The ITIL Foundation Exam Study Guide
3rd Edition

Questions? Comments? Feedback? Email scott@ITIL-Study-Guide.com

What is ITIL?

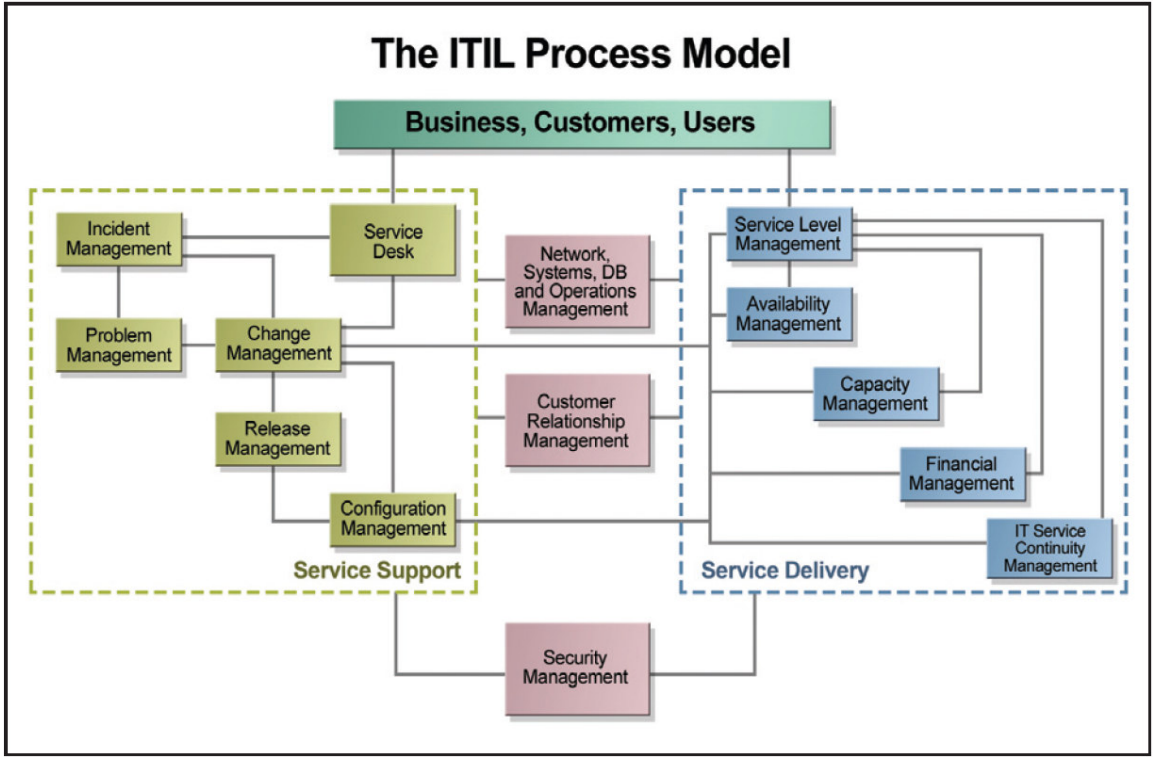
ITIL is a set of best practices for IT service management that has been evolving since 1989. It began as a set of processes for use by the UK government to improve IT service management and is gaining worldwide acceptance throughout the IT industry as the basis for successful IT service management.

At the core of the library are two volumes on the service management discipline: Service Support and Service Delivery, which were rewritten in 2000 – 2001. Security is covered in the Security Management volume written in 1999. These publications are offered by by the UK's Office of Government Commerce – website www.ogc.gov.uk/

ITIL **Service Support** includes five disciplines that provide flexibility and stability for delivering IT services to the business. These disciplines are:
• Incident management
• Problem management
• Change management
• Release management
• Configuration management

ITIL **Service Delivery** includes five disciplines that support high-quality, cost-effective IT services for the business. These disciplines are:
• Service level management
• Availability management
• Capacity management
• Financial management for IT services
• IT service continuity management

The service support and service delivery disciplines together help develop the service management capability of an organization. There are complex interrelationships among all 10 of the service management disciplines as they interact to support the overall objective of making sure the IT infrastructure delivers high levels of service to the business.



This diagram illustrates the major interactions across the disciplines and includes the service desk function.

For example, change management is related to all of the service delivery disciplines. It might require input from financial management to understand the cost of the change being considered or input from capacity management to understand the implications of the change on the infrastructure. Similarly, configuration management provides information to all of the service delivery disciplines about the structure of the enterprise.

All of the disciplines work together to deliver service management to the business and the users of the IT systems. Users can be employees of the organization or its partners or customers. Partners and customers are increasingly using the IT services directly, which is increasing the importance of effective service management.

This diagram also shows other key relationships. Both service support and service delivery interact with the networks, systems, applications and databases of the IT infrastructure as well as the operational management of those entities. The customer relationship management discipline manages the interaction among the service delivery and service support process and the users and customers of the organization to whom business services are being delivered.

The focus of ITIL in all its disciplines is on defining best practices for the processes and responsibilities that must be established to effectively manage the business' IT services, which in turn drive forward the business' objectives in service delivery and revenue generation.

All of these processes could, in theory, be implemented and supported without the use of IT tools. In practice, however, this is difficult, and electronic systems are essential to support these processes where appropriate.

Other Terms You'll Hear in Relation to ITIL:
Note: these won't be on the ITIL Foundation Exam; I've included them for your general background knowledge.

BS15000
BS15000 specifies a set of interrelated management processes based heavily on the ITIL framework and is intended to form the basis of an audit of the managed service. Customer relationship management is addressed in this standard and is aimed at businesses that require quality service. The BS15000 standard was launched at the IT Service Management Forum (itSMF) conference in Birmingham, England, on November 6, 2000. It complements the established British Standards Institute (BSI) Code of Practice for IT Service Management, PD0005 and the PD0015 self-assessment workbook. Used together, BS15000 and PD0005 provide a framework for comprehensive best practices.

ISO 17799
Security is the most important issue that companies must address in order to realize the benefits of electronic business. They must make sure that the organization's valuable resources and intellectual property are protected and that customers feel secure in doing business with the organization. ISO 17799 supports the implementation of security in several ways:
• It defines a set of key objectives and identifies a set of security controls, which are measures that can be adopted to meet the objectives of the standard.
• It specifies the security controls that can be used (based on the results of a risk management assessment) as the basis for formal certification of an IT enterprise under the BS7799 standard.

What is the relation between BS15000 and ISO20000?
ISO20000 will be the International Standard for IT Service Management. This will be taken from the British Standard BS15000, with minor alterations to correct errors and inconsistencies. It is expected that ISO20000 will be published late in 2005 or possibly early 2006. Once the international standard is published, the British Standard will be withdrawn. It is expected that companies that have BS 15000 accreditation will be able to state they have ISO 20000

ITIL has defined the best practice processes for securing the managed IT infrastructure, which is itself closely tied to the use of ISO 17799 best practices.

Based on the security section of the service level agreement (SLA), the first step is the planning phase, which relies on a business risk assessment to identify threats and vulnerabilities. This process is strongly based on ISO 17799 and results in the selection of appropriate security measures, known as controls.

During the implementation phase, the controls are implemented using the appropriate tools and processes. The remainder of the process involves continually evaluating and reviewing the security policy and its relevance to changing business conditions;

maintaining the policy at the appropriate level for consistent security for the business; and providing reports to help ensure that SLAs are being met.

Study Guide Summary:

Areas covered by ITIL
Service Support Functions:
• Service Desk
• Incident Management
• Problem Management
• Change Management
• Configuration Management
• Release Management

Service Delivery Functions:
• Availability Management
• IT Services Continuity Management
• Capacity Management
• Financial Management
• Service Level Management

Deming Circle – Plan, Do, Check, Act

KPI – Key Performance Indicators – parameters used to measure the progress relative to the objectives or Critical Success Factors (CSF)

Capability Maturity Model (CMM) - CMM is usually the wrong answer. Concerned with improving the maturity of the software creation process.

Benefits of ITIL to customer/user

- provision of IT services becomes more customer focused and agreements about service quality improve the relationship
- Services are described better, in customer language, and in more appropriate detail
- quality, availability, reliability and cost of services are managed better
- communication improved by agreeing on points of contact

Benefits of ITIL to organization

- IT organization develops a clearer structure, becomes more efficient, and more focused on corp objectives
- IT org is more in control of the infrastructure and services it has responsibility for, and changes become easier to manage
- Effective process structure provides a framework for effective outsourcing of elements of IT services
- encourages a cultural change towards providing service and supports introduction of quality mgmt systems based on ISO 9000 series or BSI5000
- provides coherent frame of reference for internal communication and communication with suppliers, and for standardization and identification of procedures

Potential problems/mistakes w/using ITIL

- introduction can take a long time, require significant effort, and may require a cultural change. Attempting to make the change to fast can lead to frustration because objectives are never met
- Unnecessary and over-complicated procedures can impact service quality, they are seen as obstacles
- No improvement is seen in IT services due to a lack of understanding of what the process should provide, kpi's, and how processes can be controlled
- Improvements in service and cost reduction are not visible because no baseline data was available for comparison and/or the wrong targets were identified.
- Successful implementation requires acceptance and participation by all departments. If a single department makes all the decisions, these decisions may not be acceptable to other departments.
- Insufficient investment in training and support tools leads to minimalization of the processes and therefore little improvement in the process. A short term increase in staff may be required if the current staffing level is already maxed.

Service Delivery – SLM, Financial Mgmt, Capacity Mgmt, IT Service Continuity Mgmt (ITSCM), Availability mgmt

Service Support – Service Desk, Incident Mgmt, Problem Mgmt, Configuration Mgmt, Change Mgmt, Release Mgmt

Incident Management

- Incident is any deviation from the norm which is why a Service Request is considered an incident (that has occurred or might occur).
- Service Request – request from a user for support, delivery, information, advice, or documentation, not being a failure in the IT infrastructure. Handled under IM if a "standard service".
- **Goal** is to get the user up and running as quickly as possible
- Priority = Impact & Urgency
- Functional vs. Hierarchical escalation –
    - Hierarchical is usually limit driven
    - Functional (horizontal) – involving personnel with more specialist skills, time, or access privileges to solve the incident.
    - Hierarchical (vertical) – involving higher level of org authority when it appears that the current level of authority is insufficient to ensure that the incident will be resolved in time and/or satisfactorily
- Benefits
    - More timely resolution of incidents resulting in reduced business impact
    - improved user productivity
    - independent, customer focused incident monitoring
    - availability of SLA focused business management information
    - improved monitoring, allowing performance of SLA's to be more accurately measured
    - useful management and SLA reporting concerned with service quality
    - better and more efficient use of personnel
    - no lost or incorrectly registered incidents and service requests
    - more accurate CMDB since it is being audited while incidents are registered in relation to CI's
    - Improved user and customer satisfaction
- Relationships
    - configuration mgmt, problem mgmt, change mgmt, SLM, availability mgmt, capacity mgmt
    - Config mgmt defines the relationship between resources, services, users, and service levels. Configuration details are linked to the incident to provide better information about the error.
    - Problem mgmt – has requirements for the quality of the information in the incident to facilitate identification of the underlying error. Problem management provides information to IM about problems, known errors, work arounds, and temporary fixes
    - Change mgmt – incidents can be resolved by implementing changes. Change mgmt provides information to IM about scheduled changes. Changes can cause incidents.
    - SLM – IM must be familiar with the SLMs so that this information can be used to communicate with customers. Incidents can be reported on to determine if SLM's are being met.

    - Availability mgmt – reporting on incident records can be used to determine availability. Requires time-stamping of incidents.
    - Capacity management – concerned with incidents caused by a shortage of capacity
- Activities
    - Incident acceptance and recording – the incident is detected or reported and an incident record is created
    - Classification and initial support – incident coded by type, status, impact, urgency, priority, SLA, etc. User may be given suggestions to solve or work around the issue
    - If service request, relevant procedure is initiated
    - Matching – check is made to determine if the incident is known, possibly related to an existing incident, problem or known error, and if there is a solution or workaround
    - Investigation and diagnosis – if there is no known solution then the incident is investigated
    - Resolution and recovery – once the solution has been found, the issue can be resolved
    - Closure – the user is asked if they are satisfied with the solution and then the incident is closed
    - Progress monitoring and tracking – entire cycle is monitored, if it appears that it cannot be resolved in time or with the current level of expertise, then escalated
- Critical success factors
    - up-to-date CMDB
    - knowledge base
    - adequate automated system for recording, tracking, and monitoring incidents
    - close ties with SLM
- KPI's
    - total number of incidents
    - average resolution time
    - percentage of incidents resolved within SLA targets
    - percentage of incidents resolved by first-line support without routing
    - average support cost per incident
    - resolved incidents per service desk workstation or per Service Desk staff member
    - incidents resolved without visiting the user
    - number of incidents or percentage with initial correct classification
    - number of incidents or percentage routed correctly
- Roles
    - Incident Manager
        - monitoring the effectiveness and efficiency of the process
        - controlling the work of the support groups
        - making recommendations for improvements
        - developing and maintaining the incident management system

    - Support group personnel
        - First-line - recording, classifying, matching, routing, resolving, and closing incidents
        - Other support groups – investigation, diagnosis, and recovery
- Bottlenecks
    - users and IT staff bypassing IM procedures
    - incident overload and backlog
    - escalations
    - lack of clear definitions and agreements
    - lack of commitment

Service Desk

Objectives:
• To be the primary point of call for all:
o Calls
o Questions
o Requests
o Complaints
o Remarks
• To restore the service as quickly as possible
• To manage the incident life-cycle (coordinating resolution)
• To support business activities
• To generate reports, to communicate and to promote
Different Desks
• Call Center: Handling large call volumes of telephone-based transactions.
• Help Desk: To manage, coordinate, and resolve Incidents as quickly as possible.
• Service Desk: Allowing business processes to be integrated into the Service Management infrastructure. It not only handles Incidents, Problems and questions, but also provides an interface for other activities.
Service Desk Essentials:
• Single point of contact / Restore service ASAP
• Tasks: Customer Interface, Business Support, Incident Control & Management Information
• Concentrates on incident lifecycle management
• Incident: Unexpected disruption to agreed service
• Priority determined by business impact and urgency
• Correct assessment of priorities enables the deployment of manpower and other resources to be in the best interests of the customer
• Escalation and referral

Key Concepts to Study:

- This is a FUNCTION not a process
- Single point of contact that logs calls – period – even if they do more than that
- May be involved in IM, Release mgmt, change mgmt, config mgmt, and SLM
- Structural options
    - Centralized – single point of contact for all users, possibly with a separate Service Desk close to the users for business applications (split function Service Desk)
    - Local (distributed) Service Desks - across a number of sites, normally will be more difficult to manage
    - Virtual – the location is immaterial due to the user of communication technology
- Activities
    - responding to calls
    - providing information
    - supplier liaison

    - operational management tasks
    - infrastructure monitoring
- KPI's
    - is the telephone answered quickly
    - are calls routed to second level within x minutes
    - is the service restored within an acceptable time and in accordance with the SLA
    - are users advised in time about current and future changes and errors
- Critical success factors
    - easy to reach the Service Desk
    - users should not try to contact specialists directly
    - there should be good SLA's and OLA's and a service catalog in place to ensure that the support provide has a clear focus

Problem Management

Objectives:
• Stabilizing IT services through:
o Minimizing the consequences of incidents
o Removal of the root causes of incidents
o Prevention of incidents and problems
o Prevent recurrence of Incidents related to errors
• Improving productive use of resources
Tasks:
• Problem Control
• Error Control (including raising RfCs – Request for Change)
• Proactive Prevention
• Identifying Trends
• Management Information
• Posit Implementation Review (PIR)
Goal is to go from reactive to proactive. Stop problems from occurring / recurring.
Inputs:
• Incident details
• Configuration details
• Defined work-arounds
Outputs:
• Known Errors
• Requests for Change
• Updated Problem Records including work-arounds and/or solutions
• Response to Incident Management from Matching Management Information
Problem Control
• Identification
• Classification
• Assign Resources
• Investigation and Diagnosis
• Establish Known Error
Error Control
• Error Identification and Recording
• Error Assessment
• Recording Error / Resolution (Send out RfC)
• Error Closure
Known Error: An Incident or Problem for which the root cause is known and for which a temporary Work-around or a permanent alternative has been identified.
Proactive Problem Management:
• Trend Analysis
• Targeting Support Action
• Providing Information to the Organization
Known Errors resulting from Development should be made known to the Helpdesk.
Reporting is also key for Problem Management.

Key Concepts to Study:

- Problem = an undesirable situation, indicating the unknown root cause of one or more existing or potential incidents
- Known error = a problem for which the root cause is known and for which a temporary workaround has been identified
- Bottlenecks
    - Poor link between IM process and PM process
    - Ineffective communication of Known Errors from dev environment to prod environment
    - Lack of management commitment
- KPI's
    - Number of Incidents opened
    - Time needed to resolve problems
    - Costs incurred during resolution of problem
- Critical Success Factors
    - Well defined process framework and set of process objectives, interfaces, and resources
    - Set of comprehensive and well-documented procedures
    - Effective automated registration and classification of Incident records
    - Setting feasible objectives and making the best use of expertise
    - Effective coordination between IM and PM processes
- Benefits
    - Improved IT Service quality
    - Increased user productivity
    - Increased support personnel productivity
    - Improved IT service reputation
    - Enhanced management and operational knowledge and learning
    - Improved incident recording
    - Higher first-line resolution rate
- Inputs
    - Incident details from IM
    - Work arounds defined by IM
    - Configuration details from CMDB
    - Service catalog and service level agreements
    - details about the infrastructure and the way it behaves (capacity, performance measures, etc)
- Outputs
    - Known Errors
    - RFC's
    - Up to date problem records
    - Closed problem records for resolved problems
    - management info to help monitor effectiveness of PM process
- Activities

    - Problem Control
        - Identifying and recording problems & past trends
        - Classifying problems according to category, impact, urgency, priority
        - Investigating and diagnosing problems (reproduced in test environment)
        - temporary fixes
    - Error control
        - Error ID and recording – once id'd labeled as known error
        - Error assessment – compares possible solutions
        - Error resolution recording and raising RFC's
        - Error closure – follows post impl review
        - Problem/error resolution monitoring – occurs during all stages
- Roles
    - Problem Manager responsibilities –
        - develop and maintain problem control and error control activities
        - assess effectiveness of Prob Control & Error Control activities
        - provide problem related info to management
        - Manage problem support staff
        - allocate resources for support activities
        - Evaluate effectiveness of proactive PM process
    - Support Group Responsibilities - Reactive
        - ID and record problem by analyzing Incident details
        - Investigate problem based on priority
        - submit RFC's
        - Monitoring resolution of Known Errors
        - Advise IM team about work arounds and quick fixes
    - Support Group Responsibilities – Proactive
        - ID trends and potential sources of problems
        - submit RFC's to prevent reoccurrence
        - prevent replication across systems
- PM interacts with CI mgmt, CM, IM, SLM, Availability Mgmt, Capacity Mgmt
    - IM – provides workarounds and temporary fixes
    - CM – provides information about the progress and completion of corrective changes. Evaluated in consultation with PM resulting in Post Impl Review of changes. If change is successful, all associated incidents and problems can be closed.
    - Availability Mgmt – provides information about agreed availability levels. PM identifies the causes of unavailability and remedies them. Availability Mgmt aims to optimize infrastructure design reducing the number of incidents and problems.
    - Capacity mgmt – provides information to PM used to define problems. PM supports capacity mgmt by identifying the causes of capacity related problems and resolving them.
    - SLM – provides information to PM used to define the problem. PM procedures should support the agreed service quality levels.

Configuration Management

Objectives:
• Providing information on the IT infrastructure
o To all other processes
o IT Management
• Enabling control of the infrastructure by monitoring and maintaining information on:
o All the resources needed to deliver services
o Configuration Item (CI) status and history
o Configuration Item relationships
Tasks:
• Identification and naming
• Management information
• Verification
• Control
• Status Accounting
Asset: Component of a business process like people, accommodation, computer systems, paper records, fax machines, etc.
Configuration Management Database: A database, which contains all relevant details of each Configuration Item (CI) and details of the important relationships between CIs.
A Configuration Item (CI):
• Is needed to deliver a service
• Is uniquely identifiable
• Is subject to change
• Can be managed
A Configuration Item (CI) has:
• a Category
• Relationships
• Attributes
• a Status
Variant: A Configuration Item (CI) that has the same basic functionality as another Configuration Item (CI) but is different in some small way (ex: has more memory)
Baseline: A snapshot of the state of a Configuration Item and any component or related Configuration Items, frozen in time for a particular purpose (such as the ability to return a service to a trusted state if a change goes wrong)
Configuration Management supports all other processes!
Scope vs. Detail
Relationships – Common Types:
• Is a component of
• Is a copy of
• Relates to
• Relates with
• Is used by

Key Concepts to Study:

- Heartbeat of Infrastructure Management

- Configuration items (CIs) – IT components and services provided
- CMDB – configuration management database – keeps track of all IT components, their versions and status, relationships between them
- Asset management – accounting process for monitoring assets whose purchase price exceeds a defined limit, which keeps records of the purchase price, depreciation, business unit, and location.
- Configuration Management – keeps technical information on CI's and details of the relationships between CI's and the standardization and authorization of CI's. Monitors feedback about current information such as the status of IT components, their location, and the changes that have been made to them
- Benefits –
    - managing IT components
    - high quality IT services
    - effective problem solving
    - more rapid processing of changes
    - better control of software and hardware
    - improved security
    - compliance with legal requirements such as licensing
    - more precise expenditure planning
    - better support for Availability mgmt and capacity mgmt
    - solid foundation for IT Service Continuity Management
- Activities
    - Planning – determine strategy, policy, and objectives of the process, analysis of available information, identifying tools and resources, creating interfaces with other processes, projects, suppliers, etc.
    - Identification – sets up processes to keep database up-to-date
    - Control – authorized CI's only are entered
    - Status accounting – stores current and historical details about the status of CI's during their life cycle.
    - Verification – verifies CMDB by audits of IT infrastructure to check accuracy of the records
    - Reporting – provides information to other processes and reports about trends and developments in the use of CI's
- Baseline – snapshot of a group of CI's (entire infrastructure) at a point in time
- Relationships
    - IM, PM, CM, Release Mgmt, SLM, Financial Mgmt, Availability Mgmt, Continuity mgmt, capacity mgmt
    - IM – IM needs access to CI information across the whole infrastructure
    - PM needs information about the complexity of the infrastructure. Verification of the actual configuration of the infrastructure against the authorized configuration in the CMDB can identify deviations or defects in the infrastructure
    - CM uses the CMDB to id the impact of changes. Change mgmt provides the major input for updating the CMDB. It is essential to the successful implementation of Config mgmt

    - Release mgmt – provides information about release plans with versions and status of CI's and provides information about implemented changes. It needs information about CI's such as location and status.
    - SLM needs information about the services along with the relationships between services and the underlying infrastructure CI's. The Service Level can be stored in the CMDB recorded against the service CI or the component hardware or software CI.
    - FM – needs information about the use of services and CI's. This process also monitors IT components and investments (Asset Management).
    - Availability mgmt – uses the CMDB to identify the CI's, which contribute to a service and for Component Failure Impact Analysis (CFIA). Configuration mgmt provides information about the composition of the infrastructure, as well as about each of the elements.
    - Continuity Mgmt uses the baseline to specify recovery requirements and checks that these configurations are available at the disaster recovery site.
    - Capacity mgmt uses data from the CMDB to plan the optimization of the IT infrastructure, to allocate the workload and to develop a capacity plan.
- Critical Success Factors
    - CMDB is up-to-date
    - change mgmt and release mgmt must be strictly enforced
    - must be a stakeholder for the information to be record in the CMDB
- KPI's
    - number of observed differences between the records and the situation found during audits
    - number of occasions on which a configuration was found to be unauthorized
    - number of occasions on which a recorded configuration could not be located
    - attribute level differences uncovered by audits
    - time needed to process a request for recording information
    - list of CI's where more than a given number of incidents or changes were recorded
- Roles
    - Configuration Manager
        - proposing changes to the scope and level of detail of configuration management
        - ensuring that the configuration management process is communicated throughout the org
        - providing personnel and training for the process
        - developing the identification system and naming conventions
        - developing interfaces to other processes
        - evaluating existing systems and implementing new systems
        - planning and implementing population of the CMDB
        - creating reports on the effectiveness, conformance and value
        - organizing configuration audits
- Bottlenecks

- wrong CMDB scope or CI level of detail
- inadequate manual systems
- affect of urgent changes
- overambitious schedules
- management acceptance
- bypassing the process

Change Management (CM)

Objective: To *implement approved* changes *efficiently, cost-effectively* and with *minimal risk* to the existing and to the new IT infrastructure. Only approved changes made, risk and cost minimized.

Change Management Tasks:

- Filtering Changes
- Managing Change Process
- Managing Changes
- Chairing CAB and CAB/EC
- Review and Closure
- Management Information

Inputs:

- Requests for Change (RfC)
- CMDB
- Forward Schedule of Changes (FSC)

Outputs:

- Forward Schedule of Changes (FSC)
- Requests for Change (RFC)
- CAB minutes and actions
- Change management reports

Impact of change:

- Category 1
  - Little impact on current services. The Change Manager is entitled to authorize this RfC.
- Category 2
  - Clear impact on services. The RfC must be discussed in the Change Advisory Board. The Change Manager requests advice on authorization and planning.
- Category 3
  - Significant impact on the services and the business. Considerable manpower and/or resources needed. The RfC will have to be submitted to the board level (CAB/EC – Change Advisory Board / Emergency Committee)

Priority Setting:

- Urgent
  - Change necessary now (otherwise severe business impact)
- High
  - Change needed as soon as possible (potentially damaging)
- Medium
  - Change will solve irritating errors or missing functionality (can be scheduled)
- Low
  - Change leads to minor improvements

A change backout plan must always be possible.

Change management always ends with a review of the change.
Change: The addition, modification, or removal of approved, supported or baselined hardware, network, software, application, environment, system, desktop build or associated documentation.
Request for Change: Form or screen, used to record details of a request for a change to any CI within an infrastructure or to procedures and items associated with the infrastructure.
Forward Schedule of Changes (FSC): Schedule that contains details of all the Changes approved for implementation and their proposed implementation dates.
Change Management Process
1. Request for a Change
2. Registration and Classification
3. Monitoring and Planning
4. Approve
5. Build & Test
6. Authorize Implementation
7. Implementation
8. Evaluate

Key Concepts to Study:

- Definition of change – modification or addition to any part of the infrastructure including hardware, software, network, or related documents is a change. Anything that would result in the modification of CMDB
- Definition of CM process – standard method for implementing changes w/ minimum incidents in the infrastructure and IT services
- Request for change – formal part of the change management process, used to record details of a request for a change to any CI within an infrastructure, or to services, procedures, and items associated with the infrastructure
- Standard changes – are service requests – fully defined and approved change models, individually recorded but not individually assessed. Made routinely.
- Non-standard changes – all other modifications of the managed infrastructure
- Roles
    - Change Manager – person responsible for filtering, accepting, and classifying all RFC's. May be supported by change coordinators who represent him or her by liaising with the other areas of the org. Responsible for obtaining required authorization. Responsible for planning and coordinating the implementation of changes.
    - CAB – change advisory board – meets regularly to assess, prioritize, and plan changes. Normally only reviews more significant changes
- Not every change is an improvement but every improvement is a change
- Change management controls flexibility (changes put in that could cause an incident) vs. stability (changes put in to fix an incident)
- Roles
    - Change manager

    - CAB
- Routine management tasks should not be included, should be clearly defined and covered by procedures (mounting backup tapes, etc), they would be Service Requests
- Objective – to ensure standard methods & procedures are used with the lowest possible impact on service quality, changes are traceable
- Benefits
    - reduced adverse impact of changes on the quality of IT services
    - better estimates of the costs of proposed changes
    - fewer changes are reversed, any backouts that are implemented proceed more smoothly
    - enhanced management information ins obtained about changes, enabling a better diagnosis of problem areas
    - improved user productivity through more stable and better IT services
    - improved IT personnel productivity, as they are not distracted from their planned work by urgent changes or backout procedures
    - increased ability to accommodate frequent changes without creating an unstable IT environment
- Inputs
    - RFC's
    - CMDB information
    - Information from other processes (Capacity, budget, etc)
    - change planning (forward schedule of change)
- Outputs
    - updated change planning
    - triggers for configuration mgmt and release mgmt
    - CAB agenda, minutes, and action items
    - Change mgmt reports
- Activities
    - Submission (recording) – responsible for ensuring that all sources of change can submit RFC's and that they are adequately recorded
    - Acceptance – filtering of the RFC's and accepting for further consideration
    - Classification – sorting RFC's by category (impact – minor, substantial, major) and priority
    - Planning and approval – consolidating changes, planning and approving their development and implementation; ensuring the required resources are available, involving the CAB where necessary to achieve the above
    - Coordination – coordinating the building, testing, and implementation of the change
    - Evaluation – determining if each change was successful and learning lessons to improve the process
- Relationships
    - IM, Configuration mgmt, Prob mgmt, Release mgmt, SLM, Availability mgmt, capacity mgmt, continuity mgmt

        - IM – two sided relationship. CM puts through changes requested by IM to resolve the incident. Implementation of CM can result in incidents. IM personnel must be informed of the implementation of changes, so that they can quickly identify and resolved any related incidents
        - Configuration mgmt – tightly coupled, so much so that the two processes can be effectively integrated (which is recommended by ITIL). Changes are recorded under the control of configuration mgmt and impact analysis of changes is done by configuration mgmt. Configuration mgmt identifies the relationships between the CI being changed and other CI's to show what is being impacted.
        - Problem mgmt – Changes often requested to correct errors and solve problems. Changes can introduce new errors and so problems
        - Release mgmt – changes often result in the development and distribution of a new set of applications or technical infrastructure subject to Release mgmt disciplines. Changes are often packaged together into a release. Rollout of new releases is controlled by change management
        - SLM – SLM is involved in determining impact of changes on services and business processes. SLM may be represented on the CAB. CM reports to SLM using a Projected Service Availability report (PSA) that lists the changes to agreed SLA's and impact of the Forward Schedule of Change on service availability
        - Availability mgmt – Avail mgmt initiates changes to improve service availability. Verifies intended improvement is actually obtained. Often involved in estimating potential impact of changes since they could affect the availability of the service
        - Capacity mgmt – concerned with the cumulative effect of changes over an extended period. Capacity mgmt will propose enhancements and changes in the form of RFC's to improve use of existing capacity.
        - Continuity mgmt – work closely together to ensure that ITSCM is aware of all changes that could affect recovery plans and can take steps to ensure recovery can be completed
- KPI's –
    - number of changes completed per time unit, by category
    - rate at which changes are implemented
    - number of rejected changes
    - number of incidents resulting from changes
    - number of backed out changes
    - cost of the implemented changes
    - number of changes within resource and time estimation
- Bottlenecks

- paper based systems are too difficult to use and will present too many problems
- may be resistance against an umbrella CM authority that monitors all aspects of the IT infrastructure
- may be attempts to implement changes w/o going through agreed procedures. There MUST be an organizational reaction to such attempts.

Release Management

Objectives:
• Safeguard all software and related items
• Ensure that only tested / correct version of authorized software are in use
• Ensure that only tested / correct version of authorized hardware are in use
• Right software, right time, right place
• Right hardware, right time, right place
Tasks:
• Define the release policies
• Control of the Definitive Software Library (DSL)
• Control of the Definitive Hardware Storage (DHS)
• Distribute Software and Associated CIs
• Carry out S/W audits (using CMDB)
• Manage the software releases
• Oversee build of the software releases
Releases are done under the control of Change Management.
DSL : Definitive Software Library. Reliable versions of software in a single logical location. However, software may be physically stored at different locations.
Release Policy:
• Release Unit
• Full / Package / Delta Releases
• Numbering
• Frequency
• Emergency Change
Version Control:
• Development
• Testing
• Live
• Archive
Process:
• Software Control and Distribution (operational)
• Change Management (control)
• Configuration Management (control and administration)
Only process which creates its own policy.

Key Concepts to Study:

- Unique characteristic – only process that crosses environments of test, development, and production
- Release unit is all the CI's that are going into a release
- Releases
    - Major releases – major rollout of new hardware or software, generally with significantly increased functionality

    - Minor releases and hardware upgrades – include a number of minor improvements and fixes of known errors.
    - Emergency fixes – normally implemented as a temporary fix for a problem or known error
- Release Types
    - Delta release – partial release, only includes changed hardware and software components. Not always possible to test all links.
    - Full release – all components of the release unit are built, tested, and distributed in its entirety, including components not changed.
    - Package release – bundle of full and/or delta releases of related applications and infrastructure that are released at longer time intervals. Includes third party software upgrades
- Definitive Software Library (DSL) – secure repository that holds the definitive authorized versions (master copies) of all software CI's. May be physically in many locations.
- Definitive Hardware Store (DHS) – contains spares and stocks of hardware. Spare components and assemblies are maintained at the same level as their counterparts in the live environment
- Objectives
    - planning, coordination, and implementing of software and hardware
    - designing and implementing efficient procedures for the distribution and installation of changes to IT systems
    - ensuring that the hardware and software related to changes are traceable, secure, and that only correct, authorized, and tested versions are installed.
    - communicating with users and considering their expectations during the planning and rollout of new releases
    - determining the composition and planning of a rollout, together with change management
    - implementing new software releases and hardware in the operational infrastructure, under control of change management and supported by configuration mgmt.
    - ensuring that the original copies of software are securely stored in the DSL, hardware in the DHL, and the CMDB is updated
- Benefits
    - software and hardware in live use are of high quality because they are developed and tested under quality control before released
    - risk of errors in software and hardware combinations or release of an incorrect version is minimized
    - business carefully handles its software and hardware combinations or release of an incorrect version is minimized
    - business carefully handles its software investments
    - fewer separate implementations and each implementation is thoroughly tested
    - risk of incidents and known errors occurring is reduced by testing and controlling implementation
    - users are more involved in testing of a release

    - release calendar is published in advance so that user expectations are more in-line with the releases
    - business has a central software and hardware design and build, or procurement facility, followed by the distribution to the site
    - business can standardize software and hardware versions between sites to facilitate support
    - risk of illegal software is reduced, along with the risk of incidents and problems due to the wrong or infected software or hardware versions being introduced into the live environment
    - unauthorized copies and incorrect versions are more easily detected
- Activities
    - Release policy and planning
    - Release design, building and configuration – while change management is responsible for making sure back-out plans are created, release management is responsible for making sure they are practical
    - testing and release acceptance
    - rollout planning
    - communication, preparation, and training
    - release distribution and installation
- Relationships
    - Configuration mgmt – software added to the DSL and hardware to the DHL are recorded in the CMDB at the agreed level of detail. Status monitoring of CI's is provided by configuration mgmt
    - Change mgmt – must arrange formal testing and signoff by the users, decides how many changes may be combined in a release.
    - SLM –
- Bottlenecks
    - resistance to change
    - bypassing release management
    - urgent fixes
    - distribution
    - testing

Service Level Management

Balance between the Demand for IT services and the Supply of IT services by knowing the requirements of the business and knowing the capabilities of IT.
Objectives:
• Business-like relationship between customer and supplier
• Improved specification and understanding of service requirements
• Greater flexibility and responsiveness in service provision
• Balance customer demands and cost of services provision
• Measurable service levels
• Quality improvement (continuous review)
• Objective conflict resolution
Tasks:
• Service Catalog
• Service Level Requirements
• Service Level Agreement
• Operational Level Agreements (OLA) and Contracts
• Service Spec sheet
• Service Quality Plan
• Monitor, Review and Report
• Service Improvement Programs
• Customer Relationship Management
Minimum Requirements for an Agreement:
• Period
• Service Description
• Throughput
• Availability
• Response Times
• Signature
Other Possible Clauses:
• Contingency arrangements
• Review procedures
• Change procedures
• Support services
• Customer responsibilities
• Housekeeping
• Inputs and Outputs
• Changes
Ideally contracts are based on targets in the SLA
SLAs must be monitored regularly and reviewed regularly
• Monitor to see if service is being delivered to specification
• Review to see if service specification is still appropriate

Key Concepts to Study:

- Service Level Requirements (SLR) – detailed definitions of customer needs, used to develop, modify, and initiate services. Blueprint for SLA's
- Service Specifications Sheets (Spec sheets) – describe the relationship between functionality and technology and provide a detailed specification of the service. Translates SLR's into technical definitions
- Service Level Agreement (SLA) – agreement between the IT org and the customer which details the service or services to be provided. Describes services in non-technical terms. Serves as the standard for measuring and adjusting the IT services.
- Service Quality Plan (SQP) – contains all management information needed to manage the IT organization. Defines the process parameters of the Service mgmt processes and operational mgmt. Defines HOW services will be delivered while SLA define WHAT will be delivered.
- Operational Level Agreement (OLA) – agreement between internal IT departments detailing provisions of certain elements of a service
- Underpinning Contract (UC) – contract with an external provider defining the provision of certain elements of service
- Benefits
    - IT services are designed to meet the expectations as defined in the SLR
    - Service performance can be measured, which means that it can be managed and reported on
    - If the IT org charges customers for the use of IT services, the customer can draw a balance between the required quality and the cost
    - As the IT org can specify the services and components required, it can take more control of resource management and costs could be reduced over the long term
    - Improved customer relationships and customer satisfaction
    - Both the customer and the IT org are aware of their responsibilities and roles leading to fewer misunderstandings
- Objectives
    - integrate the elements required for the provision of IT services
    - create documents that clearly describe the services by the various elements
    - describe the service provided to the customer in a terminology that they understand
    - align IT strategy with business needs
    - improve IT service delivery in a controlled manner
- Activities
    - Identifying – customer's needs
    - Defining – services to be provided
    - Finalizing – contract, i.e. negotiating with the customer about the required service level
    - Monitoring – service levels
    - Reporting – to the customer and the IT org about the actual service levels
    - Reviewing – the service with the customer to determine opportunities for improvement
- Relationships

    - Service Desk, Availability mgmt, Capacity mgmt, IM, PM, CM, Release mgmt, continuity mgmt, security mgmt, configuration mgmt, FM
    - Service Desk – Service desk is the initial point of contact for users and aims (through IM) to recover the agreed service levels as soon as possible. Can often provide info about the quality perception of SLM by the users
    - Availability mgmt – responsible for realizing and optimizing the availability of the services. SLM provides the input about the required availability of the IT services. Availability mgmt provides info about the actual availability to SLM
    - Capacity mgmt – provides information about the impact of new service or extension of an existing service on the overall capacity, indicates if the use made of a service is within the agreed limits. SLM provides info to capacity mgmt about expected current and future use agreed upon with (or about to be) with the customer
    - IM & PM – good indicators of effected implementation of SLA's. SLM uses information from reports provided by these processes when reporting to the customer
    - CM – SLA's can define the changes that can be requested, time for responding to these changes, cost, etc. CM may affect the service levels that have been agreed upon.
    - Release mgmt – monitors the agreements made by SLM regarding the provision of hardware and software. SLM reports on the quality of the IT service on the basis of info from release mgmt reports
    - ITSCM – agreements about recovery times in the event of a disaster are made with the customer through the SLM process. The measures and costs are included in the SLA. Changes to the service and SLA may require modification of the defined continuity measures and procedures.
    - Security mgmt – both the IT org and the customer will have certain security requirements. Those agreements are defined in the SLA. Security mgmt ensures that the agreed security measures are implemented, monitored, and reported to SLM.
    - Configuration mgmt – responsible for entering the details of the components and documentation related to a service in the CMDB, and providing information from this database. Creation or modification of a service or SLA will affect the CMDB. The CMDB is used check the agreements about the response and solution times and is used to report about the quality of the CI's. This enables SLM to report about the quality of the service provided.
    - FM - if customer charged for services then this is included in the SLA. FM provides SLM with info about the costs associated with providing a service.
- Critical Success factors
    - capable Service Level Manager with both IT and business expertise, and a supporting org
    - clear process mission and objectives

    - awareness campaign to provide people with info about the process, develop understanding, and gain support
    - clearly defined tasks, authorities, and responsibilities within the process, distinguishing between process control and operational tasks
- KPI's
    - service elements included in SLA's
    - elements of SLA supported by OLA and UC's
    - elements of SLA's which are monitored, where shortcomings are reported
    - elements of SLA's which are regularly reviewed
    - elements of SLA's where the agreed service levels are fulfilled
    - shortcomings, which are identified and covered by an improvement plan
    - actions, which are taken to eliminated these shortcomings
    - trends identified with respect to the actual service levels
    - number of times SLA not fulfilled
- Roles
    - Service Level Manager
        - creating and updating the service catalog
        - defining and maintaining an effective SLM process for the IT organization including SLA structure, OLA's with internal providers, UC's with external providers
        - updating the existing Service Improvement Program
        - Negotiating, concluding, and maintaining SLA's, OLA's, and UC's.
        - Reviewing the performance of the IT org and improving it where needed
- Bottlenecks
    - may require culture change in organization
    - customers may need help specifying SLR's
    - can be difficult to express expectations of the customer in terms of measurable standards and associated costs
    - SL manager should be wary of overambitious agreements whilst the planning, measuring, and monitoring tools, procedures, SQP, and the UC's have not been developed.
    - Overhead costs associated with monitoring and measuring service levels are easily underestimated
    - Skipping the analysis of the requirements of the customer, the design stage, and the development of the SQP can result in a process which is difficult to manage and which does not provide clear, measurable standards
    - SLM documents and process could end up becoming ends in themselves instead of a means to better the relationship between the IT service provider and the customer

Continuity Management

Why plan?
• Increases Business dependency on IT
• Reduced cost and time of recovery
• Cost to customer relationship
• Survival
Many businesses fail within a year of suffering a major IT disaster.
Business Impact Analysis:
Risk Analysis:
• Value of Assets
• Threats
• Vulnerabilities
Risk Management:
• Countermeasures
• Planning for potential disasters
• Managing a disaster
Risk Analysis: Based on the CCTA Computer Risk Analysis and Management Methodology (CRAMM)
Options:
1. Do nothing
2. Manual workarounds
3. Reciprocal arrangements
4. Gradual Recovery (cold standby)
5. Intermediate Recovery (warm standby)
6. Immediate Recovery (hot standby)
Cold start = accommodation. Environmental controls; power and communications
Hot start = cold start + computing equipment and software
7 Sections of the Plan:
1. Administration
2. The IT Infrastructure
3. IT Infrastructure management & Operating procedures
4. Personnel
5. Security
6. Contingency site
7. Return to normal
Test and Review:
• Initially then every 6 to 12 months and after each disaster
• Test it under realistic circumstances
• Move / protect any live services first
• Review and change the plan
• All changes made via the CAB – Change Advisory Board
Contingency Plan:
• Assists in fast, controlled recovery
• Must be given wide but controlled access

• Contents (incl. Admin, Infrastructure, People, Return to normal)
• Options (incl. Cold & Hot Start)
• Must be tested regularly – without impacting the live service

Key Concepts to Study:

- Disaster – an event that affects a service or system such that significant effort is required to restore the original performance level
- Helps organizations in restoring IT services ASAP after a disaster & ensuring continuity of business operations
- Enables organization to continue to provide the predetermined and agreed level of IT Services even after a calamity
- Benefits
    - Business continuity – helps in reducing risks to an acceptable level by developing plans for immediate restoring business activities if interrupted by a disaster
    - Organizational credibility – helps develop contingency facilities to increase an organizations credibility and reputation
    - Infrastructure recovery – eases faster recovery
- Recovery Plans –
    - include info like minimum required production capacity and provision of services at all times to ensure uninterrupted business operations.
    - Address risks which cannot or have not been eliminated.
    - Provides recovery options.
    - Sections – introduction, updating, routing list, recovery initiation, contingency classification, specialist sections
- Risk analysis –
    - identifies the risks that are likely to occur,
    - includes details on assets, threats, and vulnerabilities to them,
    - prevention measures,
    - recovery plans
- IT Service Continuity Strategy – process of dealing with disasters
- Inputs
    - SLA's
    - Availability, Capacity, and Configuration mgmt specification of resources that can be used for ensuring service continuity
    - Change management
- Results – recovery plan
- Phases
    - Initiation
        - determine scope by defining organizational policy
        - ID relevant areas to apply ITSCM
        - Allocation of resources
        - Setting up recovery projects w/i organization
    - Requirements and Strategy

        - ID requirements for ITSCM process and strategy to be adopted
        - Includes business impact analysis, risk assessment, and IT Service Continuity Strategy
        - Business impact analysis – determined by costs due to additional resource requirements and cascading effect of risks spreading to services related to disaster-prone service
        - Risk assessment – ID's IT components, threats & probabilities, vulnerability and counter measures
        - IT Service Continuity Strategy – no prevention available then adopt recovery option
            - Do nothing – do not need IT Services
            - Return to Manual – assumes personnel can handle this
            - Reciprocal agreements – orgs agree to use each others' facilities
            - Gradual recovery – can operate w/o IT Services for fixed time (cold stand-by)
            - Immediate recovery – similar environment created at different location, change over (warm stand-by)
            - Intermediate recovery – identical production environment including replication of data and production process (hot start, hot stand-by)
            - Combination
    - Implementation
        - Organizational planning, preventative measures & recovery options, developing plans and procedures
        - Organizational & Impl planning – address issues such as emergency response, damage assessment, crisis management, & human resource plans
        - Preventative measures & recovery options – need to draft stand-by agreements by negotiating off-site recovery facilities w/ third party, maintenance and equipment recovery facility, purchasing and installing stand-by hardware, managing dormant contracts
        - Develop plans and procedures – provide framework to draft procedures that involve installing and testing hardware and network components, restoring applications, database, and data
    - Operational Management
        - Training and awareness
        - Maintaining
        - Testing
- Key Roles
    - Business Contingency Manager (BCM) – aims at reducing risks by developing recovery plans to restore business activities
    - Board – Chief Op Offices Directors, Chief exec officer
        - define org policies and strategies
        - manage crisis
        - make timely decisions

    - Senior Mgmt – Business Unit Mgrs, Regional Mgrs
        - manage business processes and set departmental strategies
        - coord execution of recovery plan
        - managing personnel
        - involved in Recovery plan
        - resolving conflicts
        - provide funds, personnel, and resources
    - Mgmt – Project mgrs & department heads
        - define client deliverables
        - analyze risks
        - prepare contracts w/ customer, user, and suppliers
        - initiate activities, leading teams, reporting to Sr. mgmt
    - Team Leaders & Team Members
        - key people developing project deliverables and implementing procedures
        - executing recovery plan
        - reporting issues
        - provide details for future plans
- Relationships
    - SLM – specifies time & resources required to recover. Uses this to build SLA's. ITSCM process must then ensure agreed turnaround time
    - Availability Mgmt – specifies risk reduction measures & resilience, reduce vulnerability, ITSCM process id's resource level needed. Ensures availability
    - Configuration Mgmt – defines minimum configuration and IT infrastructure components needed for restoring services. ITSCM defines resources that underline continuity
    - Capacity Mgmt – determines min capacity needed to con't business operations and for recovery options. ITSCM provides info about capacity requirements & service level to be maintained
    - Change Mgmt – all changes must be communicated to the ITSCM process so the impact on the recovery plan can be assessed. ITSCM communicates changes to plan to CM
    - Security Mgmt – provides info about min security process. ITSCM includes requirements in plan and tests
- Bottlenecks
    - attitude/commitment
    - insufficient resources and support
    - unplanned implementation and infrequent testing
    - access to recovery facilities
    - estimating the damage
    - budgeting
    - perpetual delay
    - Black boxing – manager has abdicated responsibility (outsourced)
    - familiarity with the business
    - lack of awareness

- KPI's
  - # of short comings id'd in recovery plan
  - cost to company because of loss if recovery plan not executed
  - cost incurred in terms of time, resources, and money to restore IT services
- Critical success factors
  - cooperation and commitment w/i organization to create & execute recovery plan
  - effective installation and backup tools
  - effective impl of config mgmt process
  - training
  - unexpected testing of recovery plan
- Cold site – have to set up hardware after disaster
- Warm site – hardware is there, maybe software, no data
- Hot site – immediate recovery, complete mirroring of production process, high availability

Financial Management

Objectives:
To provide information about and control over the costs of delivering IT services that support customers business needs.

Costing is a must!

Input cost units recommended by ITIL:
• Equipment Cost Units (ECU)
• Organization Cost Units (OCU)
• Transfer Cost Units (TCU)
• Accommodation Cost Units (ACU)
• Software Cost Units (SCU)
Equipment = hardware
Organization = staff
Transfer = costs which IT incurs acting as an agent for the customer, they do not appear as a cost against the IT department's budget
Accommodation = buildings
Software = software
Different Cost Types:
• Fixed - unaffected by the level of usage
• Variable - varying according to the level of usage
• Direct - usage specific to one service
• Indirect or Overhead – usage not specific to one service
• Capital – not diminished by usage
• Revenue or running – diminish with usage
Charging Objectives:
• Recover from customers the full costs of the IT services provided
• Ensure that customers are aware of the costs they impose on IT
• Ensure that providers have an incentive to deliver and agreed quality and quantity of economic and effective services
Charging and Pricing Options:
Charging:
• No Charging – IT treated as support center
• Notional Charging – IT treated as cost center
• Actual Charging
Pricing:
• Recover of Costs – IT treated as a service center
• Cost Price Plus – IT treated as a profit center
• Market Prices – IT treated as a profit center
Support and Cost centers used "soft charging" in which no money changes hands; service and profit centers use "hard costing" in which money is transferred between bank accounts
Profit centers focus on the value of the IT service to the customer

Good Financial Management minimizes the risks in decision making
3 Main Processes:
Budgeting: The process of predicting and controlling the spending of money within the enterprise and consists of periodic negotiation cycle to set budgets (usually annual) and the day-to-day monitoring of the current budgets. Key influence on strategic and tactical plans.
IT Accounting: The set of processes that enable the IT organization to fully account for the way its money is spent (particularly the ability to identify costs by customer, by service, by activity).
Charging: The set of processes required to bill a customer for the services applied to them. To achieve this requires sound IT Accounting, to a level of detail determined by the requirements of the analysis, billing, and reporting procedures.

Key Concepts to Study:

- Definition – process of tracking service costs and implementing the most cost-effective services to meet customer demands
- Objectives –
    - aid IT organization in implementing cost-effective strategy for delivering IT services
    - break down costs into service specific components
    - help categorically associate costs w/ each individual service and department
- Benefits
    - Determines cost of IT services
    - Id's cost structure
    - Recovering costs from customers
    - Operating the IT department as a business unit
    - Verifying that chareges for IT services are realistic
- Concepts
    - Budgeting –
        - defines a way to plan and control expenditures
        - lays down limits
        - prepared to ensure actual expenditure does not exceed planned
        - developed by unit heads
        - must be kept in line w/ actual monetary resources
    - Accounting –
        - maintains a detailed account of all incoming and outgoing funds
        - includes detailed ledgers of daily expenditures incurred during implementation of IT services.
        - tracking direction of outflow more important than tracking exact costs
    - Charging for IT services
        - helps org recover its expenditures from its customer
        - encourages business like relationship between org and customers

        - should aim to influence customer's demands, should not aim to meet all demands
    - Cost Categories
        - Direct vs. Indirect
            - Direct – are unambiguously linked to a specific service
            - Indirect – are not specifically associated w/ a specific service
        - Fixed vs. Variable
            - Fixed – constant such as rent of facilities, not related to volume
            - Variable – related to IT service being provided, varies with volume
        - Capital vs. Operational
            - Capital – generated by purchase of assets intended for long term use, calculated based on depreciated value
            - Operational – generated by day to day costs not directly related to production resources i.e. insurance premiums
- Inputs
    - from SLM describing service requirements submitted as requests for approval of funds. FM process scrutinizes these requests
- Phases
    - ID IT needs of org. Based on these, plan budgets and financial objectives (budget)
    - ID and setup cost control methods by analyzing cost for the service (accounting)
    - Charge appropriate amount to customer (charging)
    - Request and receive feedback from customer about charges
- Activities
    - Budgeting
        - define long term objective of org and create financial plans for specific time periods
        - Ensures services are continuously available at reasonable costs
        - Zero-based – after a few years, does not use last years data as basis for current year. Each service is justified
        - Incremental – previous years data used. Factors for inc or dec are mentioned
        - ID factors that might hinder the growth prospects
        - Outline secondary budgets (sales & marketing, prod, admin, cost & investment)
        - Determine period of budget
    - Accounting
        - id's how costs are defined and divided into different categories and recorded
        - generally calculated for a department, customer, or product
        - cost structure helps id and track costs for hardware, software, and support of a service

- Charging
  - charging encourages the IT org to operate as a business
  - charging customer helps recover costs
  - charge at a reasonable rate or customer demand my decrease
  - charging should not be limited to IT service
  - should be synchronized with financial policies
  - helps organization to use services to compliment business needs through direct funding (process of charging customer and collecting funds for services)
  - Based on objectives of financial management process – communicating info, pricing flexibility, notional charges (costs invoiced but need not be paid)
- Pricing
  - accurate calculation of cost of service must be complete before pricing
  - deciding the objectives of charging
  - determining direct costs, indirect costs, and market rates
  - analyzing demand
  - analyzing number of customers
  - Cost Plus – cost incurred plus profit margin
  - Going Rate – for services where there are already price agreements
  - Target Return – services whose price was determined in advance
  - Negotiated Contract Price – prices discussed with the customer

- Roles
  - IT Finance Manager
    - owner of process
    - responsible for developing and implementing process
    - works with other departments and financial departments to develop guidelines for financial activities
    - responsibilities may be distributed between Mgr and Financial dept
    - Manage IT organization budget
    - Reporting to IT mgrs and customers about conformance to budget
    - gathering cost data for all implementation services
    - implementing suitable accounting policies
    - providing justifications for IT service charges
    - preparing regular bills
- Relationships
  - SLM, Capacity, and Configuration are directly linked
  - Release mgmt, IM, and Availability Mgmt are indirectly linked
  - SLM –
    - helps determine cost effectiveness and viability of proposed service.
    - needs details about costs and proposed charges for service before service is implemented
    - SLA agreements include cost details

        - To define costs and charges the SLM process derives info from the FM process which specifies costs and service charging methods and rates
    - Capacity Mgmt – capacity levels depend on cost considerations for each service provided by FM
    - Config Mgmt – FM obtains info about infrastructure components used for services combined w/ SLA's to determine prices and rates. FM provides details about costs calculated for the infrastructure to the config mgt process
- Bottlenecks
    - non availability of written material
    - difficulty in obtaining planning details
    - improper documentation of corp strategy and objectives
    - difficulty locating skilled personnel
    - insufficient cooperation
    - lack of management commitment
- KPI's
    - cost-benefit analysis comparing the relative benefits of service w/ costs
    - feed back from customers about implemented services
    - financial targets achieved by IT org defined by budgets
    - changes in use of services
    - timely reports sent to SLM process
- Critical success factors
    - create awareness among users about cost of implementing services
    - implement a detailed cost monitoring system that justifies all expenditures
    - provide effective services at reasonable costs
    - create complete awareness about impact and cost of implementing FM process
    - provide access to relevant info from configuration mgmt process

Security Management

Key Concepts to Study:

- Ensures data security by preventing unauthorized access to information
- Objectives
    - Comply with security requirements for SLA's
    - Meet w/ external requirements not defined in contracts, legislation, and policies
    - Provide basic level of security to information systems independent of external requirements
    - Ensure effective security measures taken at strategic, tactical, and operational levels
- Benefits
    - Providing correct and complete information
    - maintaining standards
    - enhance value of IS
    - ensure continuity (any unplanned outage)
    - security related objectives
- Information Security – Safety of information from known and unknown risks
- Confidentiality – protecting organizational information from unauthorized access and use
- Integrity – ensures accuracy, completeness, and timeliness of information
- Availability – ensures organizational information accessible
- Privacy – maintains privacy by allowing owners to restrict unauthorized users
- Verifiability – ensures correct usage of information and effective implementation of security measures
- Inputs
    - SLA's, policies, external requirements
    - SLA's – define customer security specifications
    - Policies – define organization security requirements
    - External – specify issues to keep in mind when interacting w/ external sources
- Physical security – who can get into secure areas
- Technical security – firewalls, password control, antivirus software
- Policy security – password changing policies
- Security is part of each SLA not part of operational agreement

Capacity Management

Objective:
To determine the *right, cost justifiable, capacity* of IT resources such that the Service Levels agreed with the business are achieved at the *right time*.
Objectives:
• Demand Management
o Business Capacity Management
• Workload Management
o Service Capacity Management
• Resource Management
o Resource Capacity Management
While doing the above, also need to do:
• Performance Management
o Internal and External Financial Data
o Usage Data
o SLM Data / Response Times
CDB – Capacity Data Base – Contains all Metrics, etc. Used to create a Capacity Management Plan. Performance Management Data populates the CDB.
Essentials:
• From Customer Demands to Resources
• Demand Management
• Workload Management
• Performance Management
• Capacity Planning
• Defining Thresholds and Monitoring
Application Sizing: To estimate the resource requirements to support a proposed application change to ensure that it meets its required service levels.
Modeling:
• Trend Analysis
• Analytical Modeling
• Simulation Modeling
• Baseline Models
• Used to Answer the "What If… " questions
• Data for Modeling comes from the CDB

Key Concepts to Study:

- Performance mgmt – measuring, monitoring, and tuning the performance of IT infrastructure components for optimum performance
- Application Sizing – determining the hardware or network capacity needed to support new or modified services and the predicted future workload

- Modeling – using analytical, simulation or trending models to determine the capacity requirements of services and determining the best capacity solutions. Allows various scenarios to be analyzed and the "what-if" questions addressed
- Workload mgmt – dealing with understanding what the various business drivers are doing, and what resources they require – a foundational component of modeling, but also stands alone.
- Capacity planning – developing a Capacity Plan, based on a Capacity mgmt database, analyzing the current situation and predicting the future use of the IT infrastructure and the resources needed to meet expected demand for the IT services (preferably using scenarios)
- Aims to consistently provide the required IT resources at the right time, and at the right cost, aligned with the current and future requirements of the business.
- Benefits
    - reduced risks associated with existing services as the resources are effectively manage, and the performance of the equipment is monitored continuously
    - reduced risks associated with new or modified services as Application Sizing means that the impact of new or modified services on existing systems in known
    - reduced costs as investments are made at the appropriate time
    - reduced business disruption through close involvement with CM when determining the impact on IT capacity. Preventing urgent changes resulting from inadequate or incorrect capacity estimates
    - more reliable forecasts providing quicker and more accurate response to customer requests
    - greater efficiency as demand and supply are balanced at an early stage
    - manage or even reduced capacity-related expenditure as capacity is used more efficiently
- Inputs
    - technology
    - service levels
    - business plans, strategy, requirements, volumes
    - operational schedules
    - deployment programs
    - project plans
    - forward schedule of change
    - incidents and problems
    - financial plans
    - budges
- Activities
    - Business Capacity management – trend, forecast, model, protype, size and document future business requirements
    - Service Capacity mgmt – monitor, analyze, tune, and report on service performance, establish baselines and profiles for use of services, manage demand for services

    - Resource capacity mgmt – monitor, analyze, run, and report on the utilization of component, establish baselines and profiles of use of components
    - Developing the Capacity Plan
    - Modeling
    - Application sizing
    - monitoring
    - analysis
    - tuning
    - implementation
    - demand management
    - populating the capacity database
- Outputs
    - capacity plan
    - capacity database
    - baselines and profiles
    - thresholds and alarms
    - capacity reports
    - service level recommendations
    - costing and charging recommendations
    - proactive changes
    - service improvements
    - revised operational schedules
    - effectiveness reviews
    - audit reports
- Relationships
    - IM, PM, CM, Release mgmt, Config mgmt, SLM, FM, ITSCM, Availability mgmt
    - IM informs capacity mgmt about incidents logged due to capacity or performance issues. Capacity mgmt can provide scripts for IM to assist with diagnosis or resolution of capacity problems
    - PM – Capacity mgmt tools, information, knowledge, and expertise can be used to assist PM with various activities
    - CM – capacity should be part of the CAB. Capacity mgmt provides information about the need for capacity and the potential impact of a change on the provision of service. Info about the changes provides valuable input to the Capacity plan. Capacity mgmt can also submit RFC's during implementation of the plan
    - RM – Capacity ensure that sufficient capacity is available in all required areas of distribution planning when the network and distribution servers are used for automatic or manual distribution
    - Config mgmt – information provided by the CMDB is essential for developing and effected CDB
    - SLM – advises SLM about the feasibility of service levels. Capacity mgmt measures and monitors performance levels and provides info for checking and changing the agreed service levels when needed

    - FM – capacity supports investment budgeting, cost/benefit analysis, and investment decisions. Capacity also provides essential info for charging capacity-related services. Essential that the Capacity Plan is consistent with all aspects of financial planning and plans
    - ITSCM – capacity mgmt specifies the min capacity needed to continue or recover service provision in the event of a disaster. Capacity needs of ITSCM should be constantly reviewed to ensure that they reflect day-to-day changes in the operating environment
    - Availability mgmt – Performance and capacity problems can result in poor quality IT services which can be equated with service Unavailability
- Critical success factors
    - accurate business forecasts and expectations
    - understanding of the IT strategy and planning and its accuracy
    - knowledge of current and future technologies
    - cooperation with other processes
    - an ability to demonstrate cost effectiveness
- KPI's
    - predictability of the customer demand
    - technology – ability to continually achieve the agreements laid down in the SLA even when using older technology
    - cost – reduction in number of rushed purchases, reduction in unneeded overcapacity, drawing up investment plans early on
    - operations – reduction in number of incidents due to performance or capacity issues, ability to meet customer demand all the time, extent to which capacity mgmt is taken seriously
    - reduced discrepancies about actual and planned capacity
    - reduced impact on service levels
- Roles
    - Capacity manager – manage the process, ensure that the capacity plan is developed and maintained, ensure that the CDB is kept up to date.
    - System, Network, and Application mgrs – assisting with the optimization of resources within their own areas, required to provide advice and assistance on technical issues within their area of specialized knowledge
- Bottlenecks
    - Unrealistic expectations
    - lack of appropriate information
    - supplier input or benchmarks
    - implementation in complex environments
    - determining the appropriate level of monitoring
    - lack of management support

Availability Management

Objectives:
• To predict, plan for and manage the availability of services by ensuring that:
o All services are underpinned by sufficient, reliable and properly maintained CIs
o Where CIs are not supported internally there are appropriate contractual agreements with third party suppliers
o Changes are proposed to prevent future loss of service availability
• Only then can IT organizations be certain of delivering the levels of availability agreed with customers in SLAs.
Aspects of Availability:
• Reliability
• Maintainability: Maintenance you do yourself, as a company
• Resilience: Redundancy
• Serviceability: Maintenance done by someone else
Availability Information is stored in an Availability Database (ADB). This information is used to create the Availability Plan. SLAs provide an input to this process.
Unavailability Lifecycle
MTTR: Mean Time to Repair (Downtime) – Time period that elapses between the detection of an Incident and it's Restoration. Includes: Incident, Detection, Diagnosis, Repair, Recovery, Restoration.
MTBF: Mean Time Between Failures (Uptime) – Time period that elapses between Restoration and a new Incident.
MTBSI: Mean Time Between System Incidents – Time period that elapses between two incidents. MTTR + MTBF.

"An IT service is *not available* to a customer if the functions that customer requires at that particular *location* cannot be used although the *agreed conditions* under which the IT service is supplied are being met"

Key Concepts to Study:

- Availability – IT service is continually available to the customer, little downtime, rapid service recovery
- Reliability – the service is available for an agreed period without interruptions, increases if downtime prevented
- Maintainability and recoverability – activities needed to keep the service in operation and restore it when it fails, includes preventative maintenance and scheduled inspections
- Serviceability – contractual obligations of external service providers. Define the support to be provided for the outsourced services
- Objectives –
    - provide cost effective and defined level of availability of the IT service that enables the business to reach its objectives

    - alignment of the customer demands with what the IT infrastructure and IT org is able to offer
    - ensure that the achieved availability levels are measured and improved continuously
- Benefits
    - IT services that are designed, implemented and managed fulfill the agreed availability requirements
    - single contact and person responsible for availability of products and services
    - new products and services fulfill the requirements and availability standard agreed with the customer
    - associated costs are acceptable
    - availability standards are monitored continuously and improved
    - Appropriate corrective action is undertaken when a service is unavailable
    - occurrence and duration of unavailability are reduced
    - emphasis is shifted from remedying faults to improving service
    - easier for the IT org to prove its added value
- Activities
    - Planning
        - Determining the availability requirements
        - designing for availability
        - designing for recoverability
        - security issues
        - maintenance management
        - developing the availability plan
    - Monitoring
        - Measuring and reporting
            - Mean time to repair – average time between the occurrence of a fault and service recovery (downtime). Sum of the detection time and resolution time. Relates to recoverability and serviceability
            - Mean time between failures – mean time between the recovery from one incident and the occurrence of the next, uptime. Relates to reliability
            - Mean time between system incidents – meant time between the occurrences of two consecutive incidents. sum of MTTR and MTBF
    - Methods and techniques
        - Component Failure Impact Analysis
            - uses availability matrix with the strategic components and their roles in each service.
        - Fault Tree Analysis
            - technique used to identify the chain of events leading to failure of an IT service.
            - Separate tree drawn for every service
        - CCTA risk analysis and management method

            - means of identifying justifiable countermeasures to protect confidentiality, integrity, and availability of IT infrastructure
        - availability calculations
        - Service Outage Analysis – used to identify causes of faults, investigate effectiveness of IT organization, present and implement proposals for improvement
        - Technical Observation Post – dedicated team of specialists focuses on a single aspect of availability
- Inputs
    - business availability requirements
    - impact assessment for al business processes supported by IT
    - availability, reliability, and maintainability requirements for the IT components in the infrastructure
    - data about faults affecting services or components, generally in the form of incident and problem records and reports
    - configuration and monitoring data about the services and components
    - achieved service levels, compared with the agreed service levels for all services covered under the SLA
- Outputs
    - availability and recovery design criteria for new and improved IT services
    - technology needed to obtain the required infrastructure resilience to reduce or eliminate the impact of faulty infrastructure components
    - availability, reliability, and maintainability guarantees of infrastructure components required for the IT service
    - reports about the achieved availability, reliability, and maintainability
    - availability, reliability, and maintainability monitory requirements
    - availability plan for the proactive improvement of the IT infrastructure
- Relationships
    - SLM, Config mgmt, capacity mgmt, ITSCM, PM, IM, Security mgmt, CM
    - SLM – availability is one of the most important elements in SLA's
    - Config mgmt – provides info about the infrastructure
    - Capacity mgmt – Changes in capacity often affect the availability of a service and changes to the availability with affect the capacity. Capacity provides information about the infrastructure. The two processes often exchange information about scenarios for upgrading or phasing out IT components and about availability trends that may necessitate changes to the capacity requirements
    - ITSCM – provides information about critical business process. Many measures taken to improve availability also enhance ITSCM and vice versa
    - PM – directly involved in identifying and resolving the causes of actual or potential availability problems
    - IM – provides reports to determine the achieved availability

    - Security mgmt – security criteria have to be considered when determining availability requirements. Availability mgmt can provides info to Security mgmt about new services.
    - CM – availability mgmt informs Change mgmt about maintenance issues related to new services and elements thereof. Initiates change mgmt process to implement changes necessitated by availability measures. CM informs AM about scheduled changes
- Critical success factors –
    - business must have clearly defined availability objectives and wishes
    - SLM must have been set up to formalize agreements
    - both parties must use the same definitions of availability and downtime
    - both the business and IT org must be aware of the benefits of availability mgmt
- KPI's
    - percentage availability (uptime) per service or group of users
    - downtime duration
    - downtime frequency
- Roles
    - Availability mgr
        - defining and developing the process in the org
        - ensuring that IT services are designed such that the achieved service levels in terms of availability, reliability, serviceability, maintainability, and recoverability correspond with the agreed service levels
        - reporting
        - optimizing the availability of the IT infrastructure to provide a cost-effective improvements of the service provided to the business
- Bottlenecks
    - senior management divides responsibility for availability between several disciplines
    - each manager feels responsible for his or her own area, no overall coordination
    - IT mgmt fails to understand the added value provided to the IM, PM, and CM processes
    - current availability level is consider sufficient
    - no support for appointing a single process manager
    - process manager does not have required authority
    - underestimating resources
    - lack of effective measurement and reporting tools
    - lack of other processes such as SLM, Config mgmt, and PM

About the ITIL Exams

Who Administers the Exams?
EXIN is an independent organization establishing educational requirements, and developing and organizing examinations in the field of Information Technology, including ITIL as well as other subject areas. EXIN exams are available in eleven languages.

Together with OGC and itSMF, EXIN is a founding member of the international ITIL certification board. In the past EXIN successfully launched the ITIL Foundation and ITIL Practitioner certificates and played a leading role in modernizing the examinations for the ITIL Manager's Certificate in IT Service Management.

EXIN certifies ITIL-professionals for ITIL Foundation, ITIL Service Manager and ITIL Practitioner, all over the world.

Foundation Certificate in IT Service Management (the topic of this Study Guide)
This certifies that the holder has a basic understanding of the ITIL principles: the terminology, the Service Desk function, the 10 core processes and their relationships and interfaces with other processes and the business.

This certificate is awarded after exam participants achieve a passing grade of 65% on a multiple-choice examination.

Practitioner Certificate in IT Service Management
A practitioner certificate is available for most processes. It identifies that the holder has in depth knowledge of the applicable ITIL process and is capable of managing and implementing that process in an organisation. The prerequisite is three to four years of line management experience in IT plus the Foundation Certificate in IT Service Management. This certificate is awarded after exam participants achieve a passing grade of 60% on a multiple-choice examination.

The Exams cost £110 + VAT, or part resit at £55 + VAT

For overseas costs please contact Julie Kittle by email **jk@ksl.org** or call +44 (0) 1270 611600

Manager's Certificate in IT Service Management
This certifies that the holder has an overall management view of the Service Desk, the 10 core disciplines of IT Service Management and their interrelationships and interfaces. It also identifies that the holder is capable of overseeing and managing an entire IT Service Management department either in the implementation stages or in a standing organisation.

The prerequisite is three to four years of management and/or consulting experience plus the Foundation Certificate in IT Service Management.

This certificate is awarded after participants meet the following criteria:

- Receive a passing grade of 50% on a management skills assessment
- Receive a passing grade of 50% on the Service Support examination and a passing grade of 50% on the Service Delivery examination

Typically the Managers course is 2 x 1 weeks training and costs for the Managers exam are £130 per paper, and there are 2 papers to take. Managers exams can only be taken at certain times, and usually only by an accredited training organisation. Email **jk@ksl.org** for further information.

All examinations are designed to be taken following an approved training course. The examinations are held regularly, in several countries and languages around the world.

ITIL Pins
It has been a well-known tradition for years that passing an ITIL-exam does not only result in a certificate, but is also accompanied by the presentation of this pin. This distinguishing badge in the form of the internationally well-known ITIL-logo, exists in 3 colors:

- green, for the Foundation Certificate
- blue, for the Practitioner's Certificate
- red, for with the Manager's Certificate

More information:
http://www.exin-exams.com

Are there any pre-requisites for taking the ITIL Exam?

There are no formal entry requirements for the course or examination, but it is assumed that all delegates will have a basic level of IT literacy. The course will be suitable for... Staff entering an IT environment who might have day-to-day responsibilities within one or more of the service management disciplines

Staff working in an IT service management discipline who wish to broaden their understanding of how their role fits into the wider service management framework

Other staff whose effectiveness would be enhanced by a greater awareness and

understanding of best practices in IT service management

What does having "ITIL Certification" mean?
The holder of the Foundation Certificate in IT Service Management should be aware of the techniques involved across the range of service delivery and service support activities. He or She should be able to relate these activities to each other and to wider IT issues, and should be competent to participate in service delivery/support functions, or to apply this knowledge to their own work environment.

How much does the ITIL exam cost?
The Cost of the Foundation exam is £100.00 + VAT.

How do I get Recognised In ITIL?
It depends on whether you are an individual or a company. To get recognised in ITIL as an individual you need to achieve certification at Foundation, Manager or Practitioner level. As a very rough guideline if you are involved in IT in a supporting role (you may be in a marketing, administration or technical job), Foundation level may be suffice. If generally you are leading IT projects then Practitioner is the level you should be aiming at.
For companies wishing to adopt ITIL, the route tends to be slightly different. The biggest decision is deciding if ITIL is right for you, and that requires an investment of time, collecting and reviewing information from the marketplace.

Why do I need an ITIL Qualification?
Individual
The majority of people that consider ITIL as a qualification do so for career and personal development reasons. Often this is driven by a change of job or career, where you notice that to get to the top of the CV pile, you need to have an extra qualification like ITIL (even if you have been involved in service management successfully for many years without it). In many advertised positions ITIL has become a prerequisite.
Company
The majority of companies that implement ITIL also encourage their employees to take the exams. If your staff have accredited ITIL qualifications, then you can present your company as using ITIL. This works particularly well where you tender for or supply to any large IT organisations or outsourcing companies.

What languages are the ITIL examinations available in?
The Foundation examinations are available in English, French, Spanish, German, Portugese, Chinese, Japanese and Russian. The Practitioner examinations are available in English only. The Service Manager examinations are available in English, German and Russian.

If I take a an ITIL Foundation course in Spanish, French, German etc.
Do I still have to learn the ITIL terms in English?

Yes, you do. In the examinations you will find both the English as well as the Spanish terms. The ITIL terms can be found in the exam requirements.

How many questions can I expect on my exam?
The examination will consist of a one-hour "closed book" multiple-choice paper, containing 40 questions.

How much time does the exam take?
The Foundation Exam takes 1 Hour.

Can I take the ITIL Foundation exam on-line?
You can take the English exam ITIL Foundation on-line at one of the Prometric test centres. See http://securereg3.prometric.com/ for more details

How long do I have to wait for the results of my multiple choice examinations?
For each multiple choice exam, every candidate receives the result paper and certificate within four weeks after the examination session.

How does a candidate receive the result and the certificate of an EXIN or ISEB examination?
The Authorised Examination Centres (AEC) that organized your EXIN examination will also provide you with a result paper and, if you passed, a certificate. The AEC will receive the results and certificates from EXIN.
After a computer based (Prometric) or web based multiple-choice examination you will receive the result immediately after finalizing the examination. The certificates will then be sent to you via the AEC or by EXIN directly.

How can I change the names printed on the certificate?
At the start of the examination session one fills in the Personal Data Form. On this form there is an item where you can specify exactly how your name should be printed on the certificate.

How can I retake the exam if I fail? And how many times?
In the unfortunate case you failed an examination, you can take part in another examination session. This does not necessarily have to be at the same AEC. For the retake of a Foundation examination you could for example turn to one of the Prometric Testing Centers. There is no limit to the number of times you can retake the examination.

What is the pass rate of the EXIN examinations?
Obviously, the pass rates fluctuate. EXIN does not change the pass mark automatically if a group of candidates' scores below the current pass rate. Dropping Pass rates may indicate a problem in either the preparation of the candidates or in the quality of the examination paper. EXIN monitors the exam results and investigates deviations to take appropriate measures.

Over the last year the pass rate of the ITIL examinations were approximately...
ITIL Foundation 85%
ITIL Practitioner 65%
ITIL Service Support 55%
ITIL Service Delivery 65%

I earned my Foundation Certificate a few years ago. Will I have to update this certification with the release of the new exams?
No. Your Foundation Certificate is still valid and can be used in the future to fulfill part of the prerequisites for Practitioner and/or Service Manager exams.

I passed my Service Delivery exam a few years ago and would like to take the Service Support exam. Will I need to re-sit the new Service Delivery exam to qualify for the Manager's Certificate in IT Service Management?
No. Passing a mix of the old and new exams will still qualify towards the requirements to obtain your Manager's Certificate in IT Service Management.

What is Prometric and what is its role?
Thomson Prometric is a worldwide provider of computer based examinations. The EXIN ITIL Foundation examination is one of the examinations available in the Prometric Authorized Testing Centers.

What is the difference between EXIN and ISEB?
"We were asked by one of our major clients if there was a difference - we took the short route and had the controlling body officially clear the issue, Seala said. "According to Richard Wills of the OGC, the only difference between the two is that their respective services are offered in different parts of the world."

What is ISEB?
The Information Systems Examinations Board (ISEB) is a division of the British Computer Society. ISEB was created in 1990 from the Systems Analysis Examinations Board (which was set up in 1967). ISEB administrates examinations and issues certificates in a variety of subjects in the field of information systems engineering. A list of qualifications can be obtained from ISEB.

ITIL Exam FAQ and Test-Taking Advice

As well as learn the essentials of each individual process, you will need to understand the linkages and synergies of each process. You will gain extra marks - where relevant! - for simply describing this.
Some general tips
- Use ITIL terminology throughout - but correctly!
- Answer the question that's asked. NOT the one that you think is being asked. Just because you see the phrases "Problem Management" and "benefits" doesn't always mean that's the main thrust of the answer.

Next, read the context of each question three times and ensure that you get to answering it straight away. ISEB examiners reports always make reference to the fact that a large number of students do not read the question properly.
- Avoid explaining what hasn't asked to be explained. Just because you know all there is to know about, say Change Management, is irrelevant when you have been asked to explain how Change is linked to config. Answer what's really being asked. ISEB examiners regularly highlight poor writing style and 'waffle' as being distracting. So my advice would be to keep it clear, concise and simple. Go for the marks!
- If you have pre-start reading time - use this wisely. Immediately eliminate any questions that you will truly struggle with. Select your strongest 3/4 questions first and think through the structure of your answer carefully. Save 1/2 questions that you can get away with listing things for, say the benefits of Incident Management. Saving list type questions will help you 'bag' some late marks when time's running out.

More ITIL Specific tips:-
- Answer your questions in the ITIL way - not the way you necessarily do it in real life. The examiner does not know your organisation but (s)he DOES know the syllabus for the ISEB examinations.
- Learn the benefits and advantages of each process
- Learn the disadvantages/challenges of each process
- Learn how to implement all of the processes
- Learn those generic items that are pretty much standard whichever process you implement, there is a pattern
- Learn the interface points, the outputs of one process to the inputs of another. Learn how - when implemented together - they generate further benefits for the organisation
- Learn the "desired results" that organisations/management are looking to achieve with ITIL processes
- Leave yourself some time before the end of the exam to re-read your answers - but do it from an ITIL examiners perspective
- Know the boundaries of ITIL, where ITIL effectively ends and another (e.g. COBIT, Six Sigma) begins. You don't need to know the other process in ANY detail, but simply understanding how far you can take ITIL before you need to employ the methodologies of another process is beneficial.

Running out of Time?

If you find yourself running out of time, don't panic:-
- Select the answers that score the most points!
- Use bulleted lists for maximum coverage with minimum words
- Hand your rough notes in with your answers papers - but write some "labels" on them - highlighting to the examiner that you were planning to include these points for specific answers. You may tip the balance if the examiners is thinking about giving you the benefit of the doubt for an answer

Bonus: ITIL Foundation Exam Weekend Cram Plan:

If you are a "crammer" like me, (also known as a "procrastinator") then this strategy might work for you like it did for me:

1) When you schedule your Exam (I used Sylvan Prometric), look for an exam location that is available on weekends.
2) Schedule your exam for Sunday afternoon. Yes, I know this is a major interruption to your personal life. If you don't like it, you can study the right way and avoid all the stress of last-minute cramming. I took my exam at 1pm on a Sunday.
3) Saturday morning, wake up, shower, make coffee, whatever your usual "go to work" habit is.
4) Instead of going to work, sit down at your desk or chair and read this guide, straight thru, one time. Make notes on another sheet of paper. (Science has shown that simply taking notes will improve your memory of facts, even without looking at the notes later).
5) Enjoy the rest of your Saturday as usual.
6) Sunday morning, wake up, shower, make coffee, whatever your usual "go to work" habit is.
7) Repeat step 4
8) Go take the test.

Good luck! You'll do fine!

And when you pass your exam, please send me an email with your score, and any feedback you have about this study guide.

Thanks,
Scott Braden
scott@itil-study-guide.com

