be clear, concise and unambiguous to all parties involved. Preferably the SLA should be written in business language and technical jargon should be avoided. If there is any room for mixed interpretation or confusion because of unclear terminology or wording, then this terminology or wording should be explained in a glossary of terms or rewritten in a better understandable text format. Both a representative from IT and a representative from the Business need to sign off to ensure full accountability is taken. An agreement signed off by only one stakeholder is not a mutual agreement but a waste of time and resources. All activities discussed so far are all part of the planning stage of Service Level Management.
- ☉ **Preparing the Infrastructure (Implementation):** Often, before the actual SLA “goes live” an implementation or pilot period is used to cross the 't's and dot the 'i's. Where applicable the necessary infrastructure changes are implemented and monitoring and reporting processes and systems established. SLA contents are communicated and training is provided. This stage of the Service Level Management process is a bit like preparing for an Olympic games. The 'IT' nation has been elected

to host the games, the SLA has been signed by the Olympic committee and 'IT' as both feel confident that 'IT' can deliver a fantastic event to continue the Olympic dream. Now 'IT' is at full steam building the Olympic village and all the sports venues, so everything will be ready when the grand opening day is there.

- ☯ **Delivery of Service (Go Live!):** This is the moment when there are no more excuses, no more "beating around the bush". It is delivery time! All the targets set in the SLA should now be adhered to. Where service provision targets can't be met or are likely to be breached, stakeholders need to be notified and corrective actions must be taken or recommended. Service breaches may lead to renegotiation and review of the SLA. All teething issues must be resolved as quickly as possible to minimise the negative effect on the Business and IT and the benefits of Service Level Management should be reemphasised on a regular basis.
- ☯ **Monitoring:** Service targets need to be closely monitored so any likely breaches can be acted on immediately, or even better, prevented. Data needs to be collected from the various other Service Management processes, such as Availability Management, Capacity Management, Incident Management and Change Management, but not excluding any other process. Data needs to be accumulated, filtered and processed, so not all *data*, but the right *information* ends up with the Customers. Monitoring means quantitative monitoring (e.g. number of Incidents and duration of outages), but also qualitative monitoring (e.g. customer satisfaction details and complaints) to measure perceived service provision levels by IT and perceived service provision levels by the Business. Where a **credibility gap** between these two exists, action will be required.
- ☯ **Providing Management Information (Reporting):** Regular and ad-hoc reports need to be produced to enable effective management and steering of IT and the Business. The recommendation is to provide reports that give management the ability to take decisions at a glance. Rather than providing hundreds of pages with numbers and meaningless data on whether or not service targets were met, it is often more appropriate to provide reports that support the **RAG** principle and the principle of **Management by Exception**. RAG represents the three traffic light colours Red, AMBER and Green. Everyone understands what a service in Red means! Management by Exception means that management is only informed when targets exceed certain thresholds or are likely to exceed them. This provides management with more time to manage the future of the organisation rather than flicking through the pages of reports telling them everything is "A-okay".
- ☯ **Continuous Quality Improvement:** Where service targets can not be met or are consistently exceeded, actions should be taken and recommendations given. IT should always be working to improve service provision. IT and the Business should live and breathe continuous quality improvement: "Whatever you do today, you can do it a little bit better tomorrow!" It is vital that a culture of improvement is part of the foundation of the organisation.
- ☯ **Planning for Quality Services:** All the ITIL Service Delivery (tactical) processes have two activities in common: reporting and planning. The **services quality plan**

will outline the current status of services, any hiccups and recommendations, and also the future of services and service targets. The business world and IT are both caught up in a whirlpool of continuous change. New business models and new technologies have a one-day-moth life expectancy, and seem to follow more closely than ever before. In order to survive in today's competitive environment, organisations need to reinvent themselves continuously and potentially this means an enormous impact on services and service targets. We need to be able to predict the future and its impact on our services and service provision, because when it "hits us in the face" it's already too late! Organisations like Gartner provide useful online resources when it comes to predicting the uprise of new services and trends in IT.

- ☉ **Reviewing SLAs, OLAs and UCs:** As the business and its environment will change over time, the services will need to change with it. As such, the services and service levels will have to be reviewed regularly, at least annually, to ensure services are still well aligned with business needs. The same rule applies to SLAs, OLAs and UCs. Using Theodore Levitt's (a recognised marketing guru) services model (a model that represents the 4 levels of service provision: generic, expected, exceeded and superb) it must be clear that we should aim service provision at the expected level. Delivering *under* expected levels will cause frustration and low productivity levels for our customers, delivering *above* expected levels will typically lead to higher costs and will often cause a shift in expectation levels: the exceeded service levels will soon become the expected service levels with no way back! Understanding how the various services move over Levitt's model and in what direction they move that enables us to set the frequency of service reviews.
- ☉ **Review the process:** The final activity is to "step out" of your own process and examine it. What goes well, what goes wrong, what should be improved, how much will it cost, and what are the benefits of all the recommended improvements to the Business and IT? In others words performing Quality Assurance (QA'ing) of your own Service Level Management process. After initial implementation of the SLM process, reviewing should be done regularly (e.g. monthly), once the process starts to mature and all creases have been ironed out the frequency of reviews can be reduced (e.g. quarterly, half annually or annually).

9.4 BENEFITS

Benefits:

- ☯ Clear and mutual agreements between IT and the Customers
- ☯ Clear setting of expectations
- ☯ Clear roles and responsibilities, rights and obligations for both IT and the Business
- ☯ Proper underpinning contracts and operational level agreements that support the delivery of an end-to-end Service to the Customer
- ☯ Continuous improvement of Services
- ☯ Focuses on the needs of the Business, rather than the wants of the Business
- ☯ Creates a strong, and well maintained interface between IT and the Business
- ☯ Makes the quality of a Service measurable and tangible
- ☯ Reduces the number of unwanted surprises for IT and the Business
- ☯ Optimally aligns IT technology from Business Services
- ☯ Plans for the right Services, at the right time, to the right Customers, for the right price
- ☯ Focuses the IT resources where they create optimal benefits to the Business
- ☯ Overall increases quality of Services to the Business (and IT)
- ☯ Overall reduces the costs of delivering the Services for the Business (and IT)
- ☯ Continuously realigns Business needs with IT Services using a process of reviewing Services, Service levels, Service structures and Service targets
- ☯ Objective and agreed targets to measure IT Service effectiveness Focus on managing the relationship

9.5 PROBLEMS

Problems:

- ☯ Difficulty of monitoring pre-SLA achievements
- ☯ Setting achievable targets is sometimes a challenge
- ☯ Verifying targets prior to agreements may be an issue
- ☯ SLAs based upon wants (desires) rather than needs
- ☯ No adequate focus on establishment of a mutual agreement
- ☯ Not enough resources and time (no real commitment from senior management)
- ☯ Not enough seniority given to Service Level Management
- ☯ SLAs not supported by the right UCs and/or OLAs
- ☯ Roles and responsibilities not clearly defined
- ☯ Agreements being IT based rather than business and IT aligned
- ☯ SLAs too lengthy and/or ambiguous
- ☯ SLAs not properly, or not at all, communicated to operational levels
- ☯ The process itself is seen as an overhead and increasing the bureaucracy of the organisation
- ☯ Sometimes seen as an exercise in contract negotiation/arbitration
- ☯ No real intention to enforce incentives when targets are not met

10 FINANCIAL MANAGEMENT FOR IT SERVICES

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

10.1 GOAL

The **goal** of Financial Management for IT Services is to provide cost-effective stewardship of the IT assets and resources used in providing IT Services.

10.2 TERMINOLOGY AND DEFINITIONS

Definitions (generic definitions):

- ☉ **Depreciation:** The diminishing value of an asset from wear and tear over time.
- ☉ **TCO:** The measurement to assess the total cost of maintaining, or investing in a new IT system, including hardware, software, installation and maintenance services, and the associated cost of the business processes that the IT system supports.
- ☉ **ROI:** In the private sector, the annual financial benefit after an investment minus the cost of the investment. In the public sector, cost reduction or cost avoidance obtained after an improvement in processes or systems, minus the cost of the improvement.
- ☉ **ROCE:** An accounting measure used to describe the ratio of earnings relative to the average capital invested.
- ☉ **Cost Unit:** Cost Units are the basic items of resource for which Customers are held accountable i.e. provide the method of apportioning indirect costs or calculating the actual cost of variable costs.
- ☉ **Cost per Unit:** This is the cost of a Cost Unit. A good example is the cost per Incident and the cost per workstation.
- ☉ **Capital cost (CAPEX) and Operational cost (OPEX):** A capital cost item typically means that the organisation is adding assets to the financial books for tax and depreciation purposes. An operational cost typically doesn't add a new asset to the organisation; it would be a cost like salaries and system maintenance (ongoing/recurring costs).
- ☉ **Fixed costs and variable costs:** Fixed costs do not change according to resource usage, whereas variable costs do. Monthly staff salaries can be seen as a fixed cost, whereas overtime is typically regarded as a variable cost. The cost of your mobile phone subscription is normally fixed, whereas the cost of calls, the variable part, will depend on the number, duration and destination of the calls you make.
- ☉ **Direct costs and indirect costs:** Direct costs are those costs that can be directly attributed to the conduct of a project, service, product and/or customer and are typically specified in the proposal budget. Indirect costs can not be directly attributed

and are typically shared by the projects, services, products and/or customers as an overall overhead (indirect costs are overhead).

Definitions (two types of budgeting):

- ☉ **Incremental budgeting:** Incremental budgeting is the process whereby an organisation uses current and past budgets as guides and adds or subtracts from these budgets to arrive at the coming period's expenditures (e.g. last year we had 10m, so this year we need 10m +7%).
- ☉ **Zero-based budgeting:** Zero-based budgeting assumes a starting point of zero on every budget being developed and requires detailed justification for every expense (e.g. rolling out a completely new ERP system, where there is no historic data available).

Definitions (three types of depreciation):

- ☉ **Straight line method:** This is the simplest method. Here we divide the total cost of an asset by an estimate of its working life; we also have to take into account any selling or scrap value that we might get back when we sell the asset at the end of that working life. The depreciation amount will be the same for every year for the duration of the asset's predetermined lifetime. Depreciating a 100k asset over 3 years with a residual value of 10k means depreciating the asset by 30k each year.
- ☉ **Reducing Balance method:** This method charges a lot of depreciation in the early years and less in the years after. The method works on the basis that in the early years of the life of an asset its repair and maintenance costs will be small; but they will increase as the asset gets older. A well known example is of course the experience of buying a brand new car, which might depreciate by 20-30% in the first year – sometimes even the moment we drive the brand-new car out of the showroom!
- ☉ **By usage:** This method depreciates the asset based on its usage. Tax-legislation will often determine whether or not depreciating by usage is actually allowed. A taxi could be depreciated based upon the kilometres driven, rather than years in use.

Definitions (four types of **cost models, accounting models, cost techniques**):

- ☉ **Costing by Customer:** This technique will map out all the costs made by a specific Customer (e.g. the full costs of delivering IT services to the marketing unit).
- ☉ **Costing by Service:** This technique will map out all the costs relating to the delivery of a specific service (e.g. the full costs of delivering email).
- ☉ **Cost Centre Accounting:** A cost centre is any unit in cost accounting to which costs are assigned or allocated. The unit may be a division, department or section, a group of plants and machinery, or a group of employees or a combination of several units.

Also sometimes called a budget centre. The cost centre accounting technique apportions costs to the various cost centres. (e.g. IT's budget is 10 million, there are 4 key business units, so the cost is approximately 2½ million per business unit).

- ☯ **Activity Based Costing (ABC technique):** Rather than using some sort of a volume key (see cost centre accounting), the ABC technique actually looks at the costs of performing a specific activity (e.g. the cost of processing a transaction, the cost of storing 1Gb of data on a hard disk or the cost of printing a page on the colour printer).

Definitions (six main **cost types**):

- ☯ **Hardware costs:** mainframe, workstations, printers, routers, etc.
- ☯ **Software costs:** operating systems, database systems, business applications, office applications, system management software, etc.
- ☯ **People costs:** salaries, education, etc.
- ☯ **Accommodation costs:** buildings, computer-rooms, off-site storage, etc.
- ☯ **External Service costs:** contractors, security companies, external developers, outsourcing, etc.
- ☯ **Transfer costs:** (internal transfer costs) internal business units transferring costs to each other (e.g. one business unit "sells" some hardware to another internal business unit).

Definitions (drilling down in the cost types):

- ☯ **Cost elements:** A granular approach to cost types (e.g. mainframes, workstations, etc.). There are only six main cost types (the author would like to refer to them as "main cost categories"), but there could be thousands of cost elements.

Definitions (two types of Customers):

- ☯ **Tied Customers:** Tied Customers typically do not have a choice when it comes to choosing their products and services providers (e.g. IT has a monopoly position).
- ☯ **Untied Customers:** Untied Customers are typically free to decide on who will be providing them with the products and services (e.g. there is full market competition).

Definitions (five types of **charging policies**):

- ☯ **Cost:** Recovering the costs of providing the service(s) (e.g. running IT costs us 10m\$ a year, we need to recover 10m\$ a year).
- ☯ **Cost plus:** Recovering the costs of providing the service(s), increased by a certain

mark-up percentage (standard Target Return). This extra mark-up can be used to cover new large one-off projects, research and innovation, but of course also, profit (e.g. running IT costs us 10m\$ a year, we need to recover 11m\$ a year).

- ☯ **Going rate:** The (internal) going rate typically uses prices that are comparable within the organisation or with similar organisations (e.g. Human Resources charges \$X per man-hour, so we should also charge \$X per man-hour).
- ☯ **Market rate:** The (external) market rate typically uses prices that are charged by other external suppliers (e.g. our competitor charges \$100 per identical product or service, so we should charge the same or less).
- ☯ **Fixed price:** A price based upon negotiation for a set period of time, based upon a predicted consumption (e.g. we will recover 10% from the IT services that we provide to P.R. (Public Relations) and will recover the other 90% from the Sales business unit).

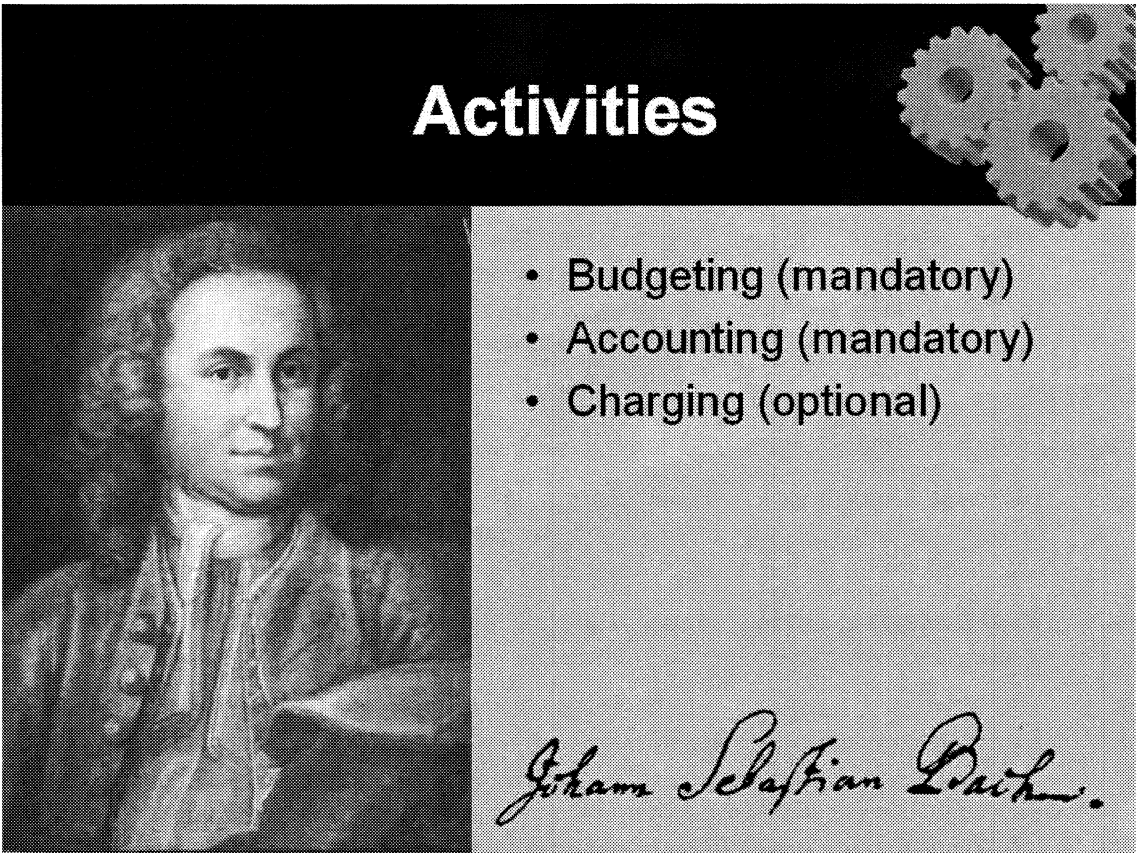
Definitions (three different types of **charging methods**):

- ☯ **Notional Charging:** Notional charging is the method where the Customer will receive an invoice, but doesn't have to pay as yet. Notional charging is often exercised within the pilot stage of introducing charging into the business.
- ☯ **Real Charging:** Real charging is the method where the Customer will receive an invoice and will have to pay the invoice.
- ☯ **Differential Charging:** Differential charging is the method where different Customers are charged different rates, or the same Customer is charged different rates under different conditions (e.g. time of the day). Differential charging is often used to influence the Customer's behavioural patterns. It supports equal spreading of the workload, thereby typically optimising resource usage. This method is often used in combination with Demand Management. Demand Management is a key activity that falls under the umbrella of Capacity Management.

10.3 ACTIVITIES

There are basically four key activities within Financial Management for IT Services.

Activities

- 
- Budgeting (mandatory)
 - Accounting (mandatory)
 - Charging (optional)

Johann Sebastian Bach.

The activities are:

- ☉ **Budgeting:** Budgeting is the process of ensuring that the correct finance is available for the provision of IT Services and that during the budget period they are not over-spent. In other words: How much money do we need to run our IT organisation effectively and efficiently?
- ☉ **Accounting:** Accounting is the process of tracking actual cost against budgeted. Furthermore it supports the development of sound investment strategies and provides cost targets for performance and Service Delivery. This activity also facilitates prioritisation of resource usage and allows day-to-day decisions with full understanding of the cost implications. Last, but not least, it also supports the introduction, if required, of Charging for IT Services. In other words, the Accounting is all about where and when we spend the money. The activity is also known as **IT Accounting, Costing** or **IT Costing**.

- ☉ **Charging:** The third and last activity is optional and will depend on a senior

management decision whether or not to charge back for the costs of providing the services. In other words: We know how much we need to spend (budgeting); we know what we are spending it on (accounting); now we want to get some money back (charging).”

- **Reporting:** Of course there is always reporting. The budget will be a report (plan) that needs to be controlled, revised and, if applicable, updated regularly (at least quarterly). Expenditures need to be closely monitored, and where overspending or underspending occurs or are likely to occur the appropriate (exception) reports will need to be created. Status reports on outgoing revenue streams versus incoming revenue streams needs to be monitored and reported against so the survival of the IT organisation is not unnecessarily jeopardised.

10.4 BENEFITS

Benefits:

- ☯ Increased buy-in and involvement when setting new budgets
- ☯ Clear understanding of the costs of providing Services
- ☯ Clear understanding of the balance between quality/quantity and costs
- ☯ Accurate cost information to support IT investment decisions
- ☯ Accurate cost information for determining total cost of ownership of Services
- ☯ More efficient and effective use of IT resources throughout the organisation
- ☯ Increased professionalism of staff within the IT organisation
- ☯ Costs of technology being translated into the costs of the business
- ☯ Clear charging policies and charging techniques used
- ☯ Ability to recover the costs of Services
- ☯ IT seen as a commercial business unit within the organisation
- ☯ IT no longer seen as a unit wasting business resources, but seen as an enabler to the organisation, understanding the financial consequences of their actions and decisions
- ☯ Forces the organisation to think long-term on the decisions they make. Also where it relates to the costs involved
- ☯ Clear accountability for financial calculations, recommendations, and decisions
- ☯ Up-to-date information on the financial position of the IT organisation
- ☯ Less hidden costs, and better and more accurate insight into the real costs of IT
- ☯ Evidence to help justify IT projects and resources Assists in changing IT mindset to that of a service provider

10.5 PROBLEMS

Problems:

- ☯ Limited understanding in accounting models and charging techniques
- ☯ IT Accounting relies on planning information provided by other business units and processes
- ☯ Staff with both skills in accountancy and IT are hard to find
- ☯ IS and/or IT strategies and objectives may not be well defined/formulated
- ☯ Senior business managers may not recognise the benefits of detailed IT accounting and/or charging
- ☯ IT organisation may not be able to respond to changes in business requirements
- ☯ Costs of IT financial management may outweigh the benefits to the organisation
- ☯ Monitoring tools may be inaccurate, irrelevant or too expensive
- ☯ Cost of capturing and processing all financial data may be high
- ☯ IT financial management may not have been allocated sufficient resources to perform effectively
- ☯ Inaccurate invoices may damage the image of IT and the organisation
- ☯ IT charging the business, without the opportunity for the business to charge IT may be seen as unfair
- ☯ Financial data may be highly dispersed (especially for large organisations)
- ☯ No clear insight into the costs of providing services may lead to frustration with the business
- ☯ Internal charging may be seen as unnecessarily increasing the bureaucracy of the organisation

11 AVAILABILITY MANAGEMENT

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

11.1 GOAL

The **goal** of Availability Management is to optimise the capability of the IT Infrastructure services and support organisation to deliver a cost effective and sustained level of Availability that enables the business to satisfy its business objectives.

To achieve this goal it is necessary to understand the Availability requirements of the business and to plan, measure, monitor and continuously strive to improve the Availability of the IT Infrastructure, services and supporting organisation to ensure these requirements are met consistently.

11.2 TERMINOLOGY AND DEFINITIONS

Definitions (VR³AMS²):

- ☉ **Vital Business Functionality:** The business critical elements of the business process supported by an IT Service.
- ☉ **Reliability:** The reliability of an IT Service can be qualitatively stated as freedom from operational failure. It is also defined as the probability that an item will perform a required function without failure under stated conditions for a stated period of time
- ☉ **Redundancy:** Duplication or repetition of elements in electronic equipment to provide alternative functional channels in case of failure. It also means repetition of parts or all of a message to circumvent transmission errors.
- ☉ **Resilience:** The ability of an IT component failure to be masked to enable normal business operations to continue. Resilience is a function of both reliability and redundancy.
- ☉ **Availability:** Ability of a component or service to perform its required function at a stated instant or over a stated period of time. It is usually expressed as the availability ratio, i.e. the proportion of time that the service is actually available for use by the Customers within the agreed service hours.
- ☉ **Maintainability:** Maintainability relates to the ability of an IT infrastructure component to be retained in, or restored to an operational state (e.g. anticipation, detection, diagnosing, resolving and recovery from failures, but also restoration of the data and IT Service and levels of preventative maintenance applied to prevent failures occurring). Maintainability is performed by your own internal business units. Service Level Management will create Operational Level Agreements (OLAs) between the various internal business units to formalise the maintainability. Availability

Management is responsible for ensuring that internal maintenance is performed according to these OLAs.

- ☯ **Serviceability:** Serviceability describes the contractual arrangements made with 3rd party service providers. This is to assure the availability, reliability and maintainability of IT Services and components under their care. Serviceability in itself cannot be measured as a specific metric and is performed by external business units. Service Level Management will create Underpinning Contracts (UCs) with the various external vendors/suppliers to formalise the serviceability. Availability Management is responsible for ensuring that external maintenance is performed according to these UCs.
- ☯ **Security:** The three foundation pillars of security are **confidentiality**, **integrity** and **availability (CIA)**. Confidentiality is the prevention of unauthorised disclosure of data, integrity is the prevention of unauthorised modification of data and availability ensures authorised access to data.

Availability Management improvement techniques:

- ☯ **CRAMM:** Central Computing and Telecommunications Agency Risk Anlalysis Management Methodology (CRAMM) is a Risk Analysis technique and delivers both the methodology to perform the analysis (capturing data on the assets, capturing the data of the various threats and capturing the data on the vulnerabilities) and also the tool/technology that automatically calculates the risks and provides a list with appropriate countermeasures. CRAMM as a technique is used to support a variety of IT Service Management processes but is most effective in addressing Availability Management and IT Service Continuity Management.
- ☯ **FTA:** Fault Tree Anlalysis (FTA) is the process of identifying potential design weaknesses using a highly detailed logic diagram depicting basic faults and events that can lead to system failure and/or safety hazard. It is a systematic way of prospectively examining a design for possible ways in which failure can occur. The analysis considers the possible direct proximate causes that could lead to the event and seeks their origins. Once this is accomplished, ways to avoid these origins and causes must be identified.
- ☯ **CFIA:** Component Failure Impact Anlalysis (CFIA) is a technique where failures of components, typically Configuration Items (CIs) that are part of the IT Infrastructure, are assessed against their likely impact on the business. Components are put in the columns of a matrix; services are put in the rows. Where failure of one component leads to a high number of service interruptions, the component can be regarded as a single point of failure (**SPOF**) and measures should be taken to reduce the risk of such an event occurring (risk mitigation). This can be accomplished by investing in redundant items, selecting reliable components and designing for immediate failover (high availability design).

- ☯ **TOP: Technical Observation Post (TOP)** is a prearranged gathering of specialist technical support staff from within the IT support organisation brought together to focus on specific aspects of IT availability. This technique makes optimal use of the existing knowledge and experience of the IT organisation. Get the IT-brains around the table regularly (e.g. once a fortnight) and let them brainstorm and identify areas of improvement.
- ☯ **SOA: System Outage Aalysis (SOA)** is a technique designed to provide a structured approach to identify end-to-end availability improvement opportunities that deliver benefits to the customers and users. It follows the process of identify underlying causes, assesses effectiveness of the IT support organisation, reports findings and recommendations, initiates an implementation programme and measures availability improvements.
- ☯ **Expanded Incident Lifecycle:** The expanded Incident lifecycle makes optimal use of the data that becomes available with Incident records. Incidents occur (Murphy's Law), and at some stage they become detected and a proper response is needed. Diagnosis can start and after some time a repair (permanent fix/work-around) will be found. If applicable, data and systems will need to be recovered and finally the service can be restored to the user. One will only have to wait until the next Incident occurs. The average time from when the Incidents occur until the time the services are restored to the user is known as the **Mean Time To Repair (MTTR)**. In other words the service will be down: **downtime**. The average time from the moment the service is restored until the next Incident occurs is known as **Mean Time Between Failures (MTBF)**. In other words the service is up and running: **uptime**. The average time between two system Incidents is known as **Mean Time Between System Incidents (MTBSI)**. The MTBSI is a good indication of the reliability of a system/service.
- ☯ **Calculating Availability:** The availability is the time a system/service is available to the user as agreed between IT and the Customer. The formula to calculate availability is $[(\text{Agreed Service Time} - \text{Down Time}) \div (\text{Agreed Service Time})] * 100\%$. The Down Time only counts when it occurs within Agreed Service Time.

11.3 ACTIVITIES

There are basically nine key activities mentioned under the chapter of Availability Management. However, you don't actually need to know all of them for the exam. It is a lot easier to remember the key activities that are part of Deming's continuous wheel of improvement.

Activities

- Determining Availability requirements
- Formulating the Availability and recovery design criteria
- Determining the Vital Business Functions
- Defining Availability, Reliability and Maintainability targets
- Establishing measures and reporting
- Monitoring and trend analysis
- Reviewing IT Service and components
- Investigating unacceptable Availability
- Producing and maintaining the Availability plan



© DIGANO 2006

These activities are:

- ☉ **Plan:** When planning for Availability one must also plan for Recovery. For “business as usual”, the Customer may require the service to be available from Monday to Friday, from 9am until 5pm. At the same time the Customer has a requirement to recover the service within 4 hours when there is an unexpected outage. When the service cannot be recovered within agreed recovery times the Availability process typically moves into the IT Service Continuity Management (ITSCM). Hence Availability Management plans for expected availability requirements, while ITSCM plans for unexpected unavailability.
- ☉ **Do/Implement/Deliver:** The Availability Management process ensures that services can be delivered against business requirements and that the infrastructure is capable of

delivering against these requirements in the present and in the future. This means that Availability Management initiates requests for changes (RFCs) to continuously meet changing availability needs and will act as the single point of contact for all availability related demands, compliments, complaints and issues.

- ☯ **Check/Monitor/Report:** Availability Management measures whether or not services are available against Service Level Agreement targets and will therefore collect data on resources (e.g. availability of a single network component), services (e.g. connectivity end-to-end – from client to server) and business levels (e.g. future anticipated availability requirements from the Customers). All data is collected in the Availability Management Database (**AMDB**) and is analysed, accumulated and processed, so the necessary Availability Management reports can be produced.
- ☯ **Act/Improve:** Where the availability targets cannot be met or are likely not be met in the future, appropriate action should be taken. Availability Management should provide recommendations on how targets will be met with information on approximate costs. Availability Management also has the responsibility of assessing the IT infrastructure for possible improvements relating to availability of services. Working closely together with Capacity Management, new resources should be assessed on their availability, reliability, maintainability, security, performance, etc. The availability plan will need to be updated on a regular interval (e.g. quarterly) to reflect new recommendations, changes in technology and most importantly changed business availability requirements.

11.4 BENEFITS

Benefits:

- ☯ Systems and Services are designed rather than evolutionary grown
- ☯ Critical Services and vital business functionality becomes better understood
- ☯ Providing the availability that is needed, rather than wanted
- ☯ Costs savings by investing in Availability there where it is needed most, and where it provides the best financial and business returns
- ☯ One central point of accountability for all Availability related issues
- ☯ IT Availability levels are cost justified and aligned to current and future business needs
- ☯ Availability levels are agreed, measured, monitored, and continuously improved
- ☯ Shortfalls in Service provision are recognised, and catered for
- ☯ Enhanced business and IT perspective on Availability of Services
- ☯ Frequency and duration of IT Service failures is reduced, and uptime is increased
- ☯ More proactive attitude towards Availability of Services. Less fire fighting, more planning
- ☯ Improved quality of Services, as Availability is one of the cornerstones that creates the whole concept of quality of Services
- ☯ Better aligned to future business direction and the impact on Availability and the infrastructure
- ☯ Increased knowledge and experience with techniques that can be used to increase Availability levels
- ☯ More accurate information available on end-to-end Service Availability

11.5 PROBLEMS

Problems:

- ☹ No full commitment of senior management to invest in the process
- ☹ Justification of costs may be difficult if other IT Service Support processes are already in place
- ☹ Current availability levels already perceived as good enough for IT and the business
- ☹ Resistance to process ownership – no-one wants to be held end-accountable
- ☹ Roles and responsibilities unclear
- ☹ Lack of skills, competencies and proper (reporting) Availability Management tools
- ☹ Lack of mature service management processes (e.g. configuration management and problem management)
- ☹ Targets set at an unrealistically high level
- ☹ Availability Management not performed at a Service or Business level, but only at a Resource level (also see Capacity Management sub-processes)
- ☹ Availability Management resources not properly assigned/distributed
- ☹ No proper alignment with IS and IT strategic plans (or these plans are not in place)
- ☹ The process may drown in useless data without the ability of providing information
- ☹ The process may become IT-driven (vendor driven), rather than driven by the needs of the Business
- ☹ Availability (outages) only measured from an IT point of view, not from a Business point of view
- ☹ The process may become another reactive process, rather than designing and planning for Availability needs

12 CAPACITY MANAGEMENT

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

12.1 GOAL

The **goal** of Capacity Management is to ensure that cost justifiable IT capacity always exists and that it is matched to the current and future identified business requirements.

This process is all about delivering *the right resources, at the right place, at the right time, to the right people, at the right costs*. It is all about doing it just right! Delivering resources too early where they will not be used productively will result in a waste of money; delivering resources too late will often result in lost productivity or lost opportunities. The author likes to refer to this process as the right process. Keywords like resources, performance, response time, utilisation, tuning, throughput, workloads and queuing theory all relate to this process.

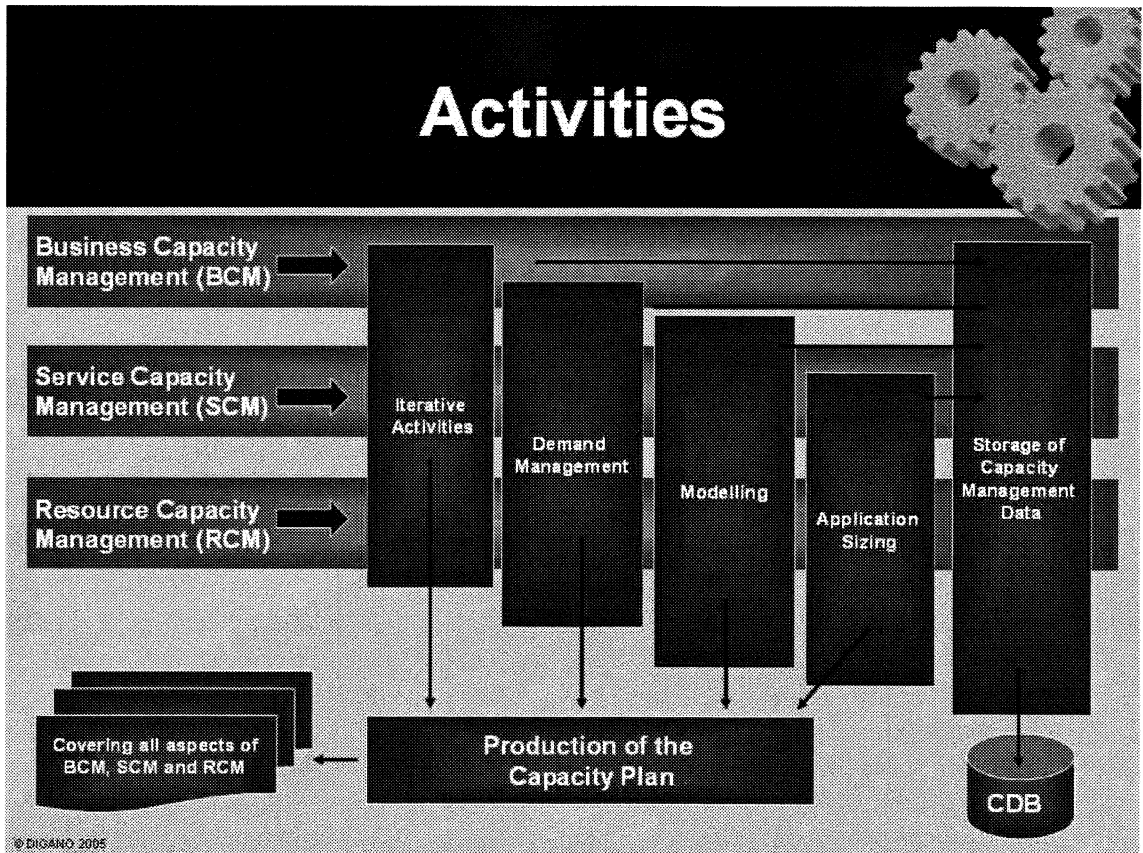
12.2 TERMINOLOGY AND DEFINITIONS

There are three laws you will need to know of that are mentioned under Capacity Management:

- ☉ **Murphy's Law:** If anything can go wrong, it will. The fact that Capacity Management will be introduced into the organisation does not mean that there will be no more capacity related Incidents in the future. Incidents will still occur, but with one big difference: Now there is a process that will assess and try to understand the nature of these Incidents and will look for ways to improve and prevent similar Incidents from happening in the future. As such, a formal and healthy relationship needs to be established between Problem Management and Capacity Management.
- ☉ **Moore's Law:** The number of transistors that can be put on a given space doubles every 18 months. This has been true since 1965 and is expected to be true until at least 2015. In other words: CPUs, and more generically Information Technology, is getting faster and typically also cheaper over time. Should we be buying an 'old' 32-bit processor today, or should we live with some pain and buy a 'new' faster and cheaper 64-bit processor tomorrow. Choices, choices, choices – that is one of the main reasons why we need Capacity Management in place: to make the right choice for the organisation with the support of the other IT Service Management processes (e.g. Availability Management and Change Management).
- ☉ **Parkinson's Law:** Work expands so as to fill the time available for its completion. We can double disk space, double bandwidth, double our screen size until the cows come home. It is imprinted in our human DNA to consume the available resources we are supplied with. We need to proactively manage our resources and set clear expectations with the business and IT that IT resources are not free!

12.3 ACTIVITIES

This process has three identified sub-process levels and eight key activities.



The sub-process levels are:

- ☉ **Resource Capacity Management:** The goal of Resource Capacity Management is to identify and understand capacity and utilisation of components like processors, disks, bandwidth, etc. On this level resources are monitored using the right procedures and tools. On this level RCM pre-empts difficulties by analysing trends and forecasting and addressing any capacity related issues. Emerging new technologies are closely monitored and where applicable assessed against their added-value to the Business and IT. Where capacity related bottlenecks in the IT infrastructure exist, Capacity Management recommends measures to increase the resilience
- ☉ **Service Capacity Management:** The goal of Service Capacity Management is to identify and understand the IT services, their use of resources, their working patterns and their peaks and troughs and to ensure that the IT Services can and do meet their SLA targets. SCM ensures compliance to the SLAs and reports on achievement against targets.

- ☯ **Business Capacity Management:** The goal of Business Capacity Management is to understand the strategy and direction of the business and to align IT decisions with the business. Awareness of emerging technologies will be created with the right business stakeholders so maximal competitive value can be gained at the right time. IT needs to understand what type of services will be added to the existing portfolio of services so resources can be planned proactively rather than reactively. The impact of adding or changing services to the current infrastructure must be assessed on technical feasibility, short- medium and long term costs and affect on the business processes.

The eight key activities of Capacity Management are:

- ☯ **Iterative activities:** The iterative activities or cyclic/repetitive activities consist of monitoring, analysing, making recommendations for tuning/improvement and finally implementation of changes into the live environment (working together with Change and Release Management). When a hard disk is monitored to be running out of disk space, activities need to be initiated to prevent system interruptions due to lack of disk space. A new or bigger hard disk might solve the issue, but a new policy on usage, spreading the load (moving data to other systems), introducing charging for hard space and setting disk quotas may also be potential solutions. Capacity Management will decide what solution is the most practical, cost effective, and beneficial to IT and the Business, and submit a Request for Change (RFC) to Change Management, so the RFC can be properly assessed and scheduled before it is implemented into the live/operational environment.
- ☯ **Demand Management:** The purpose of Demand Management is to influence the demand for computing resource and the use of that resource. It is typically used in scenarios where the organisation is running low in available resources, or it is used to spread the workload/demand evenly to prevent unnecessary and expensive upgrades of hardware or software (e.g. running out of concurrent licences). Where organisations reach peak-utilisation of their resources differential charging can be used to influence the demand of the resources. Usage during peak-hours may than be charged higher than usage during off-peak hours (e.g. mobile phone and utility companies often use this approach). When water supply becomes scarce, prices tend to go up and water usage restrictions become active – these are all examples of Demand Management. **Queuing theory**, that is deciding what type of jobs can run/start simultaneously in system-queues without putting too much demand on the resources, is also performed under the banner of Capacity Management.
- ☯ **Modelling:** The key activity, modelling uses different baseline models and “what-if techniques” to predict future demands that will be placed on the resources and services based on historical, current and future resource, service and business requirements. Some modelling techniques are relatively cheap to perform (e.g. estimation) but are therefore also typically less accurate in their results. Other modelling techniques (e.g. prototyping) will be more accurate but they also come with a higher price-tag. Moving from less accurate (cheap) to more accurate (expensive)

are the following modelling techniques: estimation, trend analysis, analytical modelling, simulation and prototyping.

- ☉ **Application sizing:** The objective of application sizing is to estimate the resource requirements to support a proposed application change or new application, to ensure it meets its required service levels. Whenever you buy a new product off the shelf (e.g. Microsoft Office 2003) have a look on the side of the box. It will provide you with minimal system requirements and will typically also specify the recommended system requirements. Applications sizing data will tell you what type of resources you will need if you want to install the software (e.g. operating systems supported/required, memory, disk-space, CPU, required Service Packs, etc). Application sizing data will often come from the vendor, supplier or your own internal developers and it is exactly here where Capacity Management will have to establish and maintain a strong relationship with the development environment to ensure smooth rollouts of software and hardware into the live environment.
- ☉ **Capturing capacity data:** Business, service, resource, technical, financial and utilisation data needs to be captured so proper analysis and reporting can be performed. Where possible, data should be gathered and processed automatically using systems, IT service management and application management tools. Although data will typically be gathered decentrally by the various IT specialised units (e.g. mainframe-unit, network-unit, server-unit and workstation-unit) a clear holistic overview of how the data actually correlates to each other is vital, as the synergy of components and services working together is larger than the sum of the individual components and services. The capacity database (CDB) needs to represent itself logically as one entity, but could physically exist of a whole variety of databases.
- ☉ **Storing capacity data:** All the collected data will be stored in the logical Capacity Database (CDB). Clear and concise backup and restore, retention, access, data-entry, modification, deletion, maintenance and archival procedures (and work-instructions) must be created to ensure confidentiality, integrity and availability of the stored data. The CDB will be used as the basis for all reporting and capacity planning activities and will most likely contain accumulated historical data for up to a number of years. For some organisations legislation might be driving the data retention period.
- ☉ **Capacity planning:** The capacity plan will typically include an introduction, any assumptions made, management summary, business scenarios, service summary, resource summary, cost models, options for service improvement and other recommendations. The capacity plan provides an overview of where you are now in terms of capacity, where you want or need to be in the future, and how you will get there.
- ☉ **Reporting (providing management information):** Last but not least: There is always reporting! Regular and exception reports will need to be created, checked for accuracy and completeness and delivered to the various stakeholders in the business and IT as agreed within the multitude of agreements and contracts. The manual procedures and supporting technology to produce the reports need to be flexible

enough to support changing business and IT requirements. A flexible and scalable relational database structure, supported by a flexible and scalable reporting tool (e.g. integration with Crystal Report Writer) is highly recommended.

12.4 BENEFITS

Benefits:

- ☯ Getting the right resources at the right time, at the right place, for the right Customers and Users
- ☯ Increased efficiency and cost savings
- ☯ Making optimal use of available resources
- ☯ Deferred expenditure – buying just in time – not too early and not too late
- ☯ Economic provision of services
- ☯ Planned buying, rather than panic buying
- ☯ Reduced risk to the organisation
- ☯ More confident forecasts of resources needed
- ☯ Value to, and better integration with, the applications lifecycle
- ☯ Increased confidence from Customers and Users
- ☯ Decreased number of Capacity related Incidents and Problems
- ☯ A more proactive approach to managing resources
- ☯ Clear understanding of performance, trends, utilisation, peak-and-troughs, and demand
- ☯ Continuous improvement recommendations made to enhance, and align the Infrastructure with changing Business needs
- ☯ Clear accountability of assessment of new technology and resources

12.5 PROBLEMS

Problems:

- ☯ No full commitment of senior management to invest in the process
- ☯ Justification of costs may be difficult if other IT Service Support processes are already in place
- ☯ Current capacity levels already perceived as good enough for IT and the business
- ☯ Resistance to process ownership – no-one wants to be held end-accountable
- ☯ Roles and responsibilities unclear
- ☯ Lack of skills, competencies and proper (reporting) Capacity Management tools
- ☯ Lack of mature service management processes (e.g. configuration management and problem management)
- ☯ Targets set at an unrealistically high level
- ☯ Capacity Management not performed at a Service or Business level, but only at a Resource level
- ☯ Capacity Management resources not properly assigned/distributed
- ☯ No proper alignment with IS and IT strategic plans (or these plans are not in place)
- ☯ The process may drown in useless data without the ability of providing information
- ☯ The process may become IT-driven (vendor driven), rather than driven by the needs of the Business
- ☯ Capacity (related-outages) only measured from an IT point of view, not from a Business point of view
- ☯ The process may become another reactive process, rather than designing and planning for Capacity

13 IT SERVICE CONTINUITY MANAGEMENT

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

13.1 GOAL

The **goal** of IT Service Continuity Management is to support the overall Business Continuity process by ensuring that the required IT technical and services facilities* can be recovered within required, and agreed, business timescales.

*These facilities include computer systems, networks, applications, telecommunications, technical support, and the Service Desk.

13.2 TERMINOLOGY AND DEFINITIONS

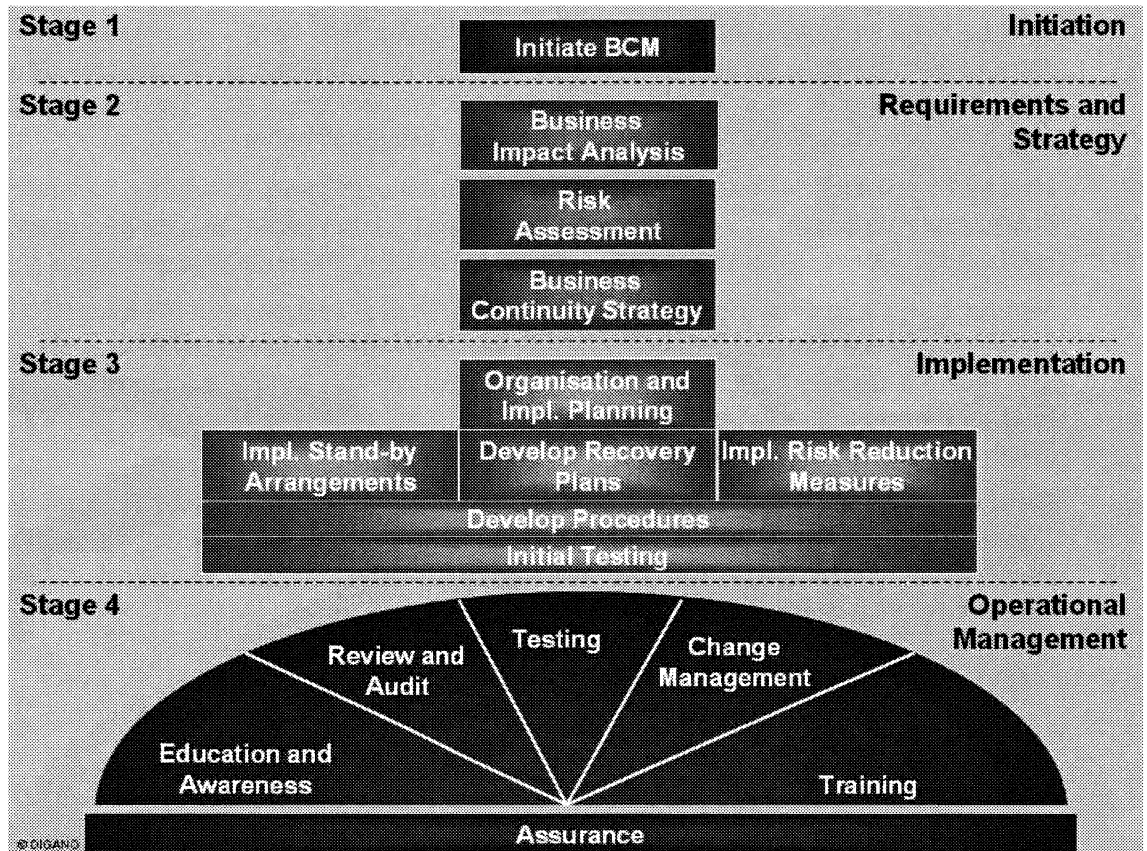
The various countermeasures available:

- ☉ **Do nothing:** In fact you have done a lot already! The BIA has been performed, Risk Analysis has been done, you've assessed the various Risks, impact of those Risks and the likelihood they will occur and finally you make a conscious decision not to invest any resources in risk mitigation.
- ☉ **Manual work-around:** Back to pen-and-paper! If the Incident Management system or the travel booking system fails, Incidents and bookings still need to be recorded. This can be done using paper based forms and templates. As soon as the electronic system is restored, the manually collected data can be transferred back into the system.
- ☉ **Reciprocal arrangement:** This is an arrangement/agreement between two or more business units or organisations. If council ABC uses mainframe type PQR and neighbouring council DEF also uses mainframe type PQR, then a mutual agreement cross covers the continuity of Services for both organisations. These types of arrangements typically exist within government organisations or within large (international) organisations and are less likely to exist between competitive organisations (for obvious reasons).
- ☉ **Gradual recovery (cold start):** A cold start recovery means that it takes more than 72 hours to restore Services to the organisation. Often computer systems will not be available and will have to be organised when the disaster strikes. This type of recovery is suitable for less critical services.
- ☉ **Intermediate recovery (warm start):** The warm start recovery means that it takes between 24 and 72 hours to restore the Services to the organisation. Often computer systems will be available, but the amount of work to restore the services is significant, or it might just take a long time to restore all the applications and data from backup. This type of recovery is suitable for services that have a medium impact on the organisation and are not critical, but also not insignificant.

- ☉ **Immediate recovery (hot start):** The hot start recovery means that it will take less than 24 hours to restore the Services to the organisation. This includes within 5 seconds, but excludes hot-standby which is covered by Availability Management as a form of redundancy/high Availability. The hot start recovery option is suitable for critical services as these typically need to be restored within the least amount of time to minimise impact and losses to the organisation.
- ☉ **Dormant contracts:** Dormant contracts are 'sleeping contracts' an organisation has with its vendors and/or suppliers. The vendor/supplier will keep a number of spare parts (whole systems) on the shelves and will typically fast-courier the systems to a pre-defined location so emergency restoration of services can start. The equipment may have been prepaid or an annual fee may apply using this option.
- ☉ **Fortress approach:** If the organisation has no option to move to another location, then the premises will have to be made as secure (disaster-proof) as possible (cost-justifiable). Good examples are Fort-Knox, the Pentagon, and telephone exchanges.
- ☉ **Mobile hot start:** The mobile hot start option is the 'computer-on-the-back-of-a-lorry'! Computer systems and network infrastructure will be placed inside a truck or van and in a disaster scenario operations will run from this mobile computer centre. For those who remember the series Knight-Rider, think of the big black truck that was filled with computer systems – that's a mobile hot start!
- ☉ **Insurance:** Another option is insurance. To some degree the whole IT Service Continuity Management process can be seen as a form of insurance. A disaster might never strike your organisation, but then again, it might happen tomorrow. The insurance payout can be used to revive the business and services.

13.3 ACTIVITIES

Although the ITIL definition of a process is 'a set of interrelated activities and or sub-processes...' the author of the chapter IT Service Continuity Management deemed it necessary to introduce the terminology **stages**. Please think of stages as being sub-processes for the sake of consistency in terminology used.



The IT Service Continuity Management (ITSCM) process consists of four main stages (sub-processes). The four main stages are:

- ☉ **Initiation:** The initiation stage is all about kick-starting the process. Business and IT Service Continuity policies need to be created, as well as terms of reference documents. A clear scope needs to be set and resources need to be allocated. Both the project organisation and the control structure need to be defined, and project plans and quality plans need to be agreed on. This stage is all about getting ready! Don't forget the three key process control components (goals, process owner, and KPIs), and commitment and involvement from senior management either as they are all key to the success of any ITIL process implementation.
- ☉ **Requirements and strategy:** The requirements and strategy stage is all about

understanding the risks and understanding the various risk mitigation countermeasures that are available. This stage has four key activities. The first activity is conducting a **Business Impact Analysis (BIA)**. This activity focuses on understanding the financial and business impact of outages (of your assets) on the services provided. Realise that impact might also be loss of trust or image with your customers. This activity will clearly separate the business critical services and business critical service times from the less critical ones. The second activity is analysing the risks, hence it is referred to as **Risk Analysis**. The **Office of Government Commerce (OGC)** offers a risk analysis methodology with the name **CCTA Risk Analysis Management Methodology (CRAMM)**. CRAMM allows any organisation to calculate its risks by assessing the combination of **assets, threats and vulnerabilities** that relate to the services provided. An email administrator is an asset, an email virus is a potential threat and as an organisation you will be more vulnerable without an up-to-date email virus scanner in place. The combination of risk, impact and likelihood will identify the amount of resources an organisation will have to invest in taking the appropriate countermeasures. Understanding the various countermeasures and prioritising them is known as **Risk Management** and this is the third key activity of this stage. The second activity (Risk Analysis) and third activity (Risk Management) combined are also known as **Risk Assessment**, so Risk Analysis + Risk Management = Risk Assessment. The fourth and final activity of this stage is designing and agreeing on a **Business Continuity Strategy**. This activity focuses on service recovery priorities (which service must be recovered first, second, third and so on), and also monitors changes to service recovery priorities based over time. It considers the various risk reduction and recovery options and allocates resources using the knowledge that it is impossible to completely eliminate all risks. It checks the capability of recovery implementation and also checks for any integration issues that the sequence of recovery may result in.

☯ **Implementation:** In this stage the supporting organisation is established, roles and responsibilities are assigned and service continuity management implementation plans are developed. The proper stand-by arrangements with providers of disaster recovery facilities are established and the various risk reduction measures are implemented. The recovery plans are created, covering both the technical side of service and system recovery, but also the people side of recovery, covering areas like transport, accommodation and health, safety and security. Procedures and work-instructions are created covering all aspects of the recovery from where do we find the tapes up to who is allowed to fly on the same airplane. Typically in a disaster scenario people do not have time to think about what they need to do next – all actions need to be scripted and planned beforehand. The final activity of the implementation stage is performing initial testing, making sure everything works and nothing is overseen. It is the small things that are often overlooked, like making sure people can get to the remote disaster recovery site on time using the public transport on a Sunday, and informing the external maintenance suppliers of the new contact numbers.

☯ **Operational Management:** Whereas the first three stages are all planning related,

stage four is considered to be the operational stage where the disaster recovery plans are maintained, and updated. It is absolutely crucial to the success of ITSCM that all those involved in the recovery of the services and systems are properly trained. This 'drilling' is vital as people need to know what to do, whom to contact, and where to go, without reading thousands of pages of manuals first. It is like keeping the crew of an airplane, oil-platform or emergency rescue unit on the tip of their toes at all times, so when it really comes to a disaster they are able to operate at maximum performance recovering systems and services with minimum downtime to the business. The disaster recovery plans, knowledge and skills of the people involved, and the recovery technology used will need to be reviewed on a regular basis so proper corrective actions can be initiated ensuring the process, people and technology are adequate to support the business disaster recovery related requirements. Regular testing (partial and/or full testing) is required to spot any irregularities and issues that may arise during recovery of services and to proactively initiate any corrective countermeasures, rather than panicking and ending up in a reactive fire fighting mode if recovery does not seem to work properly. Testing should be performed at least annually, if possible more regularly, randomly, after major changes (with a large potential impact on the organisation) and may be legislatively driven. If the disaster recovery plans/IT service continuity plans are not properly maintained and updated in pace with the changing operational infrastructure, they will become outdated and worthless within no time at all. These plans are not shelf-ware or dust-ware, but are dynamic documents that need continuous attention and, if applicable, revision. Every change being assessed should also be assessed against its impact on the current disaster recovery plans – the change could mean that plans need to be updated and tested again. It is recommended to put ITSCM-impact on the checklist that Change Management uses when assessing changes. ITSCM needs and deserves a tick-in-the-Change-Management-box! The last activity of this stage is the quality assurance, although it actually makes more sense to approach this activity as a separate stage. The IT Service Continuity Management process needs to be quality controlled and this can be performed by an internal quality assurance business unit or may be performed by an external organisation specialised in the assessment of this process. For many organisations quality assessment is legislated and non-conformance may have serious consequences to the continuity, and even very existence, of the organisation.

13.4 BENEFITS

Benefits:

- ☯ Potential lower insurance premiums as ITSCM will bear some of the risks that the insurance companies typically bear
- ☯ Meeting regulatory requirements as set by local, state and federal Government/s
- ☯ Improved relationships between IT and the Business
- ☯ Positive marketing of contingency capabilities
- ☯ Organisational credibility
- ☯ Competitive advantage to those that have no contingency plans in place
- ☯ Increased continuity of the Business even in the case of unexpected unavailability
- ☯ Clear delineation line between Availability and IT Service Continuity
- ☯ Reducing risks by eliminating the most obvious one (risk mitigation) – preventing/reducing risks is often cheaper than applying bandages (curing the disease) afterwards
- ☯ Clear roles and responsibilities assigned before and during disasters
- ☯ Trained (drilled) disaster management teams in place to take immediate action when an unexpected outage (disaster) strikes
- ☯ Formalised, maintained, distributed, and communicated contingency plan/s in place
- ☯ Proactive identification of potential single point/s of failure
- ☯ Clear understanding of the Business impact of business process, Service, and System unavailability
- ☯ Increased understanding of organisational assets, threats, and vulnerabilities

13.5 PROBLEMS

Problems:

- ☯ No full commitment of senior management to invest in the process
- ☯ Justification of costs may be difficult if no real threats are felt or seen by the business
- ☯ Roles and responsibilities unclear
- ☯ Lack of skills, competencies and proper (reporting) IT Service Continuity Management tools
- ☯ Lack of mature service management processes (e.g. Service Level Management, Capacity Management, and Security Management)
- ☯ Recovery targets set at an unrealistically high level
- ☯ IT Service Continuity Management not performed at Business level, but only at a technical level
- ☯ IT Service Continuity Management resources not properly assigned/distributed (e.g. all effort goes into the centralised systems)
- ☯ No proper alignment with IS and IT strategic plans (or these plans are not in place)
- ☯ Full tests might not be possible due to incompatible test or disaster recovery infrastructures
- ☯ Ongoing awareness and involvement (the process is seen as a once-off activity)
- ☯ Keeping the plans up-to-date/in-sync with all Business and IT changes
- ☯ Not all areas included (no full BCM) (typically this means not Business driven)
- ☯ Too much emphasis on the recovery of technology and not on the people or processes
- ☯ Time-zones and cultural differences

14 SECURITY MANAGEMENT

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

14.1 GOAL

The **goal** of security management is twofold:

- ☉ First to meet the *external* security requirements. These result from the security requirements in various SLAs. These external requirements for security also stem from contracts, legislations and any imposed security policy.
- ☉ Second to meet the *internal* security requirements. This is required to assure the IT service provider's own continuity. It is also necessary to simplify the Service Level Management for information security. After all, managing a large number of different SLAs is much more complex than managing a small number. Therefore, for instance, a certain basic level of security (the so-called **standard security baseline**) needs to be established.

14.2 TERMINOLOGY AND DEFINITIONS

Value of information: Information security is intended to safeguard information. Security is the means of achieving an acceptable level of residual risks. The value of the information has to be protected. This value is determined in terms of confidentiality, integrity and availability:

- ☉ **Confidentiality:** protecting sensitive information from unauthorised disclosure or intelligible interception
- ☉ **Integrity:** safeguarding the accuracy and completeness of information and software
- ☉ **Availability:** ensuring that information and vital IT services are available when required

An organisation can only operate properly if it has access to confidential, accurate and complete information at the right time.

Security Measures: Security Measures make it possible to reduce or eliminate the risks associated with information and IT. The starting point for these measures is to have a good security organisation, with clear responsibilities and tasks, guidelines, reporting procedures and measures that are properly matched to the needs of the business and the IT.

- ☉ **Physical** security measures involve protection at a physical level such as building access, server room access, elevator security, etc.
- ☉ **Technical** security measures involve using technology to manage the security. This includes features such as firewalls, virus protection, encryption, etc.
- ☉ **Procedural** security measures describe how staff is required to act in certain situations and in particular cases.

The security organisation needs to maintain a balanced focus on each of these security measures. Security measures can be used at a number of points in the security incident lifecycle:

- ☉ **Security threats:** Security threats are always out there and won't disappear easily. This is why the organisation needs to understand how vulnerable it is and what type of countermeasures it should take to reduce security related risks.
- ☉ **Prevention:** Security measures can be used to prevent security incidents from taking place. E.g. If you're not using email you won't be hit by email viruses.
- ☉ **Reduction:** Security measures can be used to reduce the likelihood of a security incident taking place. E.g. limiting access rights and using technologies such as firewalls and antivirus scanning software.
- ☉ **Detection:** Once a security incident has taken place, measures can be put into place to detect this breach ASAP. E.g. network monitoring tools, virus software, etc.
- ☉ **Repression:** Once a security incident has been detected, measures are needed to limit the amount of exposure or damage which may be caused by the incident. E.g. ensuring that backups are run regularly
- ☉ **Correction:** Measures need to be in place to correct and repair any damage that may have been incurred as a result of a security incident. E.g. restoring from backup, etc.
- ☉ **Evaluation:** It is important that time is spent reviewing security incidents and understanding how they happened, and what could be done in the future to prevent the recurrence of such an incident.

Managing information security: The starting point for the management of information security is proper organisation. This has a waterfall effect, and needs to be actioned in the right order as shown below:

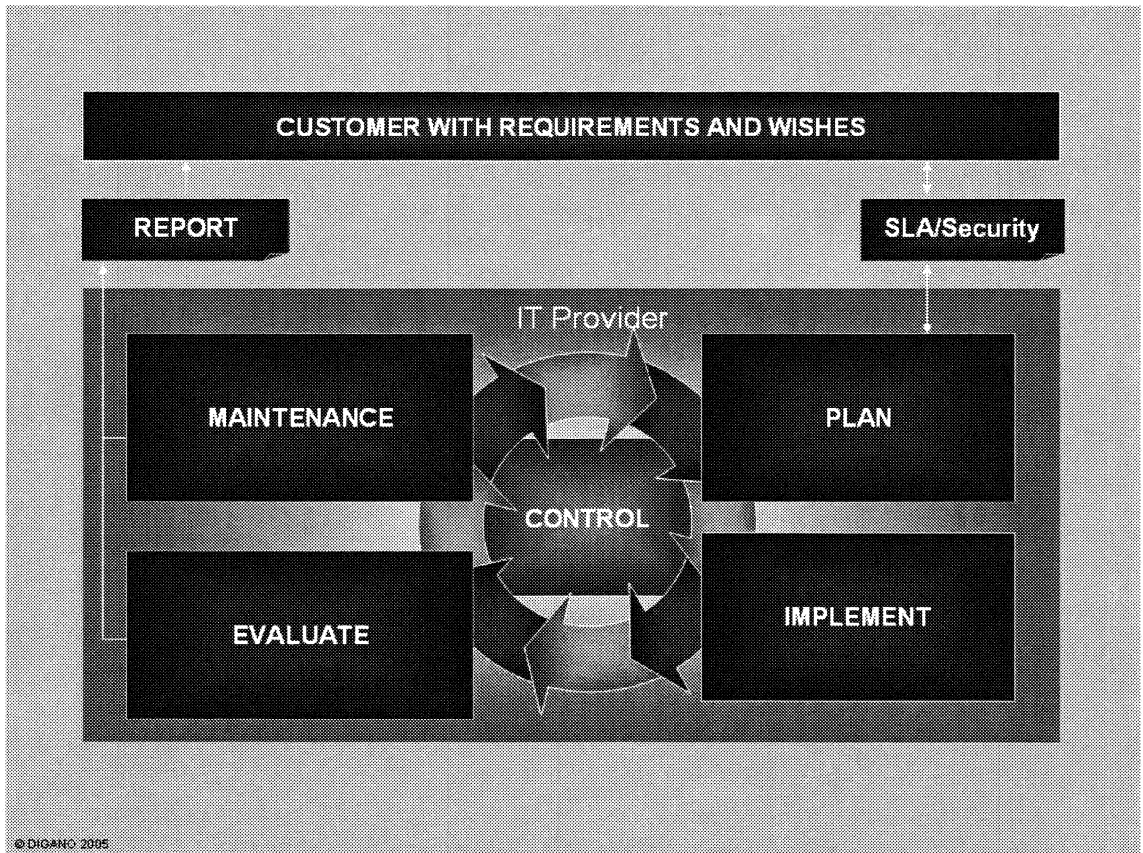
- ☉ Policy and/ or codes of conduct (the objectives we are aiming for).
- ☉ Process descriptions (what has to happen to achieve the objectives).
- ☉ Procedures (who does what and when).
- ☉ Work instructions (how do we specifically do that and when and where).
- ☉ Job descriptions (who is supposed to do what).

Internal and External Influence: Maintaining information security is an iterative process. All the factors that influence its success (and therefore must be acted upon) are seen as inputs. There are internal and external influences that have their effect on information security. The internal influences are caused by decisions within the organisation. External influences are influences that come from the environment in which the business processes take place. This makes security management a challenge. Effective security management depends on accurate risk analysis so that knowledge of the impact of risks and the cost of avoidance is understood.

Security Management and Availability Management: Every aspect of IT Service Management has Security Management considerations. There is a specific relationship with Availability Management – one of the prime aspects of security is availability – and through this, business continuity.

14.3 ACTIVITIES

There are basically six key activities within Security Management.



The activities are:

- ☉ **Control:** The control activity organises and directs the IT Security Management process itself. This includes the organisation of the management framework for information security. The management framework contains the way the security plans are established, the way in which the implementation is evaluated, the process through which the results of these evaluations are used for the maintenance of the security plans and their implementation, and, finally, the reporting structure to the customer.
- ☉ **Plan:** The plan activity includes the way the security section of the SLA is established as well as the underpinning contracts. The generic security requirements in the SLA are refined in Operational Level Agreements (OLAs). They define support requirements internally (e.g print server availability, network up-time, etc.). With respect to Security Management, these OLAs can be seen as the more detailed security plans for the organisational units of the IT service provider as well as the security handbook plans for the IT platforms. Where the IT organisation also has its own

dependencies with external providers of services to deliver its services to its own customers (e.g. external security organisations delivering security guards and monitoring capability), the proper Underpinning Contracts (UCs) need to be established. The IT organisation needs to cover the services and products it wants to deliver to its customers 'back-to-back' before it starts to deliver and commit to any service targets. It's getting your house in order first before inviting the guests.

- ☯ **Implement:** The implement activity implements the measures as defined in the plans. This may include activities such as creating awareness, classification and registration, personnel security, physical security, security management of infrastructure components, control and management of access rights, and security incident handling and registration.
- ☯ **Evaluate:** Evaluation is indispensable to close the loop of the Security Management system. It concerns the status and effectiveness of measures taken, but also concerns standards and policy. Evaluating results will provide feedback on the measures in operations. It may even indicate the need for a review of the measures which are currently being undertaken. When this review results in a need for change, a "Request for Change" (RFC) will be submitted to the change management process. There are essentially three types of evaluation which are accepted: Internal audits (reviews performed by internal auditors), external audits (reviews performed by external, independent auditors) and self Assessments (performed within the line organisation itself).
- ☯ **Maintenance:** The maintenance of security measures is based on the results of the periodic reviews, insight into the changing risk picture, and, of course, changes in the input material (i.e. the security section in the SLA). The latter changes can also be made on the basis of new customer requirements. Another way of maintaining security measures is through the control of changes in the infrastructure as outlined above.
- ☯ **Report:** Reporting is an activity in itself, although it is largely dependent on the results from other activities. Reporting takes place, for example, to support the control activities. One of the reasons for the ineffectiveness of Security measures in the past may have been because of the lack of reporting information. A lack of historical records and analyses will make the identification of problem areas difficult.

14.4 BENEFITS

Benefits:

- ☯ Security level set to meet business requirements
- ☯ Possible regulatory requirements
- ☯ Assurance to the business
- ☯ Confidence in Services provided by IT
- ☯ Increased IT credibility
- ☯ Cost justified level of Security
- ☯ Audit and review savings by means of a measurable documented set of policies, procedures and work-instructions
- ☯ Increased Business relationships/communication - breaking down barriers
- ☯ Increased cultural awareness of Security and its potential impact on the organisation
- ☯ Targeting of Security countermeasures/resources as a result on an increased understanding of the various assets, threats and vulnerabilities
- ☯ Security baseline and policy, which enable rapid identification of any Security Incidents and/or failings
- ☯ Meeting regulatory requirements as set by local, state and federal Government/s
- ☯ Consistent approach to all Security reviews
- ☯ Clear roles and responsibilities for all personnel involved
- ☯ Ensures confidentiality, integrity and availability of information and systems to a level that is required by the Business and IT

14.5 PROBLEMS

Problems:

- ☯ No full commitment of senior management to invest in the process
- ☯ Justification of costs may be difficult if other IT Service Support processes are already in place
- ☯ Current security levels already perceived as good enough for IT and the business
- ☯ Resistance to process ownership – no-one wants to be held end-accountable
- ☯ Roles and responsibilities unclear
- ☯ Lack of skills, competencies and proper (reporting) Security Management tools
- ☯ Lack of mature service management processes (e.g. Service Level Management, Capacity Management, Availability Management and IT Service Continuity Management)
- ☯ Targets are unclear or unrealistic
- ☯ Security Management not performed at a Service or Business level, but only at a Resource/technical level
- ☯ Security Management seen as something that needs to be managed by IT
- ☯ No proper alignment with IS and IT strategic plans (or these plans are not in place)
- ☯ Not enough knowledge and skills available to implement and maintain the process
- ☯ The process may become IT-driven (vendor driven), rather than driven by the needs of the Business
- ☯ Security Incidents only measured from an IT point of view, not from a Business point of view
- ☯ Business has no clear understanding of what “cost-effective” level of security is required

15 ACRONYMS USED

The Hitchhiker's Guide to ITIL – EXAM Preparation Guide

ABC	Activity Based Costing
AMDB	Availability Management Database
AST	Agreed Service Time
BCM	Business Continuity Management
BCP	Business Continuity Planning
BIA	Business Impact Analysis
BU	Business Unit
CAB	Change Advisory Board
CAB/EC	Change Advisory Board/Emergency Committee
CDB	Capacity Database
CFIA	Component Failure Impact Analysis
CI	Configuration Item
CIA	Confidentiality, Integrity and Availability
CMDB	Configuration Management Database
COE	Common Operating Environment
CRAMM	Central Computing and Telecommunications Agency Risk Analysis Management Methodology
CSF	Critical Success Factor
DHS	Definitive Hardware Store
DSL	Definitive Software Library
DT	Downtime
EDP	Electronic Data Processing
EXIN	Examination Institute for Information Science
FSC	Forward Schedule of Change
FTA	Fault Tree Analysis
GNOC	Global Network Operations Centre
ICT	Information and Communication Technology

ISEB	Information Systems Examination Board
IT	Information Technology
IT/EC	Information Technology/Executive Committee
ITIL	Information Technology Infrastructure Library
ITSCM	Information Technology Service Continuity Management
ITSM	Information Technology Service Management
ITSMF	Information Technology Service Management Forum
KE	Known Error
KER	Known Error Record
KPI	Key Performance Indicator
MOR	Management of Risk
MTBF	Mean Time Between Failures
MTBSI	Mean Time Between System Incidents
MTTR	Mean Time To Repair
OGC	Office of Government Commerce
OLA	Operational Level Agreement
PICAR	Planning, Identification, Control, Status Accounting, Audit and Verification, and Reporting
PIR	Post Implementation Review
PPP	People, Processes and Products
PRINCE2	Projects in Controlled Environments 2
PSA	Projected Service Availability
QA	Quality Assurance
RAID	Redundant Array of Inexpensive Disks
RCM	Resource Capacity Management
RFC	Request For Change
RFID	Radio Frequency Identifier
ROCE	Return On Capital Employed
ROI	Return On Investment
SAM	Software Asset Management
SCM	Service Capacity Management

SLM	Service Level Management
SLR	Service Level Requirements
SMO	Service Maintenance Objectives
SOA	System Outage Analysis
SOE	Standard Operating Environment
SPOC	Single Point Of Contact
SPOF	Single Point Of Failure
SSADM	Structured Systems Analysis Development Methodology
TCO	Total Cost of Ownership
TOP	Technical Observation Post
UC	Underpinning Contract
VBF	Vital Business Functionality
VR ³ AMS ²	Vital Business Functionality, Reliability, Redundancy, Resilience, Availability, Maintainability, Serviceability, and Security
WIIFM	What's In It For Me

ITIL

Foundation Certificate in IT Service Management

(ITIL Foundation)

sample examination

Contents

2	introduction
4	sample questions
14	answer key

Place in the qualification structure

This is the sample examination for the Foundation Certificate in IT Service Management (ITIL Foundation).

Composition of the sample examination

This sample examination consists of 40 multiple-choice questions. These questions are representative of those asked during an actual examination. The questions are designed to fulfil the examination requirements for the ITIL Foundation module specified in the ITIL, PRINCE2, ISPL and DSDM 2001-2002 examination plan.

Each question in this sample examination is multiple choice, with only one correct answer.

Distribution of the questions across the examination requirements

The 40 questions in this sample examination cover the examination requirements as illustrated in the table below. The questions in the examination are not arranged in the order of examination requirement, but are in random sequence.

examination requirement	number of questions	question number in sample examination
General (1, 2)	3	2, 22, 32
ITIL processes (3, 4)		
Service desk	3	1, 13, 27
Incident Management	4	3, 10, 19, 24
Problem Management	5	4, 18, 20, 35, 36
Change Management	6	5, 6, 25, 34, 37, 40
Configuration Management	5	7, 26, 28, 33, 38
Release Management	2	11, 29
Service Level Management	3	12, 16, 30
Availability Management	2	17, 39
Capacity Management	2	14, 23
IT Service Continuity Management	2	8, 21
Financial Management for IT Services	1	15
Security Management	2	9, 31

Literature, notes and calculator

When taking the examination, you may not use literature, notes or a (pre-programmable) calculator.

Time

You have 60 minutes to complete this examination.

Examination scoring

Each correct answer earns 1 point, for a maximum possible score of 40 points. A score of 26 points or more is considered a passing grade.

- 1 Which of the following is a Service desk activity?
- A. functioning as the first point of contact for the customer
 - B. investigating the cause of disruptions for the customer
 - C. tracing the cause of incidents
- 2 What is the role of ITIL within IT Service Management?
- A. to provide an approach based on the best examples from practice
 - B. to serve as the international norm for IT Service Management
 - C. to serve as the standard model for IT service provision
 - D. to serve as a theoretical framework for process design
- 3 The network managers are completely overloaded with work. They rarely have time to proactively manage the network. One of the reasons is that they are contacted directly by users to resolve all sorts of disruptions.

What ITIL process would improve this situation?

- A. Change Management
 - B. Configuration Management
 - C. Incident Management
 - D. Problem Management
- 4 Which of the following tasks is the responsibility of Problem Management?
- A. coordinating all modifications to the IT infrastructure
 - B. recording incidents for later study
 - C. approving all modifications made to the Known Error database
 - D. signalling any user needs and modifying the IT infrastructure based on these needs
- 5 Data in the Configuration Management Database (CMDB) may only be modified after permission is granted to modify the infrastructure.

What process grants this permission?


- A. Change Management
- B. Configuration Management
- C. Incident Management
- D. Service Level Management

6 Which of the following concepts is part of Change Management?

- A. post implementation review (evaluation after implementation)
- B. emergency release
- C. service request
- D. work-around

7 A user receives a new PC that is linked to the network. His old PC is installed as a print server for the local network.

What process is responsible for registering this modification in the Configuration Management Database (CMDB)?

- 
- A. Change Management
 - B. Configuration Management
 - C. Problem Management
 - D. Release Management

8 Over the years an insurance broker has become more and more dependent on its information systems. Thus, the decision has been made that there must be assurances regarding IT service provision following an interruption to the business.

What process should be set up to assure this?

- 
- A. Availability Management
 - B. IT Service Continuity Management
 - C. Service Level Management
 - D. Service Management

9 The data for financial administration is only to be made accessible to authorised users. The security management function takes steps to ensure this is so.

What aspect of the data is ensured by the security management function taking these steps?

- A. Availability
- B. Integrity
- C. Stability
- D. Confidentiality

10 A computer operator sees that a disk is about to become full.

To what ITIL process must he report this?

- A. Availability Management
- B. Capacity Management
- C. Change Management
- D. Incident Management

11 For which of the following activities is Release Management responsible?

- A. checking whether there is any illegal software on the computers within the organization *configuration management*
- B. saving the original copies of all authorized software within the organization
- C. registering the location of each version of the software

12 For what purposes does Service Level Management use data from the service desk's incident registration?

- A. to draw up service level agreements (SLAs) ~~configuration management~~
- B. to draw up reports regarding the number and nature of incidents that occurred during a specific period *incident mgt*
- C. to determine the availability of an IT service using the number of resolved incidents *availability mgt*
- D. to use together with other data to check whether the agreed upon service level is being provided

13 The service desk has handled 2317 calls this month.

What would be the reason for most of these calls?

- A. modifications to Service Level Agreements (SLAs)
- B. notices regarding modified Configuration Items (CIs)
- C. requests to the IT organization for user support

14 A steel company is merging with a competitor. The IT departments, along with the IT infrastructures of both companies will be combined.

What process is responsible for determining the disk and memory space that will be required for applications running in the combined IT infrastructure?

- A. Application Management
- B. Capacity Management
- C. Computer Operations Management
- D. Release Management

15 Which concept is not part of Financial Management for IT Services?

- A. Budgeting
- B. Charging
- C. Procuring
- D. Costing of services

16 Service level requirements are used in the service level management process.

What do these service level requirements represent?

- A. the customer's expectations and needs regarding the service
- B. what the IT organization expects of the customer
- C. the conditions required for the Service Level Agreement (SLA)
- D. a paragraph of the SLA with additional specifications required to execute the SLA

17 Which of the following is one of the goals of Availability Management?

- A. entering into contracts with suppliers ← service level management
- B. monitoring the availability of a charge-through system
- C. verifying the reliability and the service level of the configuration items (CIs) purchased from and maintained by third parties ← service ab
- D. planning and managing the reliability and availability of the Service Level Agreements ←

18 A user calls the service desk with the complaint that an error continually occurs when using a specific application. This causes the connection with the network to be broken.

Which ITIL process is responsible for tracing the cause?

- A. Availability Management
- B. Incident Management
- C. Problem Management
- D. Release Management

19 A serious incident has occurred. The assigned solution team cannot resolve the problem within the agreed time. The Incident Manager is called in.

What form of escalation is involved here?

- A. formal escalation
- B. functional escalation
- C. hierarchical escalation
- D. operational escalation

20 Which of the following is the best description of a Problem?

- A. another term for one or more known errors
- B. a known cause of one or more disruptions
- C. the unknown cause of one or more incidents
- D. a known error with one or more incidents

21 Which of the following concepts is part of IT Service Continuity Management?

- A. Application Sizing *capacity*
- B. Vulnerability
- C. Maintainability *} availability*
- D. Resilience

22 How does IT Service Management contribute to the quality of IT service provision?

- A. by recording agreements between internal and external customers and suppliers in formal documents
- B. by defining generally accepted norms for Service Levels *SLM not acceptable*
- C. by promoting a customer focus among all the employees in the IT organization
- D. by setting up processes for the creating of services, ensuring that services are manageable, and harmonising them

23 Demand Management and Resource Management are parts of what process?

- A. Availability Management
- B. Capacity Management
- C. IT Service Continuity Management
- D. Service Level Management

24 The steps in the Incident Management process might best be described as:

- A. Incident recording and alerting, initial support and classification, investigation and diagnosis, resolution and recovery, closure.
- B. Incident recording, initial codification and allocation, trend analysis, problem resolution, maintaining customer contact, service recovery.
- C. First line incident support, day to day contact with users, business system support, management reporting on IT services quality.

25 Company ABC believes it is important that each request for the set up and connection of a new workstation be handled as efficiently and effectively as possible.

RFC

What ITIL process is designed to ensure this outcome?

- A. Change Management
- B. Customer Liaison
- C. Problem Management
- D. Service Level Management

26 Which of the following can be considered a Configuration Item (CI)?

- A. a call
- B. documentation
- C. an incident
- D. a process

27 How does Problem Management support the activities of the service desk?

Problem Management...

- A. resolves serious incidents for the service desk.
- B. studies all incidents the service desk resolves.
- C. relieves the service desk by communicating a solution for a problem directly to the users.
- D. makes information regarding a known error available to the service desk.

28 What is the correct description of 'impact'?

- A. The degree to which the provision of services is disrupted and the speed with which this must be remedied
- B. The degree to which the user indicates how quickly the incident must be resolved.
- C. The effect that an incident has on the components of the IT infrastructure, including the consequences for the service that has been agreed upon.
- D. The effect that an incident has on the activities of the users and the speed with which the incidents must be resolved.

29 Which of the following is the role of the Definitive Software Library (DSL) in the Release Management process?

- A. a (physical) storage area for the original versions of all authorized software in use
- B. a reference work that includes all software documentation (manuals and the like)
- C. a registration tool for all software items
- D. a type of Configuration Management Database (CMDB) for software

30 The Network department within an organization has made an agreement with an external organization in order to fulfil an agreement with its internal customer.

In which of the following would the agreement with the external organization be specified?

- A. Operational Level Agreement (OLA)
- B. Service Level Agreement (SLA)
- C. Service Level Requirements (SLR)
- D. Underpinning Contract (UC)

31 How does Availability Management work together with Security Management?

Security over

- A. by making agreements regarding the availability of the Security database
- B. by making agreements regarding the security of the Availability database
- C. by establishing the security boundaries based on the availability requirements
- D. by implementing the measures specified by security management for securing the data

32 If a company decides to charge its internal customers for the IT services they use in order to improve general cost awareness, which function will make sure that the charges and the services to which they relate are formally agreed and documented?

- A. Service Level Management.
- B. Financial Management for IT Services.
- C. Local Management.
- D. Customer Management.

33 Which of the following is a Configuration Management task?

- A. convening the Configuration Advisory Board
- B. physically managing software items
- C. installing equipment at the workplace
- D. recording the relationships between Configuration Items (CIs)

34 After the requisite search, the common cause of a series of comparable incidents is found. This has resulted in a known error.

What will generally happen now?

- A. All incidents must be resolved as quickly as possible.
- B. A request for change form will be completed recommending a resolution.
- C. The error must be included in the Configuration Management Database (CMDB).
- D. The problem in question must be identified.

35 What is the primary task of error control?

- A. to come up with and work out the details for work-arounds
 - B. to resolve known errors through the Change Management process
 - C. to recognize and register known errors
 - D. to register and manage known errors
- THE ^{update} Known Data.

36 What ITIL process is associated with the concept of a post implementation review (an evaluation after an implementation)?

- A. Application Management
- B. Incident Management
- C. Change Management
- D. Release Management

37 Consider the following statements; which is NOT true?

- A. Change Management is responsible for providing a detailed specification of the effect on CIs of an authorised change. done b ← exp
- HH B. Change Management keeps a record of all changes by logging, tracking and reviewing them.
- C. Change Management receives, records and helps allocate priorities to all RFCs.
- D. Change Management will ensure that adequate back-out plans are prepared before changes are implemented.

38 What is the difference between Asset Management and Configuration Management?

- A. Asset Management only deals with what you own; Configuration Management deals with everything in your infrastructure.
- B. Asset Management is a superset of Configuration Management, as it includes non-IT assets such as chairs and tables.
- C. Asset Management deals with the financial aspects of Configuration Items; Configuration Management only deals with the technical details of the infrastructure.
- D. Configuration Management includes more details than Asset Management, by specifying the relationships between the assets.

39 For what ITIL process is Mean Time Between Failures (MTBF) a commonly used concept?

- A. Availability Management
- B. Capacity Management
- C. IT Service Continuity Management
- D. Service Level Management

40 A company sets up an Intranet and starts using graphic design workstations. Because a lot of illustrations are transmitted over the network, more bandwidth is needed, and the network capacity has to be expanded.

What process must approve the implementation of the capacity expansion?

- A. Capacity Management
- B. Change Management
- C. Availability Management
- D. Problem Management

The evaluation

Examination results

A maximum of 40 points can be earned on an ITIL Foundation examination.

A score of 26 points or higher is considered a passing grade.

The following table relates the number of points earned to a grade.

A maximum of 40 points can be earned on an ITIL Foundation examination.

A score of 26 points or higher is considered a passing grade.

The following table relates the number of points earned to a grade.

failed

number of points earned	grade
0 – 11	1
12 – 15	2
16 – 18	3
19 – 22	4
23 – 25	5

passed

number of points earned	grade
26 – 29	6
30 – 32	7
33 – 36	8
37 – 39	9
40	10

Sample examination

The table below shows the correct answers to the questions in this sample examination.

number	answer	points
1	A	1
2	A	1
3	C	1
4	C	1
5	A	1
6	A	1
7	B	1
8	B	1
9	D	1
10	D	1
11	B	1
12	D	1
13	C	1
14	B	1
15	C	1
16	A	1
17	C	1
18	C	1
19	C	1
20	C	1

number	answer	points
21	B	1
22	D	1
23	B	1
24	A	1
25	A	1
26	B	1
27	D	1
28	C	1
29	A	1
30	D	1
31	D	1
32	A	1
33	D	1
34	B	1
35	B	1
36	C	1
37	A	1
38	D	1
39	A	1
40	B	1

1.

Apply Impact, i.e. the number of customers affected. Due to the nature of the company organisation, the hierarchical position of the customer is included in this variable.

Impact	Description
1	Whole Organisation, Complete section/department or revenue system affected
2	Executive* and/or Several customers affected
3	One customer affected (no executive involved)

*Executive is defined as the company staff directly reporting to the managing director and their PA's.

2.

Apply Urgency; i.e. how severely the customer's work process is affected. This influences the timeframe that is allowed to solve the problem.

Urgency	Description
1	Process stopped; customer(s) cannot work
2	Process affected; customer(s) cannot use certain functions
3	Process not affected; customer(s) request extra/optimised function

3. Apply Impact/Urgency matrix to determine the priority of the incident.

Urgency	Impact			
		3	2	1
	3	5	4	3
	2	4	3	2
	1	3	2	1

4. Apply priority using the Priority Code Table below and work to the times.

Priority	Resp. Time	Soln. Time	1 st Esc after	1 st Esc. to	2 nd Esc. after	2 nd Esc to
1	5 mins	60 mins	5 mins Or when expertise level reached	• Marcus • Paul • Dave	15 mins	Peter
2	10 mins	2 hours	15 mins Or when expertise level reached	• Bradley • Position 1 • 2nd level support	35 mins	Peter Ronald
3	15 mins	4 hours	1 hour Or when expertise level reached	• (Department Name) Coordinator • 2nd Level support	2 hours	Hans
4	45 mins	1 day	4 hours Or when expertise level reached	• (Department Name) Coordinator • 2nd Level support	5 hours	Tim
5	4 hours	5 days	2 days Or when expertise level reached	• (Department Name) Coordinator 2 nd Level support	4 days	Sergei

Information which may be included on a Request for Change form:

- RFC Number
- Details of person requesting change
- Date change proposed
- CI identity and description
- Version of item to be changed
- Change priority
- Reason for change
- Relationship with other changes
- Impact and resource assessment
- CAB recommendations
- Authorisation signature
- Authorisation date
- Details of change builder
- Scheduled implementation date
- Actual implementation date
- Review date
- Review results
 - *Did the change have the desired effect?*
 - *Are the users happy with the results?*
 - *Were there any unexpected or undesirable side effects?*
 - *Were the resources used the same as those planned?*
- Date and time of RFC closure

Main duties of a Change Manager (some of which may be delegated)

- Receive, log and allocate a priority to all RFCs. Reject any impractical RFCs
- Table all RFCs for a CAB meeting, issue an agenda and circulate all RFCs to CAB members in advance of meeting to allow prior consideration
- Decide which people will come to which meetings
- Convene urgent CAB or CAB/EC meetings for all urgent RFCs
- Chair all CAB and CAB/EC meetings
- After consideration of the advice given by the CAB or CAB/EC, authorise acceptable changes
- Issue FSCs via the Service Desk
- Liaise with all necessary parties to coordinate change building, testing and implementation in accordance with schedules
- Update the change log with all progress that occurs, including any actions to correct problems and/or to take opportunities to improve service quality
- Review all implemented changes to ensure that they have met their objectives. Refer back any that have been backed out or have failed
- Review all outstanding RFCs awaiting consideration or awaiting action
- Analyse change records to determine any trends or apparent problems that occur. Seek rectification with relevant parties
- Close RFCs
- Produce regular and accurate management reports

A standard CAB agenda should include a review of:

- Failed changes, backed-out changes, or changes applied with out reference to the CAB by incident management, problem management or change management
- RFCs to be assessed by CAB members
- RFCs that have been assessed by CAB members
- Change reviews
- The change management process including any amendments made to it during the period under discussion, as well as proposed changes
- Change management wins/ accomplishments for the period under discussion, i.e. a review of the business benefits accrued by way of the change management process.

Information required for a process specification

- Process name, description and administration – (version, Change control, etc.)
- Vision and mission statements
- Scope, objectives and terms of reference
- Process overview
 - Description and overview
 - Inputs
 - Sub processes
 - Activities
 - Outputs
 - Triggers
 - Tools and other deliverables
 - Communication
- Roles and responsibilities
 - Operational responsibilities
 - Process owner
 - Process members
 - Process users
 - Other roles
- Associated documentation
- Interfaces
 - To other service management processes
 - To other IT processes
 - To business processes
- Dependencies
 - On and to other service management processes
 - On and to other IT processes
 - On and to business processes
- Formal targets
 - Measurements
 - Metrics
 - Targets and timescales
- Reviews assessment and audit
- Reports produced by the process
 - Frequency
 - Content
 - Distribution
- Glossary, acronyms and references

The Process Maturity Framework (PMF)

The PMF can be used either as a framework to assess the maturity of each of the ten service management processes individually, or to measure the maturity of the overall service management process as a whole. This is an approach that has been widely used in the IT industry for a number of years, with many proprietary models being used by a number of organisations. This particular PMF has been developed to bring a common, best practice approach to the review and assessment of service management process maturity. This framework can be used by organisations to internally review their own service management processes as well as third party organisations brought in as external assessors/ auditors.

The maturity of the service management processes is heavily dependent upon the stage of growth of the IT organisation as a whole. It is difficult, if not impossible, to develop the maturity of the service management processes beyond the maturity and capability of the overall IT organisation. The maturity of the IT organisation is not just dependent upon the maturity of the service management processes. Each level requires a change of a combination of elements in order to be fully effective. Therefore a review of processes will require an assessment to be completed against the five areas of:

1. Vision and steering
2. Process
3. People
4. Technology
5. Culture

The major characteristics of each level of the PMF from a process perspective are as follows:

INITIAL (Level 1): The process has been recognised but there is little or no process management activity and it is allocated no importance, resources or focus within the organisation. This level can also be described as 'ad hoc' or occasionally even 'chaotic'. The characteristics of a process at this stage of maturity are:

- Loosely defined processes and procedures, used reactively when problems occur
- Totally reactive process
- Irregular, unplanned activities

REPEATABLE (Level 2): The process has been recognised and is allocated little importance, resource, or focus within the operation. Generally activities related to the process are uncoordinated, irregular, without direction and are directed towards process effectiveness. The characteristics of a process at this stage of maturity are:

- Defined processes and procedures
- Largely reactive process
- Irregular, unplanned activities

DEFINED (Level 3): The process has been recognised and is documented but there is no formal agreement, acceptance and recognition of its role within the IT operation as a whole. However the process has a process owner, formal objectives and targets with allocated resources and is focussed on the efficiency as well as the effectiveness of the process. Reports and results are stored for future reference. The characteristics of a process at this stage of maturity are:

- Clearly defined and well publicised processes and procedures
- Regular, planned activities
- Good documentation
- Occasionally proactive processes

MANAGED (Level 4): The process has now been fully recognised and accepted throughout IT. It is service focussed and has objectives and targets that are based on business objectives and goals. The process is fully defined, managed and has become proactive, with documented, established interfaces and dependencies with other IT processes. The characteristics of a process at this stage of maturity are:

- Well defined processes, procedures and standards, included in all IT staff job descriptions
- Clearly defined process interfaces and dependencies
- Integrated service management and systems development processes
- Mainly proactive process

OPTIMISING (Level 5): The process has now been fully recognised and has strategic objectives and goals aligned with overall strategic business and IT goals. These have now become 'institutionalised' as part of the everyday activity for everyone involved with the process. A self contained continuous process of improvement is established as part of the process, which is now developing a pre-emptive capability. The characteristics of a process at this stage of maturity are:

- Well defined processes and procedures are part of the corporate culture
- Proactive and pre-emptive process

Service Level Agreement

for

.....

between

.....

and

.....

Table of Contents

- 1. General Agreement 3**
- 2. Service Description 4**
- 3. Service Levels..... 5**
 - 3.1 Opening hours5
 - 3.2 System availability.....5
 - 3.3 User support.....5
 - 3.4 System performance6
 - 3.5 Changes.....6
 - 3.6 Contingency6
 - 3.7 Back up & Restore of Data7
 - 3.8 Security7
 - 3.9 Deliverables7
- 4. Restrictions 8**
 - 4.1 Growth thresholds8
 - 4.2 Exclusions.....8
- 5. Reporting 9**
 - 5.1 Standard reports9
 - 5.2 Reports on customer demand.....9
 - 5.3 Retention of reports9
- 6. Charging 10**
 - 6.1 Fees and tariffs.....10
 - 6.2 Payments10
- 7. Changes to the SLA..... 11**
 - 7.1 Procedure11
 - 7.2 Minor changes to the SLA11
 - 7.3 Thresholds11
 - 7.4 SLA reviews.....11

1. General Agreement

Purpose of the agreement

This agreement applies to the warranties and commitments related to the service:
....., referred to hereafter: the service, and the usage of the service.

Scope of the agreement

The scope of this agreement is all the conditions concerning the service, the service levels and the restrictions as described in the remainder of this document which is an integral part of this agreement.

Parties

Parties to this agreement are, referred to hereafter: the service provider, and, referred to hereafter: the customer.

General responsibilities of parties

The service provider is responsible for the proper operation of the environment of the service. The service includes: maintaining the general availability and performance of the system, the integrity of the data and the timely accessibility of the new data, supplying end user support and the implementation of changes.
The customer is responsible for the proper use of the service environment. This means that it sees to it that its users comply to the agreements and procedures in this SLA and other documents related to the service.

Start date

This agreement will be effective as from:

Duration

This agreement will remain in effect for a period of: ... year(s)

Automatic extension

This agreement shall be automatically extended by consecutive 12 months' periods except in case of termination by either party at least 3 months prior to the expiration of the initial period or to the expiration of each subsequent period.

Disputes

All disputes arising from this agreement shall preferably be settled in an amicable manner. If such renders no result, the case will be referred to a jointly selected arbiter, whose decision will be binding to both parties.

Signatories

Parties details	customer representative(s)	service provider representative(s)	CAB authorisation
Department			
Signature			
Name			
Function			
Date			

2. Service Description

Service Name	
Service Owner	
Primary User	
Other Users	
Primary Locations	
Functional Description	
Scope of the Service	
Related Services	
Technical Requirements	

3. Service Levels

3.1 Opening hours

Opening hours	
Attended hours	
Maintenance hours	
Unattended hours	

Scheduled maintenance	
frequency	
days	
times	
duration	

Unscheduled maintenance	
total-time	
when	
duration	

3.2 System availability

System availability	attended hours	unattended hours	measuring period
availability			
reliability			
recovery			

3.3 User support

User support	office hours	standby hours
Opening hours		
Name Help Desk		
Tel.		
Fax		
E-Mail		

3.3.1 User support main tasks and key performance metrics

Support task	reaction time	time to repair
<i>solving of network failure</i>		
<i>solving of workstation failure</i>		
<i>solving of printer failure</i>		
<i>solving of standard software questions</i>		
<i>solving of non-standard software questions</i>		
.....		

3.3.2 Information

3.4 System performance

System performance	attended hours	unattended hours	measuring period
user response times			
turnaround times			

3.5 Changes

3.5.1 General procedure

This section describes the procedure to follow to make a request for change.

e.g.:
Whenever a change to the service is needed this can be requested via general change management procedures.

3.5.2 Change management performance

Standard or cat.0 changes	RFC confirmation	RFC assessment	implementation
new user			
new workstation			
move workstation			
change user profile			
change software			
.....			
.....			

Non-standard changes	RFC confirmation	RFC assessment	implementation
Cat.1 changes			
Cat.2 changes			
Cat.3 changes			
Urgent changes			

3.5.3 Planned changes

3.6 Contingency

3.6.1 Contingency plans

document name	copy holder(s)	location(s)
.....		
.....		

3.6.2 Contingency Levels

levels at contingency site	service	basic functionality	full functionality

functionality level	basic functionality	full functionality

3.7 Back up & Restore of Data

3.7.1 Back up of data

Moment of Backup	Type of back up	retention time	number of copies
Monday			
Wednesday			
Friday			
Last Friday			
December, 31			
.....			

All backup activities are executed during Maintenance hours.

3.7.2 Restoring of data

3.8 Security

3.8.1 Access of data

3.8.2 Changing and resetting of password

3.9 Deliverables

3.10 Training

4. Restrictions

The purpose of this section is to make clear in which cases service levels can't be guaranteed anymore. If any of the threshold figures is exceeded this could be a trigger to review the SLA.

4.1 Growth thresholds

4.1.1 Throughput thresholds

4.1.2 End user thresholds

4.2 Exclusions

4.2.1 Circumvention

4.2.2 User mistakes

5. Reporting

In this section the content of SLA monitoring reports is described. Typical reporting aspects to be described here are function responsible, frequency, function to report to, retention of reports and reports on demand.

5.1 Standard reports

service level	agreed metric	actual metric	measuring period	function responsible	function to report to
System Availability					
availability					
reliability					
recovery					
User Support					
reaction times					
time to repair					
System Performance					
user response times					
turn around times					
Changes					
Growth/Usage					
usage statistics					

5.2 Reports on customer demand

5.3 Retention of reports

6. Charging

This section describes the charges for the agreed services and service levels. It also explains the charging method.

6.1 Fees and tariffs

The service fee is subject for review at each new SLA period.

For the service provided a tariff applies of : \$ per

For standard options a tariff applies of : \$ per

For every modification to the service, a separate price and/or modification of tariff will be agreed upon, prior to the development.

6.2 Payments

Settlement takes place via the general internal charging system.
Monthly invoices will be provided by the service provider.

7. Changes to the SLA

7.1 Procedure

At the end of the SLA period the SLA will be evaluated and can be renegotiated. This can result in changes to the SLA. A change to the SLA can result in changes to the IT infrastructure and vice versa. Therefore a change to the SLA or IT infrastructure must be authorised through standard change procedures (CAB authorisation). During the SLA period there will be a number of SLA reviews. The purpose of these reviews is to see if Service Levels are met and, if not, to take necessary measures to stay in line with the SLA. In case the outcome of a review shows that certain thresholds are passed, the SLA can also be changed and discussed as stated above.

7.2 Minor changes to the SLA

Minor changes to the SLA are changes made to the service or service levels that do not directly lead to SLA review and renegotiation. A minor change is recorded in the amendment list attached to this document (see Annex B.)

7.3 Thresholds

An ad hoc SLA review will be initiated whenever one of the following thresholds is passed:

- thresholds mentioned in the Restrictions section earlier in this SLA are exceeded.
- the number of minor changes recorded in the amendment list exceeds a total of

7.4 SLA reviews

The SLA is reviewed regularly on the basis of service level reporting and User Board Meetings. The outcome of these reviews may result in renegotiation and/or changing of the SLA, and, once a year, in prolongation or even termination of the SLA.

7.4.1 Planned SLA reviews

2 reviews a year: one after 6 months, one after 12 months.
Unplanned or ad hoc SLA reviews can be held when thresholds are passed.

7.4.2 Reports

Every review will be based on Service Level reports of the past 12 months.

7.4.3 User Board Meetings

A User Board Meeting will be held a month before every planned SLA review.
User Board members are :

Customer representative(s)	Service provider representative(s)
Business Unit representative(s)	Account Manager service provider
End user manager(s) ¹⁾	User Support representative(s) ²⁾
End users ¹⁾	System Management representative(s) ²⁾

1) to be appointed by the Business Unit representative
2) to be appointed by the Service Level Manager

ANNEX A. DEFINITION OF TERMS

agreed metric	the SLA-metric used, together with its target outcome, to define a service level
attended hours	the usage period(s) in which full system availability and performance is delivered at the service levels specified
availability	the totality of interruption-free parts of the opening hours in which the customer can make use of the system, expressed in a percentage
basic functionality	basic, contingency level functionality. In other words: the minimum level of functionality needed to start up primary processes.
CAB	Change Advisory Board, i.e. a representative group of people who are responsible for assessing, from both a business and a technical viewpoint, all RFCs. They advise on the priorities of RFCs and propose allocations of resources to implement those changes
Change Management	the process of controlling and managing requests to effect changes to the IT Infrastructure or any aspect of IT services, and of controlling and managing the implementation of those changes that are subsequently given approval
contingency	an unplanned event of which the effect on IT service provision exceeds formerly specified thresholds
deliverables	tangible output of an information system (IS).
diversion	a measure to cope with a contingency by which some or all parts of IT service provision are diverted to other locations and or facilities
fix time	Recovery time, time needed to fix an interruption
full functionality	full, contingency level functionality. In other words: the highest level of functionality provided in contingency situations
Help Desk	an organisational unit which is responsible to perform end user support tasks regarding IT services
host response time	average time between arrival of a command at the entry point of the host and reply by the host at its exit point to these commands
interruption	a continuous period during opening hours in which the service or a service component is not available
maintenance hours	The period(s) in which system maintenance is or can be performed. During this period the service is totally unavailable to the users. Service levels are not guaranteed
measuring period	a specification of the period at which a service level is measured and reported
network response time	average time between arrival of a command at the entry point of the network and arrival of this command at the entry point of its

	destination
office hours	the period(s) which are the regular working hours of the business employees. Normally these hours are also used as opening hours for the user support group(s)
opening hours	= Service hours, i.e. a reference period during which the service is provided
performance	the level of achievement of a service or system. System performance for instance, can be expressed in response time, throughput time or turnaround time.
reliability	the number or frequency of interruptions allowed during a discrete period
reaction time	the time between notification of the Help Desk and action by the Help Desk
retention time	period of time an certain object is safeguarded
RFC	Request for Change, i.e. a form or screen used to record details of a request for a change to any component of an IT infrastructure or any aspect of IT services
RFC assessment	the process of assessing all (possible) effects of a requested change, time and money needed etc. resulting in authorisation or negation of a RFC
RFC confirmation	a confirmation of reception of the RFC to the sender of the RFC
service	an IT service, i.e.: a compound of IT facilities, applications and/or supporting processes delivered by an IT service organisation
service level	the level of quality at which an IT service aspect is delivered
Service Level Management	the process that manages IT service provision in a business-wise manner by means of SLAs
service-level-period	see: measuring period
SLA	Service Level Agreement
SLA metric	metric or formula at which an agreed service level is measured
SLA period	the period during which the SLA is valid or running
SLA review	evaluation of the actual service levels provided against the service level targets as described in the SLA, but in particular the perceived service quality as expected from these targets
standby hours	the period outside the office hours at which no regular user support is available. Support can only be obtained in exceptional situations by means of standby arrangements
system	either an information system or computer system. A computer system can be part of an information system. A system can be part of a service

throughput time	the time elapsed between the moment of arrival at a processing unit of a block of data and the moment the processed block of data leaves that unit again. Throughput time will be verified by means of a periodic, representative sample
turnaround time	the average time between a request of information and the delivery of output
unattended hours	The usage period(s) outside the attended hours, during which the service is available. Service levels are not guaranteed or guaranteed at a specified lower level
user board meeting	a meeting between customer and service provider representatives held to exchange experiences with the IT service(s) delivered on which basis the SLA is reviewed.
user response time	the average time between entry of commands into the system and reply by the system to these commands on user screen
user support group	see: Help Desk

CONFIGURATION MANAGEMENT

The Scenario

"The Money Makers" Investment Managers have experienced an unprecedented amount of growth over the past 5 years. Five years ago, they were a 50 person company with a few influential (and wealthy) clients. Since these humble beginnings, they have grown to be a company of 1000 people. You have been hired as an external consultant with the mandate "build a Configuration Management Database". They have no current CMDB and do not know where to start. As yet, you have not met with the CIO and do not have a great deal of understanding about the reasons behind this decision. You are planning your first meeting with the CIO.

The Exercise

In your groups, list the questions you would ask of the CIO to ensure that you build an appropriate CMDB. (bullet points will suffice).

- Drivers for this / motivation / goals
what do they hope to accomplish?
 - Budget ?
 - Future growth
 - Level of detail / hierarchy
 - How often do changes occur / existence of change control
 - ownership
 - management commitment
 - Timeframe
 - what data is available
 - what resources are available
 - legal / regulatory
 - Perceptions
 - Business criticality of various C.I. items
 - Locations
 - Implementation approach
 - Security issues
-

PROBLEM MANAGEMENT

The Scenario

Your entire IT Organisation has been trained on ITIL and uses the terminology which ITIL recommends – particularly the terms “Incident”, “Problem”, and “Known Error”. A new employee at the Service Desk is unfamiliar with ITIL and has difficulty in making a distinction between an incident, a problem and a known error.

The Exercise

In pairs, think of an example of an incident, a problem and a known error as illustrations for the new employee. Do this for:

- (i) an example from your own IT organisation;
 - (ii) an example unrelated to IT
-

CHANGE MANAGEMENT

The Scenario

One of the key skills which is required by a Change Manager is the ability to develop relationships within the organisation to ensure that all the information which is required is gathered in the most efficient way possible. The same is true of the Change Management process – the success of the process depends strongly on other processes.

The Exercise

Explain the relationship and the information exchange which would take place between Change Management and the following three processes:

- Incident Management

- Configuration Management

- Problem Management

SERVICE LEVEL AGREEMENTS

The Scenario

Now that you are working full time for “The Money Makers”, you have been asked to provide a Service Level Agreement between the IT Organisation and the business which covers the entire email service. All the information you have on current usage is that it costs \$1,000,000 to provide the service per annum. This includes everything which is needed to keep the email service up and running. There are 1,000 users working in the organisation and you are able to track exactly how many emails have been sent by any individual user.

The Exercise

...is to create a Service Level Agreement to cover this service. You only need to provide bullet points covering what would go under each heading. For the headings, use the contents on the slide titled “Sample SLA contents”.

In your service level agreement, you will also need to show the users how they will be charged for the service.

In a real situation, you would have a client to provide you with expectations (eg the required opening hours of the Service Desk). In the absence of this client, feel free to be creative with any information not contained in this exercise. Ie make it up.

FINANCIAL MANAGEMENT

Case Study One: Internal money versus external money

A company has an underground parking lot. This parking lot is for the use of all employees but is over-subscribed. The company decides to introduce Cost Accounting and calculates that the \$200,000 yearly cost of the car parking facility will have to be recovered by an internal charge to each department of \$50/month for each car park pass issued.

The company parking lot is:

- * underground, at the office
- * provided as a benefit to staff
- * fitted with electronic remote control to open/close the main door
- * under surveillance by cameras and security guards.

A hotel nearby provides parking facilities:

- * outside, 200m away
- * with a hotel-operated barrier
- * with no security or guarantee of safety.

Because the hotel has the space free during working hours, it need only recover costs of administration plus any profit it wishes to make. It decides to charge \$30/month for business car parking. The result of this is that the internal parking lot is only used at 20% of its Capacity while the hotel parking lot is full.

Using the external hotel parking facility costs less to the department manager but more overall to the organisation, as it has to pay the costs of the building and would usually prefer to minimise external spend. They cannot reduce their overall costs, as the company parking is an integral part of the offices and grounds.

Case Study Two: Exceeding business need

One company is charging \$860 a year for the provision of an Infrastructure to which Users' workstations are connected. This Infrastructure is available 24 hours a day, monitored 16 hours a day and includes a number of facilities such as office automation tools, shared printers, e-mail, external gateways (faxes, Internet, access to large servers).

Some small departments (from 5 to 20 Users) were used to very simple peer-to-peer Infrastructure that suited their needs. Moving to the new, more expensive common Infrastructure did not appear to provide any benefits and even seemed to add to overheads.

Several of these departments conducted a study and found that it would be less expensive for them to continue with their dedicated Infrastructure and just have one shared workstation connected to the common Infrastructure for e-mail purposes.

Case Study Three: Discouraging use of services

A company provided its Users with a dedicated, outsourced Service Desk facility. The vendor charged the company on a per-call basis, the price varying in bands, depending upon the total number of calls during the month. The charging policy was to recharge all IT spending to the business on the basis of true cost.

Once the Service Desk was in place, Customers realised that they could reduce their costs by not placing Service Desk calls. Some business managers instructed their Users not to use the Service Desk, or to route all issues through a single, local support person.

Decreasing the total number of calls decreased the calculated charges to the Customer but did not reduce overall price of the service by the same amount. It also resulted in:

- * increased wasted time for Users
- * reduced effectiveness of IT systems
- * poor perception of the IT Services and the IT organisation
- * additional work for the IT organisation to discover problems
- * reduced leverage in negotiating service costs with the outsourcing vendor.

Case Study Four: Hidden costs

In the same Service Desk context as the previous example, business managers may be tempted to set up their own Service Desk facility by appointing staff dedicated to this. It may cost less to the business department than a centralised desk and allows the business to direct the efforts of the staff toward the Incidents and Problems that concern them. However, the total cost to the organisation of allowing one or more businesses to do this is:

- * the quality and level of service will obviously not be the same
- * knowledge will not be shared with other departments
- * studies will be undertaken on a department basis where they should have been on the company or group basis
- * costs for this dedicated facility will not be monitored or at least not monitored centrally.

This results in an under-used central facility and an increase in hidden costs of IT as the business Service Desks are not accounted for in the IT budget and probably not fully costed by the businesses.

AVAILABILITY MANAGEMENT

The Scenario

You are working for Snowbound Ski Resort Systems, who manage an entire skifield. They want to upgrade all of their facilities, including their computer systems, mechanics, communications links, and facilities.

Before beginning negotiations with external IT and engineering companies who will be undertaking the various activities, they want to understand the ebbs and flows of their business, and also establish which parts of their business are critical, and which parts are not so critical.

The following business lines on the ski fields require upgrades:

- a. The food outlets located all over the ski fields
- b. The Slippery Feet Ski hire shop
- c. The Mountain Man bar
- d. The Point of Sale terminals in the Winter Wonderland Clothing Store
- e. The credit card systems in the lift ticket sales centre
- f. The IT systems which control and monitor "Riding High" – the two person chairlift.
- g. The Salary systems to pay all of the casual and permanent staff

The Exercise

Place these seven business lines in order of criticality to the business (from 1 to 7). Most Critical to least critical.

Next to each of the business lines, identify when you think the periods of high demand are, and when you think the periods of low demand are. This may vary depending on the time of day, the time of week, the time of month, or the time of year.

- g. All year
- a. winter
- f. winter day
- e. ✓
- c. - night/day
- b. - day
- d. - day

PROCESS RELATIONSHIPS

The Exercise

As you have probably become aware over the past two days, none of the processes exist in isolation, they all depend on each other in varying degrees. Some are more closely related, and others not so.

Using the table below, identify the *two* processes you think most closely relate to the process on the left. Be prepared to explain why you have answered in the way that you have.

This Process...	...is most closely related to
Configuration Mgmt	
Incident Mgmt	
Problem Mgmt	
Change Mgmt	
Release Mgmt	
SLM	
Financial Mgmt	
Availability Mgmt	
Capacity Mgmt	
ITSCM	
Security Mgmt	

IMPLEMENTATION

“Buy in”

The purpose of this exercise is two fold:

- 1 – to understand the links between the goals of an organization and the process implementation
- 2 – to identify the benefits of the relevant processes and establish ways of measuring them.

The Exercise

Focus on one of the organizations in your group. For this organization, do three things:

- 1 – list the top three priorities of the company as a whole
 - 2 – on a scale of 1 to 5, perform a (very basic) assessment of ITIL process maturity for the processes of Incident Management, Problem Management, Change Management and Configuration Management.
 - 3 – Based on the organisation's priorities and the current process maturity, show the benefits of implementing ITIL, and how the organization as a whole will benefit.
-

IMPLEMENTATION

The How of ITIL Service Management

What's hard and what's easy

You have decided to modify the way you currently your IT Services as a result of understanding the ITIL Process methodology. In order to show that you understand what you are getting yourself in for, your manager has asked you to provide some more information on the processes.

For the processes assigned to your group, list:

1 two benefits which you will achieve from implementing your ITIL processes

2 two problem areas which you think will need particular attention to ensure that your processes work