IT 495
Selected Topics in Information Technology-1

IT Service Analysis, Design, and Operation

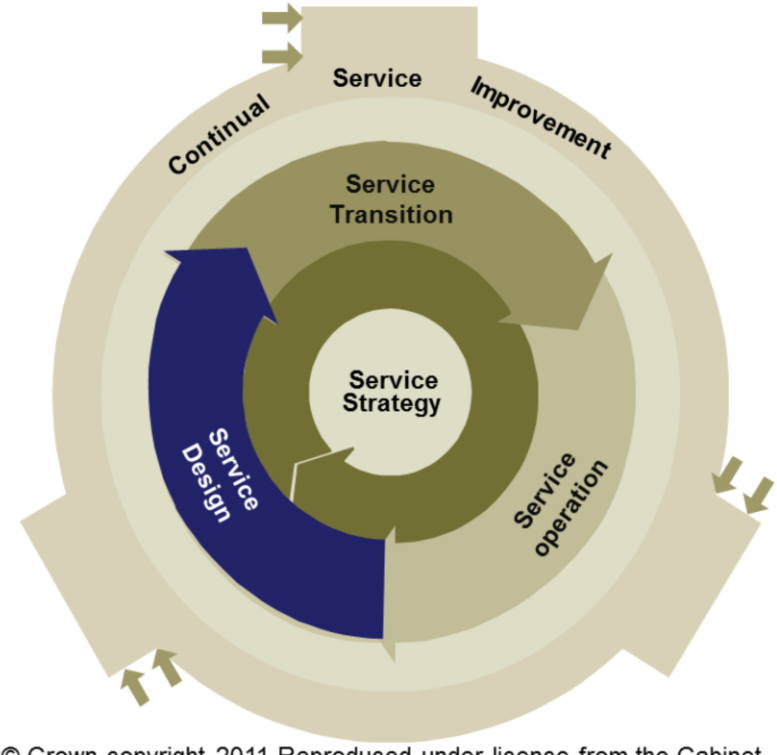
Part 2: Service Design

Haitham S. Hamza, Ph.D.
Cairo University
Spring 2023

Acknowledgment

- Slides are based on the ITIL® Foundation Course developed by the Software Engineering Competence Center (SECC).
- All ITIL® Figures are © OGC's Official Accreditor - The APM Group Limited 2008
- I have modified them and added new slides

Service Life-Cycle



Contents

Introduction

Service Design – Purpose

- Design IT services, together with the governing IT practices, processes and policies, to:
  - realize the service provider's strategy
  - facilitate the introduction of these services into supported environments in order to ensure quality service delivery, customer satisfaction and cost-effective service provision

The main purpose of the Service Design stage of the lifecycle is the design of new or changed services for introduction into the live environment. It is important that a holistic approach to all aspects of design is adopted, and that when changing or amending any of the individual elements of design all other aspects are considered. Thus when designing and developing a new application, this shouldn't be done in isolation, but should also consider the impact on the overall service, the management systems and tools (e.g. Service Portfolio and Service Catalogue), the architectures, the technology, the Service Management processes and the necessary measurements and metrics. This will ensure not only that the functional elements are addressed by the design, but also that all of the management and operational requirements are addressed as a fundamental part of the design and are not added as an afterthought.

Not every change within an IT service will require the instigation of Service Design activity. It will only be required where there is 'significant' change. Every organization must define what constitutes 'significant' so that everyone within the organization is clear as to when Service Design activity is instigated. Therefore all changes should be assessed for their impact on Service Design activities to determine whether they are significant in terms of requiring Service Design activity. This should be part of the Change Management process impact assessment

within the Service Transition service lifecycle stage.

Service Design – Objective

- Design IT services so effectively that minimal improvement during their lifecycle will be required

Continual improvement should be embedded in all service design activities to ensure that the solutions and designs become even more effective over time, and to identify changing trends in the business that may offer improvement opportunities.

Service design activities can be periodic or exception-based when they may be triggered by a specific business need or event.

Service Design – Scope

- *ITIL Service Design* provides guidance for the design of appropriate and innovative IT services to meet current and future agreed business requirements
- It describes the principles of service design and looks at identifying, defining and aligning the IT solution with the business requirement
- It also introduces the concept of the service design package and looks at selecting the appropriate service design model

ITIL Service Design provides guidance for the design of appropriate and innovative IT services to meet current and future agreed business requirements. It describes the principles of service design and looks at identifying, defining and aligning the IT solution with the business requirement. It also introduces the concept of the service design package and looks at selecting the appropriate service design model. Service Design covers the methods, practices and tools to achieve excellence in service design. It discusses the fundamentals of the design processes and attends to what are called the 'five aspects of service design'.

ITIL Service Design enforces the principle that the initial service design should be driven by a number of factors, including the functional requirements, the requirements within service level agreements (SLAs), the business benefits and the overall design constraints.

The processes considered important to successful service design are design coordination, service catalogue management, service level management, availability management, capacity management, IT service continuity management, information security management and supplier management. These processes are also active throughout the other stages of the service lifecycle. All processes within the service lifecycle must be linked closely together for managing, designing, supporting and maintaining the services, the IT infrastructure, the environment, the applications and the data. The interfaces between processes need to be clearly defined when designing a service or improving or implementing a process.

Service Design – Value to Business

- Reduce total cost of ownership (TCO)
- Improve quality of service
- Improve consistency of service
- Ease the implementation of new or changed Services
- Improve service alignment
- Improve service performance
- Improve IT governance
- Improve effectiveness of service management and IT processes
- Improve information and decision-making
- Improve alignment with customer values and strategies

Adopting and implementing standard and consistent approaches for service design will:

•**Reduce total cost of ownership (TCO)** Cost of ownership can only be minimized if all aspects of services, processes and technology are designed properly and implemented against the design.

•**Improve quality of service** Both service and operational quality will be enhanced through services that are better designed to meet the required outcomes of the customer.

•**Improve consistency of service** This will be achieved by designing services within the corporate strategy, architectures and constraints.

•**Ease the implementation of new or changed services** Integrated and full service designs and the production of comprehensive service design packages will support effective and efficient transitions.

•**Improve service alignment** Involvement of service design from the conception of the service will ensure that new or changed services match business needs, with services designed to meet service level requirements.

•**Improve service performance** Performance will be enhanced if services are designed to meet specific performance criteria and if capacity, availability, IT service continuity and financial plans are recognized and incorporated.

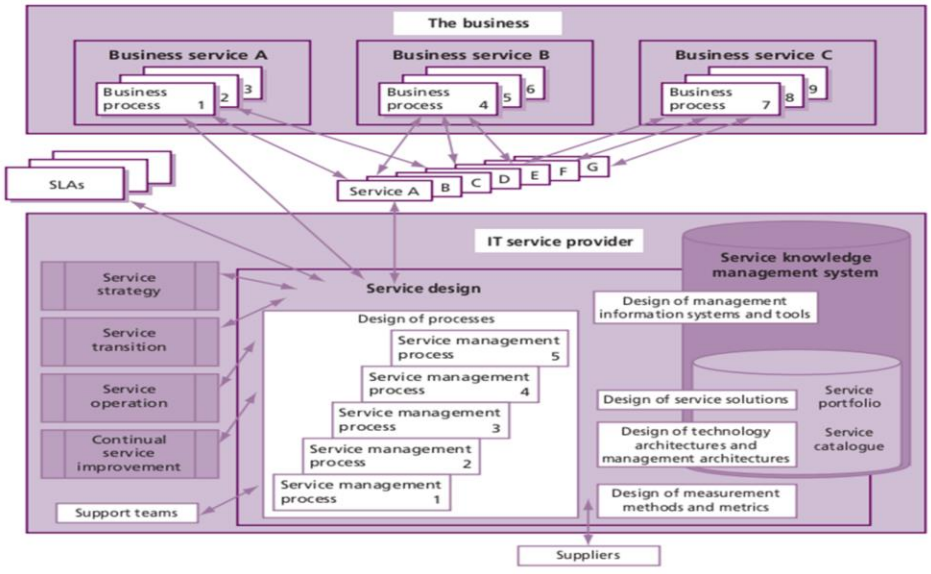
•**Improve IT governance** By building controls into designs, service design can contribute towards the effective governance of IT.

•**Improve effectiveness of service management and IT processes** Processes will be designed with optimal quality and cost effectiveness.

•**Improve information and decision-making** Comprehensive and effective measurements and metrics will enable better decision-making and continual improvement of services and service management practices throughout the service lifecycle.

•**Improve alignment with customer values and strategies** For organizations with commitments to concepts such as green IT or that establish strategies such as the use of cloud technologies, service design will ensure that all areas of services and service management are aligned with these values and strategies.

Service Design – The Big Picture



Service Design – Processes

- Design coordination
- Service catalogue management
- IT service continuity management
- Information security management
- Capacity management
- Service level management
- Availability management
- Supplier management

Key Principles, Models, and Concepts

Major Aspects of Service Design

- Service solutions for new or changed services
- Management information systems and tools, (especially the service portfolio, including the service catalogue)
- Technology architectures and management architectures
- The processes required
- Measurement methods and metrics.

A holistic approach should be adopted for all service design aspects and areas to ensure consistency and integration within all activities and processes across the entire IT technology, providing end-to-end business-related functionality and quality.

It is important that a holistic, results-driven approach to all aspects of design is adopted, and that when changing or amending any of the individual elements of design all other aspects are considered. When designing and developing a new application, this should not be done in isolation, but should also consider the impact on the overall service, the management information systems and tools (e.g. service portfolio and service catalogue), the architectures, the technology, the service management processes, and the necessary measurements and metrics. This will ensure not only that the functional elements are addressed by the design, but also that all of the management and operational requirements are addressed as a fundamental part of the design and are not added as an afterthought.

This holistic approach and the five aspects of design identified above are

important parts of the service provider's overall service management system.

There are five individual aspects of service design

•**Service solutions for new or changed services:** The requirements for new or changed services are extracted from the service portfolio. Each requirement is analysed, documented and agreed, and a solution design is produced that is then compared with the strategies and constraints from service strategy to ensure that it conforms to corporate and IT policies. The design must ensure that this new or changed service is consistent with all other services, and that all other services that interface with, underpin or depend on the new or changed service are consistent with the new service. If not, either the design of the new service or the other existing services will need to be adapted. Each individual service solution design is also considered in conjunction with each of the other four aspects of service design.

• **The management information systems and tools, especially the service portfolio:** The management information systems and tools should be reviewed to ensure they are capable of supporting the new or changed service.

•**The technology architectures and management architectures:** These are reviewed to ensure that all the technology architectures and management architectures are consistent with the new or changed service and have the capability to operate and maintain the new service. If not, then either the architectures will need to be amended or the design of the new service will need to be revised.

•**The processes required:** These are reviewed to ensure that the processes, roles, responsibilities and skills have the capability to operate, support and maintain the new or changed service. If not, the design of the new service will need to be revised or the existing process capabilities will need to be enhanced. This includes all IT

•and service management processes, not just the processes involved in the service design stage itself.

• **The measurement methods and metrics:** These are reviewed to ensure that the existing measurement methods can provide the required metrics on the new or changed service. If not, then the measurement methods will need to be enhanced or the service metrics will need to be revised.

Completion of all of the above activities during the service design stage will ensure minimal issues arising during the subsequent stages of the service lifecycle. Therefore service design must consolidate the key design issues and activities of all IT and service management processes within its own design activities, to ensure that all aspects are considered and included within all designs for new or changed services as part of everyday process operation.

Not every change within an IT service will require the instigation of the same level of service design activity. It can be argued that every change, no matter how small, needs to be designed, but the scale of the activity necessary to ensure success will vary greatly from one change type to another. Every organization must define what categories of change require what level of design activity and ensure that everyone within the organization is clear on these requirements. In other words, all changes should be assessed for their service design requirements to determine the correct service design activities to undertake in each circumstance. This should be part of the change management process impact assessment described within *ITIL Service Transition.*

Service Design Package – SDP

- The SDP is produced during the design stage, for each new service, major change to a service or removal of a service or changes to the SDP itself
- An SDP contains:
  - Requirements (business requirements, service applicability, and service contracts)
  - Service design (Service functional requirements, Service level requirements, Service and operational management requirements, Service design and topology)
  - Organizational readiness assessment
  - Service Lifecycle Plan: Service programme, Service transition plan, Service operational acceptance plan, Service acceptance criteria)
- SDP is passed from service design to service transition and details all aspects of the service and its requirements through all of the subsequent stages of its lifecycle

Requirements

•**Business requirements**: The initial agreed and documented business requirements

•**Service applicability**:defines how and where the service would be used. This could reference business, customer and user requirements for internal services

•**Service contacts**: The business and customer contacts, and other stakeholders in the service

Service design

•**Service functional requirements**: The changed functionality (utility) of the new or changed service, including its planned outcomes and deliverables, in a formally agreed statement of requirements (SoR)

•**Service level requirements**: The service level requirements (SLR), representing the desired warranty of the service for a new or changed service. Once specific service level targets have been agreed and validated, the revised or new service level agreement (SLA), including service and quality targets

•**Service and operational management requirements**: Management requirements to manage the new or changed service and its components, including all supporting services and agreements, control, operation, monitoring, measuring and reporting

•**Service design and topology**: The design, transition and subsequent implementation and operation of the service solution and its supporting components, including:

- •The service definition, service model, packaging and service options
- •All service components and infrastructure (including hardware, software, networks, environments, data, applications, technology, tools, documentation), including version numbers and relationships, preferably within the configuration management system (CMS)
- •All user, business, service, component, transition, support and operational documentation
- •Processes, procedures, measurements, metrics and reports
- •Supporting products, services, agreements and suppliers

•**Service design and topology**: The design, transition and subsequent implementation and operation of the service solution and its supporting components, including:

- •The service definition, service model, packaging and service options
- •All service components and infrastructure (including hardware, software, networks, environments, data, applications, technology, tools, documentation), including version numbers and relationships, preferably within the CMS
- •All user, business, service, component, transition, support and operational documentation
- •Processes, procedures, measurements, metrics and reports
- •Supporting products, services, agreements and suppliers

Organizational readiness assessment: 'Organizational readiness assessment' report and plan, including: business benefit, financial assessment, technical assessment, resource assessment and organizational assessment, together with details of all new skills, competences, capabilities required of the service provider organization, its suppliers, supporting services and contracts

Service lifecycle plan

•**Service programme**: An overall programme or plan covering all stages of the lifecycle of the service, including the timescales and phasing, for the transition, operation and subsequent improvement of the new service including:

- •Management, coordination and integration with any other projects, or new or changed activities, services or processes
- •Management of risks and issues
- •Scope, objectives and components of the service
- •Skills, competences, roles and responsibilities
- •Processes required
- •Interfaces and dependencies with other services
- •Management of teams, resources, tools, technology, budgets, facilities required
- •Management of suppliers and contracts
- •Progress reports, reviews and revision of the programme and plans
- •Communication plans and training plans
- •Timescales, deliverables, targets and quality targets for each stage

•**Service transition plan:** Overall transition strategy, objectives, policy, risk assessment and plans including:

- •Build policy, plans and requirements, including service and component build plans, specifications, control and environments, technology, tools, processes, methods and mechanisms, including all platforms
- •Testing policy, plans and requirements, including test environments, technology, tools, processes, methods and mechanisms
- •Testing must include:
  - •Functional testing
  - •Component testing, including all suppliers, contracts and externally provided supporting products and services
  - •User acceptance and usability testing
  - •System compatibility and integration testing
  - •Service and component performance and capacity testing
  - •Resilience and continuity testing
  - •Failure, alarm and event categorization, processing and testing
  - •Service and component, security and integrity testing
  - •Logistics, release and distribution testing
  - •Management testing, including control, monitoring, measuring and reporting, together with backup, recovery and all batch scheduling and processing
- •Deployment policy, release policy, plans and requirements, including logistics, deployment, staging, deployment environments, cultural change, organizational change, technology, tools, processes, approach, methods and mechanisms, including all platforms, knowledge, skill and competence transfer and development, supplier and contract transition, data migration and conversion

•**Service operational acceptance plan**: Overall operational strategy, objectives, policy, risk assessment and plans including:

- •Interface and dependency management and planning
- •Events, reports, service issues, including all changes, releases, resolved incidents, problems and known errors, included within the service and any errors, issues or non-conformances within the new service
- •Final service acceptance

•**Service acceptance criteria**: Development and use of service acceptance criteria for progression through each stage of the service lifecycle, including: All environments, and Guarantee and pilot criteria and periods.

Underpinning Agreements

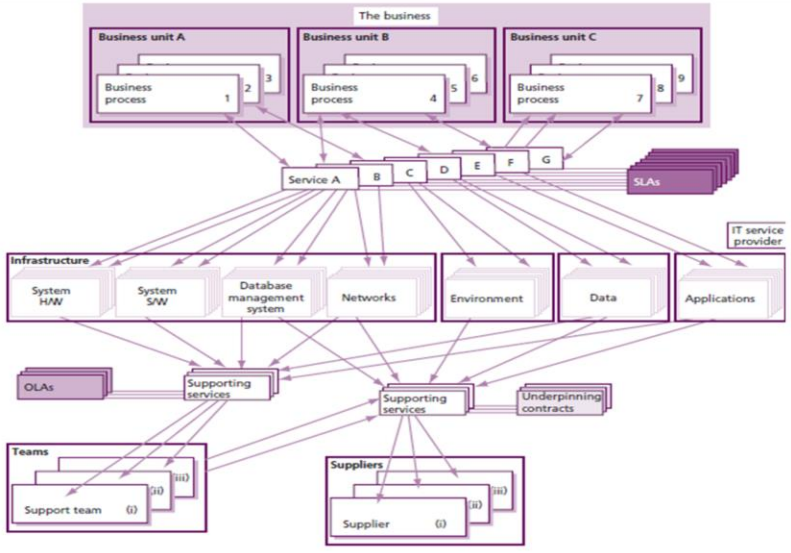
- **Underpinning agreements**: is a term used to refer to all OLAs, and contracts or other agreements that underpin the customer SLAs
- **Service Level Agreement (SLA):** a written agreement between an IT service provider and the IT customer(s), defining the key service targets and responsibilities of both parties
- **Operational Level Agreement (OLA):** an agreement between an IT service provider and another part of the same organization that assists with the provision of services
- **Underpinning Contract (UC):** an agreement between a service provider and supplier, and it typical contains:
  - Basic terms and conditions
  - Service description and scope
  - Service standards
  - Workload ranges
  - Management information
  - Responsibilities and dependencies
- **Formal contract:** agreement that provide for binding legal commitments between an IT service provider and an external supply that make a significant contribution to the delivery and development of the business

Underpinning agreements: is a term used to refer to all OLAs, and contracts or other agreements that underpin the customer SLAs.

An SLA is a written agreement between an IT service provider and the IT customer(s), defining the key service targets and responsibilities of both parties. An SLA will typically define the warranty a service is to deliver and describe the utility of the service.

An OLA is an agreement between an IT service provider and another part of the same organization that assists with the provision of services – for instance, a facilities department that maintains the air conditioning, or network support team that supports the network service. An OLA should contain targets that underpin those within an SLA to ensure that targets will not be breached by failure of the supporting activity.

SLAs, OLAs, and UCs



The nature and extent of an agreement between a service provider and supplier depends on the relationship type and an assessment of the risks involved. A comprehensive agreement minimizes the risk of disputes arising from a difference of expectations. The contents of a basic underpinning contract or service agreement are:

- **Basic terms and conditions** The term (duration) of the contract, the parties, locations, scope, definitions and commercial basis.
- **Service description and scope** The functionality of the services being provided and its extent, along with constraints on the service delivery, such as performance, availability, capacity, technical interface and security. Service functionality may be explicitly defined, or included by reference to other established documents (service catalogue).
- **Service standards** The service measures and the minimum levels that constitute acceptable performance and quality – for example, IT may have a performance requirement to respond to a request for a new desktop system in 24 hours, with acceptable service deemed to have occurred where this performance requirement is met in 95% of cases. Service levels must be realistic, measurable and aligned to the organization's business priorities and underpin the agreed targets within SLRs and SLAs.
- **Workload ranges** The volume ranges within which service standards apply, or for which particular pricing regimes apply.
- **Management information** The data that must be reported by the supplier on operational performance – take care to ensure that management information is focused on the most important or headline reporting measures on which the relationship will be assessed. KPIs related to supplier CSFs and balanced scorecards may form the core of reported performance data.
- **Responsibilities and dependencies** Description of the obligations of the organization and of the supplier, including communication, contacts and escalation.

Formal contracts are appropriate for external supply arrangements that make a significant contribution to the delivery and development of the business. Contracts provide for binding legal commitments between IT service provider and supplier, and cover the obligations each organization has to the other from the first day of the contract, often extending beyond its termination.

Sourcing Options

Sourcing structure	Description
Insourcing	This approach relies on utilizing internal organizational resources in the design, development, transition, maintenance, operation and/or support of new, changed or revised services.
Outsourcing	This approach utilizes the resources of an external organization or organizations in a formal arrangement to provide a well-defined portion of a service's design, development, maintenance, operations and/or support. This includes the consumption of services from application service providers (ASPs) described below.
Co-sourcing or multi-sourcing	Often a combination of insourcing and outsourcing, using a number of organizations working together to co-source key elements within the lifecycle. This generally involves using a number of external organizations working together to design, develop, transition, maintain, operate and/or support a portion of a service.
Partnership	Formal arrangements between two or more organizations to work together to design, develop, transition, maintain, operate and/or support IT service(s). The focus here tends to be on strategic partnerships that leverage critical expertise or market opportunities.
Business process outsourcing (BPO)	The increasing trend of relocating entire business functions using formal arrangements between organizations where one organization provides and manages the other organization's entire business process(es) or function(s) in a low-cost location. Common examples are accounting, payroll and call centre operations.

Although the readiness assessment determines the gap between the current and desired capabilities, an IT organization should not necessarily try to bridge that gap by itself. There are many different delivery strategies or models that can be used, reflecting how and to what degree the service provider will rely on suppliers. Each strategy has its own set of advantages and disadvantages, but all require some level of adaptation and customization for the situation at hand. The shown table lists the main categories of sourcing structure (delivery strategy) with a short abstract for each. Delivery practices tend to fall into one of these categories or some variant of them.

The table highlights a key point: the set of sourcing structures/delivery strategies varies widely and ranges from a relatively straightforward situation, solely managed within the boundaries of a company, all the way to a full KPO situation, or even a multi-vendor approach. This broad range of alternatives provides significant flexibility, but often with added complexity, and in some cases additional risk.

All of the above arrangements can be provided in both an offshore or onshore situation. In the onshore case, both organizations are based within the same country/continent, whereas in the offshore situation the organizations are in different countries/continents. Very complex sourcing arrangements exist within the IT industry and it is impossible to cover all combinations and their implications here.

Mergers and acquisitions can also complicate the issues. These situations occur when one company acquires or merges with another company for cash and/or equity swaps of the company's stock. Again, this occurs generally in response to industry consolidations, market expansion, or in direct response to competitive pressures. If companies that have different service delivery strategies are acquired or merge, a period of review and consolidation is often required to determine the most appropriate sourcing strategy for the newly merged organization. However, mergers and acquisitions can often provide organizations with the opportunity to consolidate the best practice from each organization, thereby improving the overall service capability and achieving synergies across the organization. Opportunities will also exist to provide improved career development options to service management personnel and to consolidate supplier contract for services.

Sourcing Options (cont.)

Sourcing structure	Description
Application service provision	Involves formal arrangements with an application service provider (ASP) organization that will provide shared computer-based services to customer organizations over a network from the service provider's premises. Applications offered in this way are also sometimes referred to as on-demand software/applications. Through ASPs, the complexities and costs of such shared software can be reduced and provided to organizations that could otherwise not justify the investment.
Knowledge process outsourcing (KPO)	KPO is a step ahead of BPO in one respect. KPO organizations provide domain-based processes and business expertise rather than just process expertise. In other words the organization is not only required to execute a process, but also to make certain low-level decisions based on knowledge of local conditions or industry specific information. For example, the outsourcing of credit risk assessment, where the outsourcing organization has historical information that they have analysed to create knowledge which in turn enables them to provide a service. For every credit card company to collect and analyse this data for themselves would not be as cost effective as using KPO.
'Cloud'	Cloud service providers offer specific pre-defined services, usually on-demand. Services are usually standard, but can be customized to a specific organization if there is enough demand for the service. Cloud services can be offered internally, but generally refer to outsourced service provision.
Multi-vendor sourcing	This type of sourcing involves sourcing different sources from different vendors, often representing different sourcing options from the above.

Service Design Processes

Service Level Management (SLM)

SLM – Purpose and Objectives

- **Purpose:** ensure that all current and planned IT services are delivered to agreed achievable targets
- **Objectives:**
  - Define, document, agree, monitor, measure, report and review the level of IT services provided and instigate corrective measures whenever appropriate
  - Relationship Management: Provide and improve the relationship and communication with the business and customers in conjunction with BRM
  - Ensure that specific and measurable targets are developed for all IT services
  - Customer Stratification: Monitor and improve customer satisfaction with the quality of service delivered
  - Expectation Management: Ensure that IT and the customers have a clear and unambiguous expectation of the level of service to be delivered
  - Proactive Improvement: Ensure proactive cost-effective continual improvements are performed to the service level

The purpose of the SLM process is to ensure that all current and planned IT services are delivered to agreed achievable targets. This is accomplished through a constant cycle of negotiating, agreeing, monitoring, reporting on and reviewing IT service targets and achievements, and through instigation of actions to correct or improve the level of service delivered.

The objectives of SLM are to:

- Define, document, agree, monitor, measure, report and review the level of IT services provided and instigate corrective measures whenever appropriate
- Provide and improve the relationship and communication with the business and customers in conjunction with business relationship management
- Ensure that specific and measurable targets are developed for all IT services
- Monitor and improve customer satisfaction with the quality of service delivered
- Ensure that IT and the customers have a clear and unambiguous expectation of the level of service to be delivered
- Ensure that even when all agreed targets met, the levels of service delivered are subject to proactive, cost-effective continual improvement.

SLM – Scope

- The SLM process should include:
  - Cooperation with the BRM process
  - Negotiation and agreement of current and future SLRs and targets
  - Documentation and management of SLAs for all operational services
  - Development and management of appropriate OLAs
  - Review of agreements and UCs with supplier management
  - Proactive prevention of service failures
  - Reporting and management of service level achievements and review of SLA breaches
  - Periodic review, renewal and/or revision of SLAs, service scope and OLAs
  - Identifying, reviewing and prioritizing improvements in the CSI register
- The SLM process does not include:
  - Negotiation and agreement of requirements for service functionality (utility), except to the degree functionality influences an SLR or target
  - Detailed attention to the activities necessary to deliver service levels
  - Negotiation of UCs and agreements (supplier management process)

SLM should represent the IT service provider to the business, and the business to the IT service provider. SLM needs to manage the expectation and perception of the business, customers and users and ensure that the quality (warranty) of service delivered by the service provider is matched to those expectations and needs.

The SLM process should include:

•Cooperation with the BRM process: this includes development of relationships with the business as needed to achieve the SLM process objectives

•Negotiation and agreement of future service level requirements and targets, and the documentation and management of SLRs for all proposed new or changed services

•Negotiation and agreement of current service level requirements and targets, and the documentation and management of SLAs for all operational services

•Development and management of appropriate OLAs to ensure that targets are aligned with SLA targets

•Review of all supplier agreements and underpinning contracts with supplier management to ensure that targets are aligned with SLA targets

•Proactive prevention of service failures, reduction of service risks and improvement in the quality of service, in conjunction with all other processes

•Reporting and management of all service level achievements and review of all SLA breaches

•Periodic review, renewal and/or revision of SLAs, service scope and OLAs as appropriate

•Identifying improvement opportunities for inclusion in the CSI register

•Reviewing and prioritizing improvements in the CSI register

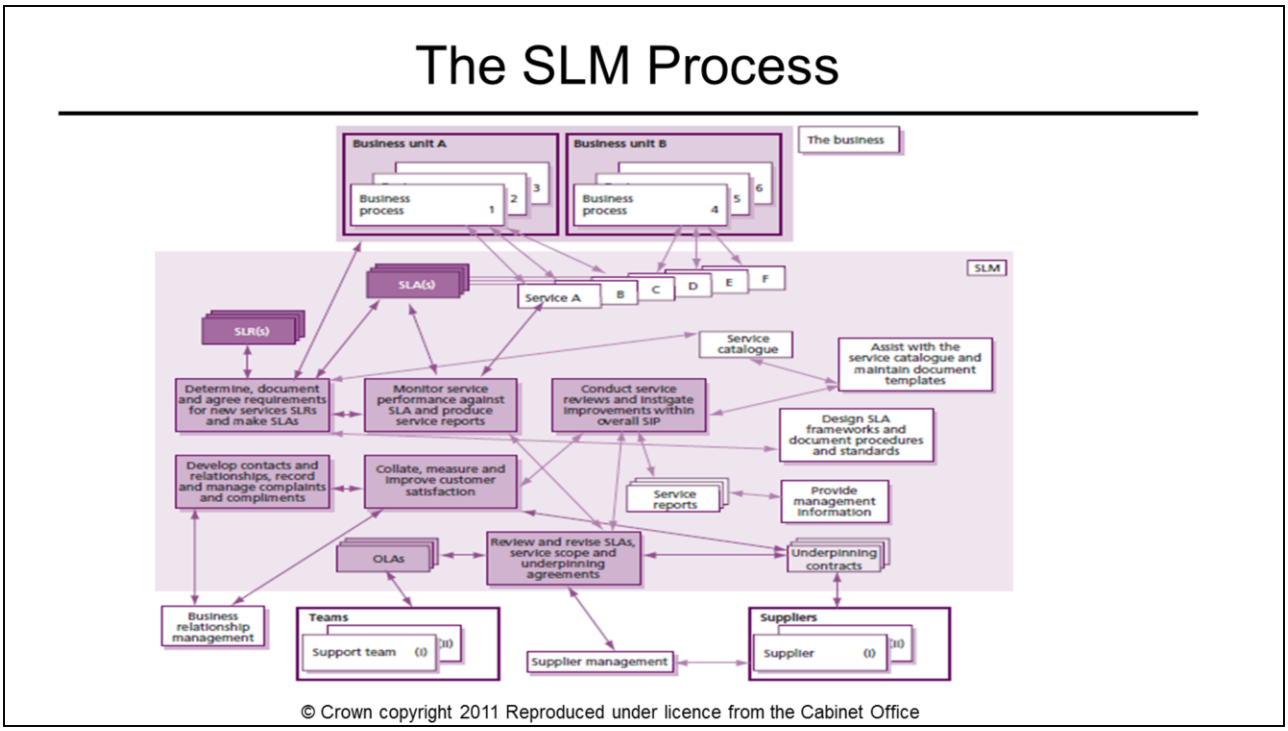
•Instigating and coordinating SIPs for the management, planning and implementation of service and process improvements.

The SLM process does not include:

•Negotiation and agreement of requirements for service functionality (utility), except to the degree functionality influences a service level requirement or target. SLAs typically describe key elements of the service's utility as part of the service description, but SLM activity does not include agreeing what the utility will be.

•Detailed attention to the activities necessary to deliver service levels that are accounted for in other processes such as availability management and capacity management.

•Negotiation of underpinning supplier contracts and agreements. This is part of the supplier management process to which SLM provides critical input and consultation.



The main activities of SLM shown in the figure should be implemented as one integrated SLM process that can be consistently applied to all areas of the businesses and to all customers:

Designing SLA frameworks: Using the service catalogue as an aid, SLM must design the most appropriate SLA structure to ensure that all services and all customers are covered in a manner best suited to the organization's needs.

Determining, documenting and agreeing requirements for new services and producing SLRs: This is one of the earliest activities within the service design stage of the service lifecycle. Once the service catalogue has been produced and the SLA structure has been agreed, the first SLRs must be drafted. An SLR is a customer requirement for an aspect of an IT service. SLRs are based on business objectives and are used to negotiate agreed service level targets. SLRs relate primarily to the warranty of the service: What levels of service are required by the customer in order for them to be able to receive the value of the utility of the service? How available does the service need to be? How secure? How quickly must it be restored if it should fail?

Negotiating, documenting and agreeing SLAs for operational services: Before a new or changed service is accepted into live operation, an SLA should be agreed, detailing the service level targets to be achieved and specifying the responsibilities of both the IT service provider and the customer. For a new service, the targets in the SLA are likely to originate from SLRs developed early in the service design stage. For changes to existing services, targets may also be defined in this way – as part of SLR development, particularly if the change to the service is significant, or the new targets may simply be refinements to targets in an existing SLA. There may be a temptation to agree to targets that cannot be adequately measured, but only measurable targets should be included in the SLA.

Monitoring service performance against SLA: Nothing should be included in an SLA unless it can be effectively monitored and measured at a commonly agreed point. Inclusion of items that cannot be effectively monitored almost always results in disputes and eventual loss of faith in the SLM process. Many organizations have discovered this the hard way and as a result have absorbed heavy costs, both in a financial sense as well as in terms of negative impacts on their credibility.

Producing service reports: Immediately after the SLA is agreed and accepted, monitoring must be instigated, and service achievement reports must be produced. Operational reports must be produced frequently (weekly or perhaps even more frequently) and, where possible, exception reports should be produced whenever an SLA has been broken (or threatened).

Conducting service reviews and instigating improvements within an overall service improvement plan: Review meetings must be held on a regular basis with customers (or their representatives) to review the service achievement and to preview any issues for the coming period.

Collating, measuring and improving customer satisfaction: There are a number of important 'soft' issues that cannot be monitored by mechanistic or procedural means, such as customers' overall feelings. For example, even when there have been a number of reported service failures, customers may still have a positive feeling because they are satisfied that appropriate actions are being taken to improve things. The opposite is also true. The BRM process is concerned with overall customer satisfaction with all aspects of service provision. SLM activity is focused around customer satisfaction relating specifically to the levels of service provided – essentially the warranty aspect of the service.

Reviewing and revising SLAs, service scope and underpinning agreements: All SLAs and the agreements that underpin them, including OLAs, and underpinning contracts, must be kept up to date. They should be brought under the control of change management and service asset and configuration management. They should also be reviewed periodically, at least annually, to ensure that they are still current and comprehensive, and are still aligned to business needs and strategy. In the case of contracts or agreements with suppliers, the supplier management process is responsible for this activity with the active consultation of SLM.

Reviewing and revising OLAs, underpinning agreements and service scope: IT service providers are dependent on their own internal support teams as well as on external partners or suppliers. The service provider cannot commit to meeting SLA targets unless their own support teams' and suppliers' performances underpin these targets. Underpinning contracts with external suppliers are mandatory, but many organizations have also identified the benefits of having simple agreements with internal support groups, usually referred to as OLAs.

Developing contacts and relationships: It is very important that the service provider develops trust and respect with the business, especially with the key business contacts. The SLM process contributes to this trust and respect by working closely with key business contacts throughout SLM activity to ensure that service levels are agreed and delivered. As customers experience the results of successful SLM, their trust in and respect for the service provider increase. The BRM process ensures that the right customer representatives participate in SLM and contributes extensively to the understanding of business needs and priorities that must inform all SLM activity.

Handling complaints and compliments: The SLM process should also include activities and procedures for the logging and management of complaints and compliments that relate to service levels. This work represents a significant contribution to the overall customer satisfaction work being done in the BRM process. SLM may also be actively involved in the management of service level complaints and compliments originating from users, as well as from customers, as user perceptions will add an important perspective.

Service Level Requirements (SLRs)

- SLR: a customer requirement for an aspect of an IT service
- SLRs are based on business objectives and are used to negotiate agreed service level targets.
- SLRs relate primarily to the warranty of the service:
  - What levels of service are required by the customer in order for them to be able to receive the value of the utility of the service?
  - How available does the service need to be?
  - How secure?
  - How quickly must it be restored if it should fail?

It is important to establish procedures for agreeing service level requirements for new services being developed or procured. The SLRs should be an integral part of the overall service design criteria which also include the functional or 'utility' specifications. SLRs should, from the very start, form part of the testing/trialling criteria as the service progresses through the stages of design and development or procurement.

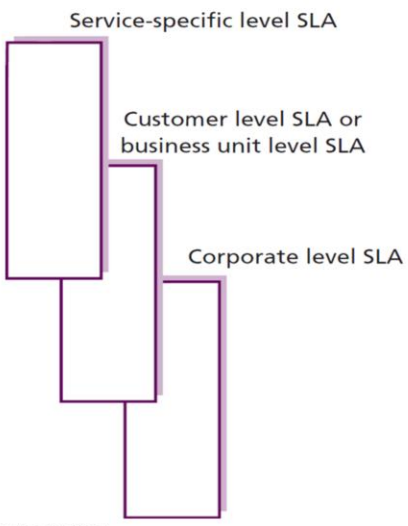
It is advisable to involve customers from the outset, but rather than approaching customers with a 'blank page', it may be better to produce an outline SLR draft with potential performance targets and management and operational requirements, as a starting point for more detailed and in-depth discussion.

In order to ensure a focus on required business outcomes, it is important to maintain clarity in the difference between the SLR and the specific service level target(s) associated with the achievement of the SLR. For example, an SLR relating to performance might be expressed by the customer as 'fast enough to support the anticipated volume of orders to be placed during peak activity periods without failures or delays', while the service level target negotiated to support this requirement will define specific, measurable response times and the conditions under which the target will be deemed to have been breached.

Determining the high-level, business objective-oriented SLRs will typically begin during the service strategy stage as part of defining the information needed to make the strategic decision to charter and fund the service. The service portfolio management and business relationship management processes are very involved in this high-level warranty determination. Once the service charter has been issued, the SLM process continues the work of determining any additional SLRs and refining all SLRs to the detailed, measurable level needed for design of the service solution.

SLA Frameworks

- Service-based SLA: an SLA covers one service, for all the customers of that service
  - Example: an SLA for an organization's email service
- Customer-based SLA: an agreement with an individual customer group, covering all the services they use
  - Example: agreements with an organization's finance department covering the payroll system and the billing system
- Multi-level SLAs: For example, a three-layer structure:
  - Corporate level
  - Customer level
  - Service level



Service-based SLA: an SLA covers one service, for all the customers of that service – for example, an SLA may be established for an organization's email service – covering all the customers of that service. This may appear fairly straightforward. However, difficulties may arise if the specific requirements of different customers vary for the same service, or if characteristics of the infrastructure mean that different service levels are inevitable (e.g. head office staff may be connected via a high-speed LAN, while local offices may have to use a lower-speed WAN line). In such cases, separate targets may be needed within the one agreement. Difficulties may also arise in determining who should be the signatories to such an agreement. However, where common levels of service are provided across all areas of the business (e.g., email or telephony), the service-based SLA can be an efficient approach to use. Multiple classes of service (e.g., gold, silver and bronze) can also be used to increase the effectiveness of service-based SLAs.

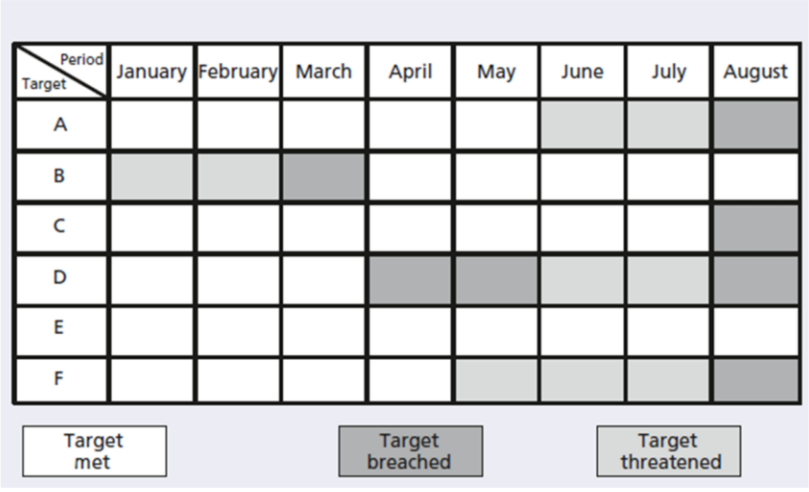
Customer-based SLA: an agreement with an individual customer group, covering all the services they use. For example, agreements may be reached with an organization's finance department covering, say, the finance system, the accounting system, the payroll system, the billing system, the procurement system, and any other IT systems that they use. Customers often prefer such an agreement, as all of their requirements are covered in a single document. Only one signatory is normally required, which simplifies this issue.

Multi-level SLAs: Some organizations have chosen to adopt a multi-level SLA structure. For example, a three-layer structure as follows:

- **Corporate level**: covers all the generic SLM issues appropriate to every customer throughout the organization. These issues are likely to be less volatile, so updates are less frequently required.
- **Customer level**: covers all SLM issues relevant to the particular customer group or business unit, regardless of the service being used.
- **Service level:** covers all SLM issues relevant to the specific service, in relation to a specific customer group (one for each service covered by the SLA).

Such a structure allows SLAs to be kept to a manageable size, avoids unnecessary duplication, and reduces the need for frequent updates. However, it does mean that extra effort is required to maintain the necessary relationships and links within the service catalogue and the CMS.

SLA Monitoring



Immediately after the SLA is agreed and accepted, monitoring must be instigated, and service achievement reports must be produced. Operational reports must be produced frequently (weekly or even more frequently) and, where possible, exception reports should be produced whenever an SLA has been broken (or threatened, if appropriate thresholds have been set to give an 'early warning').

The shown figure gives an example of an SLA monitoring chart that provides a visual representation of an organization's ability to meet defined targets over a period of months.

The periodic reports should incorporate details of performance against all SLA targets, together with details of any trends or specific actions being undertaken to improve service quality. A useful technique is to include a SLA monitoring (SLAM) chart at the front of a service report to give an 'at-a-glance' overview of how achievements have measured up against targets. These are most effective if colour coded (red, amber, green, and sometimes referred to as RAG charts as a result). Other interim reports may be required by IT management for OLA or internal performance reviews and/or supplier management. This is likely to be an evolving process – a first effort is unlikely to be the final outcome.

Service Reports

- The SLA reporting mechanisms, intervals and report formats must be defined and agreed with the customers
- The resources required to produce and verify reports can be extremely time-consuming, thus, SLM should identify the specific reporting needs and automate production of these reports whenever possible
- It is essential that accurate information from all areas and all processes

Periodic reports must be produced and circulated to customers (or their representatives) and appropriate IT managers a few days in advance of service level reviews, so that any queries or disagreements can be resolved ahead of the review meeting. The meeting is then not diverted by such issues.

The SLA reporting mechanisms, intervals and report formats must be defined and agreed with the customers. The frequency and format of service review meetings must also be agreed with the customers. Regular intervals are recommended, with periodic reports synchronized with the reviewing cycle.

The resources required to produce and verify reports should not be underestimated. It can be extremely time-consuming, and if reports do not reflect the customer's own perception of service quality accurately, they can make the situation worse. It is essential that accurate information from all areas and all processes (e.g. incident management, problem management, availability management, capacity management, change management, and service asset and configuration management) is analysed and collated into a concise and comprehensive report on service performance, as measured against agreed business targets.

SLM should identify the specific reporting needs and automate production of these reports, as far as possible. The extent, accuracy and ease with which automated reports can be produced should form part of the selection criteria for integrated support tools. These service reports should not only include details of current performance against targets, but should also provide historic information on past performance and trends, so that the impact of improvement actions can be measured and predicted.

Service Review

- Review meetings must be held on a regular basis (monthly or quarterly) with customers (or their representatives) to review the service
- Particular attention should be focused on each breach of service level to determine what caused the loss of service and what can be done to prevent any recurrence:
  - Review, renegotiate, and agree different service targets if current service level was, or has become, unachievable
  - Review the UCs or OLA if the service break has been caused by a failure of a third party or internal support group
- The review process may result in instigating improvements via a service improvement plan (SIP)
- **Service Improvement Plan (SIP):** an overall programme or plan of prioritized improvement actions, encompassing appropriate services and processes, together with associated impacts and risks

Review meetings must be held on a regular basis with customers (or their representatives) to review the service achievement in the last period and to preview any issues for the coming period. It is normal to hold such meetings monthly or, as a minimum, quarterly.

Actions should be assigned to the customer and provider as appropriate to improve weak areas where targets are not being met. All actions must be minuted, and progress should be reviewed at the next meeting to ensure that action items are being followed up and properly implemented.

Particular attention should be focused on each breach of service level to determine exactly what caused the loss of service and what can be done to prevent any recurrence. If it is decided that the service level was, or has become, unachievable, it may be necessary to review, renegotiate, review and agree different service targets. If the service break has been caused by a failure of a third party or internal support group, it may also be necessary to review the underpinning contract or OLA. Analysis of the cost and impact of service breaches provides valuable input and justification of SIP activities and actions. The constant need for improvement needs to be balanced and focused on those areas most likely to give the greatest business benefit. SIP activity is essentially part of the CSI stage of the lifecycle.

Reports should also be produced on the progress and success of the SIP, such as the number of SIP actions that were completed and the number of actions that delivered their expected benefit.

Service Design Processes

Service Catalogue Management (SCM)

SCM – Purpose and Objectives

- **Purpose:**
  - provide and maintain a single source of consistent information on all operational services and those being prepared to be run operationally
  - ensure that this information is widely available to those who are authorized to access it.
- **Objectives:**
  - Manage the information contained within the service catalogue
  - Ensure that the service catalogue:
    - Is accurate and reflects the current details
    - is made available to those approved to access it
    - supports the evolving needs of all other service management processes

The service catalogue is one of the most valuable elements of a comprehensive approach to service provision and, as such, it should be given proper care and attention. The service catalogue management process provides the means of devoting that care and attention in a consistent fashion, ensuring that the organization accrues all of the potential benefits of a service catalogue in the most efficient manner possible.

The purpose of the service catalogue management process is to provide and maintain a single source of consistent information on all operational services and those being prepared to be run operationally, and to ensure that it is widely available to those who are authorized to access it.

The objectives of the service catalogue management process are to:

•Manage the information contained within the service catalogue

•Ensure that the service catalogue is accurate and reflects the current details, status, interfaces and dependencies of all services that are being run, or being prepared to run, in the live environment, according to the defined policies

•Ensure that the service catalogue is made available to those approved to access it in a manner that supports their effective and efficient use of service catalogue information

•Ensure that the service catalogue supports the evolving needs of all other service management processes for service catalogue information, including all interface and dependency information.

SCM – Scope

- The SCM process covers:
  - Contribution to the definition of services and service packages
  - Development and maintenance of service and service package descriptions appropriate for the service catalogue
  - Production and maintenance of an accurate service catalogue
  - Interfaces, dependencies and consistency between the service catalogue and the overall service portfolio
  - Interfaces and dependencies all services and:
    - supporting services within the service catalogue and the CMS
    - supporting components and configuration items (CIs) within the service catalogue and the CMS

The scope of the service catalogue management process is to provide and maintain accurate information on all services that are being transitioned or have been transitioned to the live environment. The services presented in the service catalogue may be listed individually or, more typically, some or all of the services may be presented in the form of service packages.

The service catalogue management process covers:

- Contribution to the definition of services and service packages
- Development and maintenance of service and service package descriptions appropriate for the service catalogue
- Production and maintenance of an accurate service catalogue
- Interfaces, dependencies and consistency between the service catalogue and the overall service portfolio
- Interfaces and dependencies between all services and supporting services within the service catalogue and the CMS
- Interfaces and dependencies between all services, and supporting components and configuration items (CIs) within the service catalogue and the CMS.

The service catalogue management process does not include:

- Detailed attention to the capturing, maintenance and use of service asset and configuration data as performed through the service asset and configuration management process (*ITIL Service Transition*)
- Detailed attention to the capturing, maintenance and fulfilment of service requests as performed through request fulfilment (*ITIL Service Operation*).

Service Design Processes

Availability Management

Availability Management – Purpose

- Ensures that the level of availability delivered in all IT services meets the agreed availability needs and/or service level targets in a cost-effective and timely manner.
- Availability management is concerned with meeting both the current and future availability needs of the business.

Availability management defines, analyses, plans, measures and improves all aspects of the availability of IT services, ensuring that all IT infrastructure, processes, tools, roles etc. are appropriate for the agreed availability service level targets. It provides a point of focus and management for all availability-related issues, relating to both services and resources, ensuring that availability targets in all areas are measured and achieved.

Availability Management – Objectives

- Produce and maintain an appropriate and up-to-date availability plan
- Provide advice and guidance to all other areas of the business and IT on all availability-related issues
- Ensure that service availability achievements meet all their agreed targets
- Assist with the diagnosis/resolution of availability-related incidents and problems
- Assess the impact of all changes on the availability
- Ensure that proactive measures to improve the availability of services are implemented

The objectives of availability management are to:

- Produce and maintain an appropriate and up-to-date availability plan that reflects the current and future needs of the business
- Provide advice and guidance to all other areas of the business and IT on all availability-related issues
- Ensure that service availability achievements meet all their agreed targets by managing services and resources-related availability performance
- Assist with the diagnosis and resolution of availability-related incidents and problems
- Assess the impact of all changes on the availability plan and the availability of all services and resources
- Ensure that proactive measures to improve the availability of services are implemented wherever it is cost-justifiable to do so.

Availability management should ensure the agreed level of availability is provided. The measurement and monitoring of IT availability is a key activity to ensure availability levels are being met consistently. Availability management should look to continually optimize and proactively improve the availability of the IT infrastructure, the services and the supporting organization, in order to provide cost-effective availability improvements that can deliver business and customer benefits.

Availability Management – Scope

- Availability management process covers the design, implementation, measurement, management and improvement of IT service and component availability
- The availability management process includes two key elements:
  - **Reactive activities**: monitoring, measuring, analysis and management of all events, incidents and problems involving unavailability
  - **Proactive activities** : proactive planning, design and improvement of availability
- The availability management process should include:
  - Monitoring of availability, reliability and maintainability of IT services/components
  - Calculations for all availability measurements, metrics and reporting
  - Actively participating in risk assessment and management activities
  - Collecting measurements and the analysis and production of availability reports
  - Producing an availability plan
  - Maintaining a schedule of tests for all resilience and fail-over components and mechanisms
  - Assisting with the identification/resolution of incidents/problems related to unavailability
  - Proactively improving service or component availability wherever it is cost-justifiable
- The availability management process does not include business continuity management (BCM)

Availability management commences as soon as the availability requirements for an IT service are clear enough to be articulated. It is an ongoing process, finishing only when the IT service is decommissioned or retired.

Availability management needs to understand the service and component availability requirements from the business perspective in terms of the:

- Current business processes, their operation and requirements
- Future business plans and requirements
- Service targets and the current IT service operation and delivery
- IT infrastructure, data, applications and environment and their performance
- Business impacts and priorities in relation to the services and their usage.

Understanding all of this will enable availability management to ensure that all the services and components are designed and delivered to meet their targets in terms of agreed business needs. The availability management process should:

- Be Applied to all operational services and technology, particularly those covered by SLAs. It can also be applied to those IT services deemed to be business-critical, regardless of whether formal SLAs exist
- Be Applied to all new IT services and for existing services where SLRs or SLAs have been established
- Be Applied to all supporting services and the partners and suppliers (both internal and external) that form the IT support organization as a precursor to the creation of formal agreements
- Consider all aspects of the IT services and components and supporting organizations that may impact availability, including training, skills, process effectiveness, procedures and tools.

The availability management process does not include business continuity management (BCM) and the resumption of business processing after a major disaster. The support of BCM is included within ITSCM. However, availability management does provide key inputs to ITSCM, and the two processes have a close relationship, particularly in the assessment and management of risks and in the implementation of risk reduction and resilience measures.

Service and Component Availability

- Availability management is completed at two inter-connected levels:
  - **Service availability**: involves all aspects of service availability and unavailability and the impact of component availability, or the potential impact of component unavailability on service availability.
  - **Component availability**: involves all aspects of component availability and unavailability.

Elements of Availability Management

- Purpose: ensure that all current and planned IT services are delivered to agreed achievable targets

- Objectives:
  - Define, document, agree, monitor, measure, report and review the level of IT services provided and instigate corrective measures whenever appropriate
  - Relationship Management: Provide and improve the relationship and communication with the business and customers in conjunction with BRM
  - Ensure that specific and measurable targets are developed for all IT services
  - Customer Stratification: Monitor and improve customer satisfaction with the quality of service delivered
  - Expectation Management: Ensure that IT and the customers have a clear and unambiguous expectation of the level of service to be delivered
  - Proactive Improvement: Ensure proactive cost-effective continual improvements are performed to the service level

Availability

- Availability is the ability of a service, component or CI to perform its agreed function when required

$$\text{Availability (\%)} = \frac{\text{Agreed service time (AST)} - \text{downtime}}{\text{AST}} \times 100$$

- Note that down time should only be included in the following calculation when it occurs within the agreed service time (AST)
- However, total down time should also be recorded and reported.

Reliability

- Reliability is a measure of how long a service, component or CI can perform its agreed function without interruption

$$\text{Reliability (MTBSI in hours)} = \frac{\text{Available time in hours}}{\text{Number of breaks}}$$

$$\text{Reliability (MTBF in hours)} = \frac{\text{Available time in hours} - \text{Total downtime in hours}}{\text{Number of breaks}}$$

MTBSI: mean time between service incidents **MTBF:** mean time between failures

- The reliability of the service can be improved by:
  - increasing the reliability of individual components
  - increasing the **resilience** of the service to individual component failure (i.e. increasing the component redundancy, e.g., by using load-balancing techniques)

Maintainability

- Maintainability is a measure of how quickly and effectively a service, component or CI can be restored to normal working after a failure

$$\text{Maintainability (MTRS in hours)} = \frac{\text{Total downtime in hours}}{\text{Number of service breaks}}$$

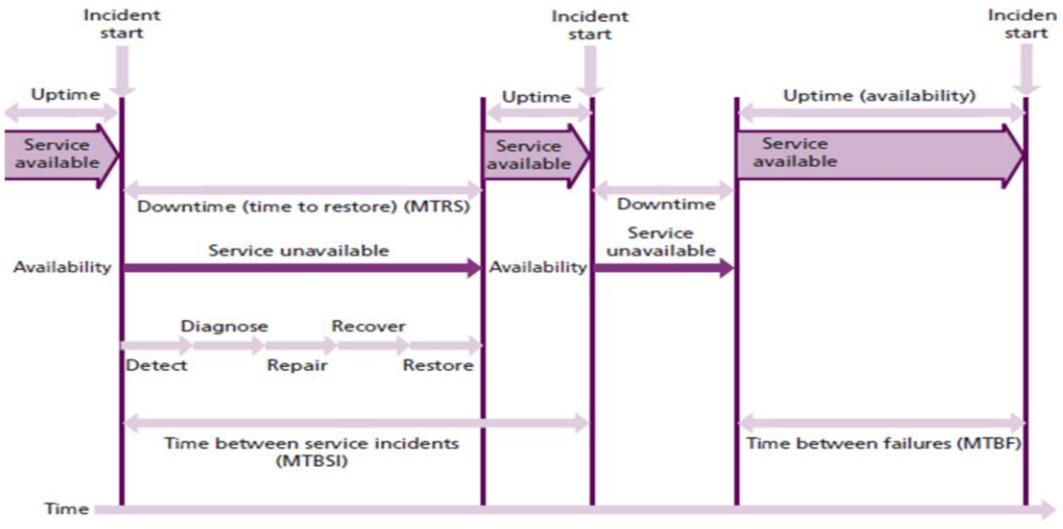
MTRS: mean time to restore service (MTRS)

MTRS should be used to avoid the ambiguity of the more common industry term mean time to repair (MTTR), which in some definitions includes only repair time, but in others includes recovery time.

The down time in MTRS covers all the contributory factors that make the service, component or CI unavailable:

- Time to record
- Time to respond
- Time to resolve
- Time to physically repair or replace
- Time to recover.

Availability and Incident Lifecycle



Serviceability

- Serviceability is the ability of a third-party supplier to meet the terms of its contract.
- This contract will include agreed levels of availability, reliability and/or maintainability for a supporting service or component

Example

A 24 × 7 service has been running for a period of **5,020** hours with only **two** breaks, one of **six hours** and one of **14 hours**, compute the availability, reliability and maintainability of this service.

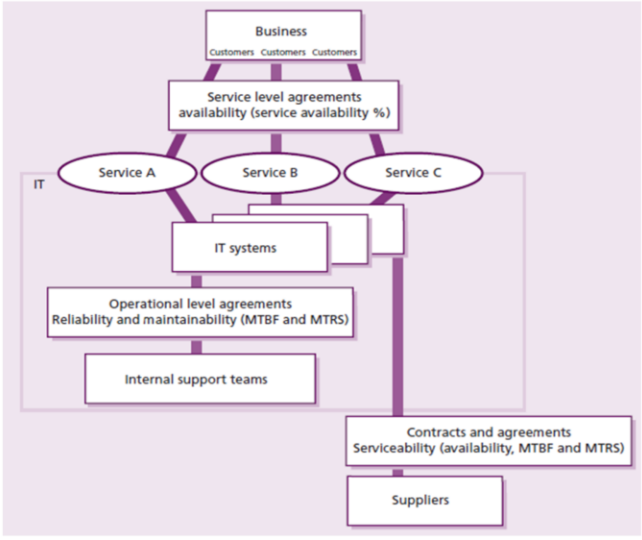
Availability = (5,020–(6+14))/5,020 × 100 = **99.60%**

Reliability (MTBSI)= 5,020/2 = **2,510 hours**

Reliability (MTBF)= 5,020–(6+14)/2 = **2,500 hours**

Maintainability (MTRS)= (6+14)/2 = **10 hours**

Availability Terms and Measurements



Although the principal service target contained within SLAs for customers and the business is availability, some customers also require reliability and maintainability targets to be included in the SLA as well. Where these are included they should relate to end-to-end service reliability and maintainability, whereas the reliability and maintainability targets contained in OLAs and contracts relate to component and supporting service targets and can often include availability targets relating to the relevant components or supporting services.

Vital Business Functions (VBF)

- An IT service may support a number of business functions that are less critical
- **Vital business function** (VBF) reflect the part of a business process that is critical to the success of the business
- This distinction should influence availability design and associated costs

The term vital business function (VBF) is used to reflect the part of a business process that is critical to the success of the business. An IT service may support a number of business functions that are less critical.

For example, an automated teller machine (ATM) or cash dispenser service VBF would be the dispensing of cash. However, the ability to obtain a statement from an ATM may not be considered as vital. This distinction is important and should influence availability design and associated costs.

For all services, whether VBFs or not, the availability requirements should be determined by the business and not by IT. The initial availability targets are often set at too high a level, and this leads to either over-priced services or an iterative discussion between the service provider and the business to agree an appropriate compromise between the service availability and the cost of the service and its supporting technology.

Service Design for VBFs

- **High availability**: minimizing or masking the effects of IT component failure to the users of a service
- **Fault tolerance:** operating correctly after failure of a component part
- **Continuous operation**: eliminating planned downtime of an IT service
- **Continuous availability**: achieving 100% availability

The more vital the business function generally, the greater the level of resilience and availability that needs to be incorporated into the design required in the supporting IT services.

Certain VBFs may need special designs, which are now being used as a matter of course within service design plans, incorporating:

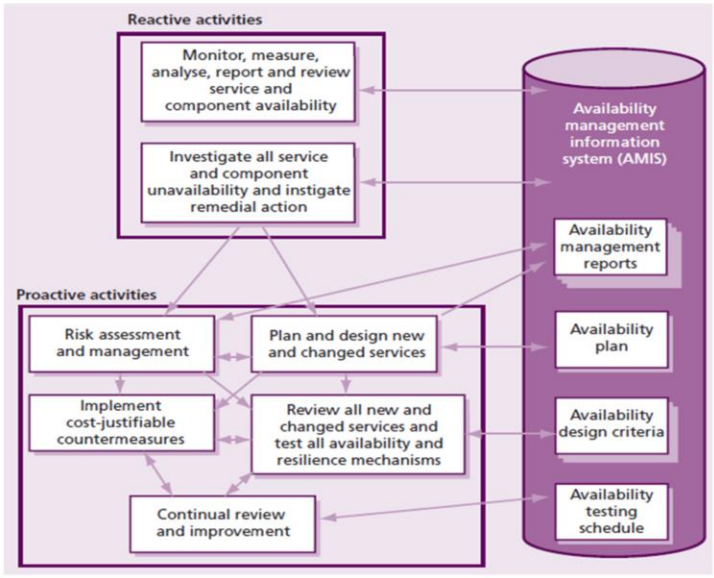
•**High availability** A characteristic of the IT service that minimizes or masks the effects of IT component failure to the users of a service.

•**Fault tolerance** The ability of an IT service, component or CI to continue to operate correctly after failure of a component part.

•**Continuous operation** An approach or design to eliminate planned downtime of an IT service. Note that individual components or CIs may be down even though the IT service remains available.

•**Continuous availability** An approach or design to achieve 100% availability. A continuously available IT service has no planned or unplanned downtime.

Availability Management Process



Reactive activities

The reactive aspect of availability management involves work to ensure that current operational services and components deliver the agreed levels of availability and to respond appropriately when they do not.

The reactive activities include:

- Monitoring, measuring, analysing, reporting and reviewing service and component availability
- Investigating all service and component unavailability and instigating remedial action. This includes looking at events, incidents and problems involving unavailability.

These activities are primarily conducted within the service operation stage of the service lifecycle and are linked into the monitoring and control activities and incident management processes.

Proactive activities

The proactive activities of availability management involve the work necessary to ensure that new or changed services can and will deliver the agreed levels of availability and that appropriate measurements are in place to support this work. They include producing recommendations, plans and documents on design guidelines and criteria for new and changed services, and the continual improvement of service and reduction of risk in existing services wherever it can be cost-justified. These are key aspects to be considered within service design activities.

Proactive activities include:

• Planning and designing new or changed services:

- •Determining the VBFs, in conjunction with the business and ITSCM
- •Determining the availability requirements from the business for a new or enhanced IT service and formulating the availability and recovery design criteria for the supporting IT components
- •Defining the targets for availability, reliability and maintainability for the IT infrastructure components that underpin the IT service to enable these to be documented and agreed within SLAs, OLAs and contracts
- •Performing risk assessment and management activities to ensure the prevention and/or recovery from service and component unavailability
- •Designing the IT services to meet the availability and recovery design criteria and associated agreed service levels
- •Establishing measures and reporting of availability, reliability and maintainability that reflect the business, user and IT support organization perspectives

•Risk assessment and management:

- •Determining the impact arising from IT service and component failure in conjunction with ITSCM and, where appropriate, reviewing the availability design criteria to provide additional resilience to prevent or minimize impact to the business

•Implementing cost-justifiable counter-measures, including risk reduction and recovery mechanisms

•Reviewing all new and changed services and test all availability and resilience mechanisms

•Continual reviewing and improvement:

- •Producing and maintaining an availability plan that prioritizes and plans IT availability improvements

Service Design Processes

Information Security Management (ISM)

ISM – Purpose and Objective

- **Purpose:** align IT security with business security and ensure that the confidentiality, integrity and availability of the organization's assets, information, data and IT services always matches the agreed needs of the business
- **Objective:** protect the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of confidentiality, integrity and availability

For most organizations, the security objective is met when:

- Information is observed by or disclosed to only those who have a right to know (confidentiality)
- Information is complete, accurate and protected against unauthorized modification (integrity)
- Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures (availability)
- Business transactions, as well as information exchanges between enterprises, or with partners, can be trusted (authenticity and non-repudiation).

ISM – Scope

- Production, maintenance, distribution and enforcement of an information security policy
- Understanding the agreed current and future security requirements
- Implementation and documentation of security controls
- Management of:
  - suppliers and contracts regarding access to systems and services (in conjunction with supplier management)
  - security breaches, incidents and problems
- Proactive improvement of security controls and security risk management
- Integration of security aspects within all other ITSM processes

ISM process should be the focal point for all IT security issues, and must ensure that an information security policy is produced, maintained and enforced that covers the use and misuse of all IT systems and services. Information security management needs to understand the total IT and business security environment, including the:

- Business security policy and plans
- Current business operation and its security requirements
- Future business plans and requirements
- Legislative and regulatory requirements
- Obligations and responsibilities with regard to security contained within SLAs
- The business and IT risks and their management.

Understanding all of this will enable information security management to ensure that all the current and future security aspects and risks of the business are cost-effectively managed. Prioritization of confidentiality, integrity and availability must be considered in the context of business and business processes. The primary guide to defining what must be protected and the level of protection has to come from the business. The information security management process should include:

- The production, maintenance, distribution and enforcement of an information security policy and supporting security policies
- Understanding the agreed current and future security requirements of the business and the existing business security policy and plans
- Implementation of a set of security controls that support the information security policy and manage risks associated with access to services, information and systems
- Documentation of all security controls, together with the operation and maintenance of the controls and their associated risks
- Management of suppliers and contracts regarding access to systems and services, in conjunction with supplier management
- Management of all security breaches, incidents and problems associated with all systems and services
- The proactive improvement of security controls, and security risk management and the reduction of security risks
- Integration of security aspects within all other ITSM processes.

To achieve effective information security governance, management must establish and maintain an information security management system (ISMS) to guide the development and management of a comprehensive information security programme

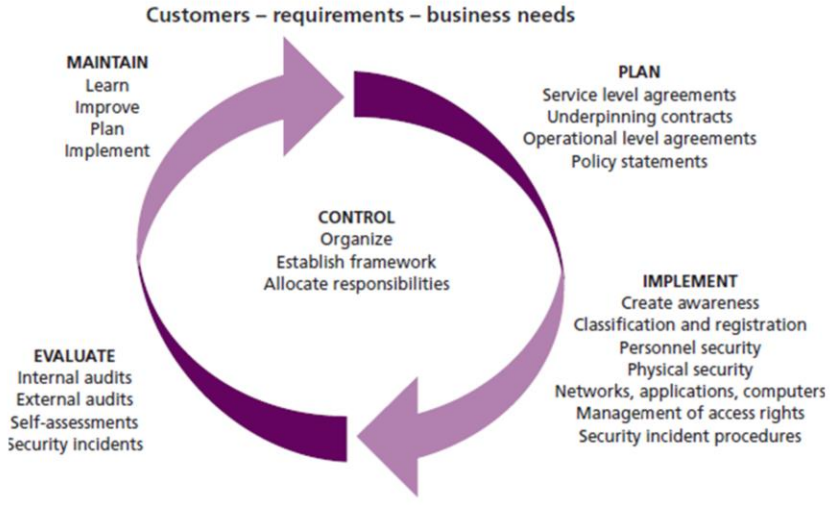
that supports the business objectives.

ISM – Purpose and Objective

- **Purpose:** align IT security with business security and ensure that the confidentiality, integrity and availability of the organization's assets, information, data and IT services always matches the agreed needs of the business

- **Objective:** protect the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of confidentiality, integrity and availability

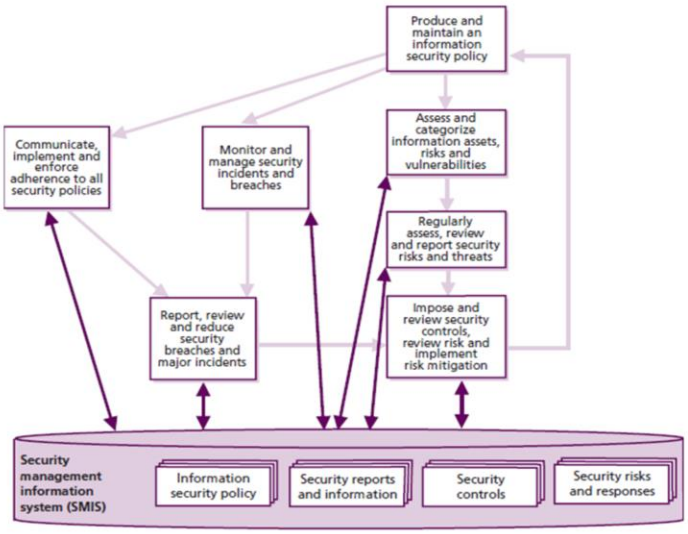
Information Security Management System



The information security management system (ISMS) provides a basis for the development of a cost-effective information security programme that supports the business objectives. It will involve the four Ps of people, process, products (technology) and partners (suppliers) to ensure high levels of security are in place wherever it is appropriate.

ISO/IEC 27001 is the formal standard against which organizations may seek independent certification of their ISMS (meaning their frameworks to design, implement, manage, maintain and enforce information security processes and controls systematically and consistently throughout the organizations). The ISMS shown above shows an approach that is widely used and is based on the advice and guidance described in many sources, including ISO/IEC 27001.

Information Security Management Process



The information security management process ensures that the security aspects with regard to services and all service management activities are appropriately managed and controlled in line with business needs and risks.

The key activities within the information security management process are:

- Production and maintenance of an overall information security policy and a set of supporting specific policies
- Communication, implementation and enforcement of the security policies, including:
- Provision of advice and guidance to all other areas of the business and IT on all information security-related issues
- Assessment and classification of all information assets and documentation
- Implementation, review, revision and improvement of a set of security controls and risk assessment and responses, including:
- Assessment of the impact of all changes on information security policies, controls and measures
- Implementation of proactive measures to improve information security wherever it is in the business interest and cost-justifiable to do so
- Monitoring and management of all security breaches and major security incidents
- Analysis, reporting and reduction of the volumes and impact of security breaches and incidents
- Schedule and completion of security reviews, audits and penetration tests.

ISM Polices

- ISM activities should be focused on and driven by an overall information security policy and a set of underpinning specific security policies.
- The policy should include:
  - An overall information security policy
  - Use and misuse of IT assets policy
  - An access control policy
  - A password control policy
  - An email policy
  - An internet policy
  - An anti-virus policy
  - An information classification policy
  - A document classification policy
  - A remote access policy
  - A policy with regard to supplier access to IT service, information and components
  - A copyright infringement policy for electronic material
  - An asset disposal policy
  - A records retention policy.

ISM activities should be focused on and driven by an overall information security policy and a set of underpinning specific security policies. The information security policy should have the full support of top executive IT management and ideally the support and commitment of top executive business management. The policy should cover all areas of security, be appropriate, meet the needs of the business and should include:

- An overall information security policy
- Use and misuse of IT assets policy
- An access control policy
- A password control policy
- An email policy
- An internet policy
- An anti-virus policy
- An information classification policy
- A document classification policy
- A remote access policy
- A policy with regard to supplier access to IT service, information and components
- A copyright infringement policy for electronic material
- An asset disposal policy
- A records retention policy.

In most cases, these policies should be widely available to all customers and users, and their compliance should be referred to in all SLRs, SLAs, OLAs, underpinning contracts and agreements.

The only exception to this approach is in the case of Type III service providers where the information security policies related to one external customer should be confidential from other customers, and the provider's own detailed policies are likely to be confidential from the customers for intellectual property rights reasons. The only sharing of security policies in this case should be the aspects that relate directly to the provision of service to that specific customer.

The policies should be authorized by top executive management within the business and IT, and compliance to them should be endorsed on a regular basis. All security policies should be reviewed – and, where necessary, revised – on at least an annual basis.

Service Design Processes

Supplier Management

Supplier Management – Purpose and Objectives

- **Purpose:** obtain value for money from suppliers and to provide seamless quality of IT service to the business by ensuring that all contracts and agreements with suppliers support the needs of the business and that all suppliers meet their contractual commitments

- **Objectives:**
  - Obtain value for money from suppliers and contracts
  - Ensure that contracts with suppliers are aligned to business needs
  - Manage suppliers relationships and performance
  - Negotiate and agree contracts with suppliers and manage them
  - Maintain:
    - Supplier policy
    - Supplier and contract management information system (SCMIS)

The supplier management process ensures that suppliers and the services they provide are managed to support IT service targets and business expectations. The aim of this section is to raise awareness of the business context of working with partners and suppliers, and how this work can best be directed toward realising business benefit for the organization.

The purpose of the supplier management process is to obtain value for money from suppliers and to provide seamless quality of IT service to the business by ensuring that all contracts and agreements with suppliers support the needs of the business and that all suppliers meet their contractual commitments.

The main objectives of the supplier management process are to:

•Obtain value for money from suppliers and contracts

•Ensure that contracts with suppliers are aligned to business needs, and support and align with agreed targets in SLRs and SLAs, in conjunction with SLM

•Manage relationships with suppliers

•Manage supplier performance

•Negotiate and agree contracts with suppliers and manage them through their lifecycle

•Maintain a supplier policy and a supporting supplier and contract management information system (SCMIS).

Supplier Management – Scope

- Implementation and enforcement of the supplier policy
- Maintenance of an SCMIS, standard contracts, terms and conditions
- Supplier and contract categorization and risk assessment
- Supplier and contract evaluation and selection
- Development, negotiation and agreement of contracts
- Contract review, renewal and termination
- Identification and implementation of improvement opportunities
- Management of
  - suppliers and supplier performance
  - contractual dispute resolution
  - sub-contracted suppliers

The supplier management process should include the management of all suppliers and contracts needed to support the provision of IT services to the business. Each service provider should have formal processes for the management of all suppliers and contracts. However, the processes should adapt to cater for the importance of the supplier and/or the contract and the potential business impact on the provision of services. Many suppliers provide support services and products that independently have a relatively minor, and fairly indirect, role in value generation, but collectively make a direct and important contribution to value generation and the implementation of the overall business strategy. The greater the contribution the supplier makes to business value, the more effort the service provider should put into the management of the supplier and the more that supplier should be involved in the development and realization of the business strategy. The smaller the supplier's value contribution, the more likely it is that the relationship will be managed mainly at an operational level, with limited interaction with the business. It may be appropriate in some organizations, particularly large ones, to manage internal teams and suppliers, where different business units may provide support of key elements.

The supplier management process should include:

•Implementation and enforcement of the supplier policy

•Maintenance of an SCMIS

•Supplier and contract categorization and risk assessment

•Supplier and contract evaluation and selection

•Development, negotiation and agreement of contracts

•Contract review, renewal and termination

•Management of suppliers and supplier performance

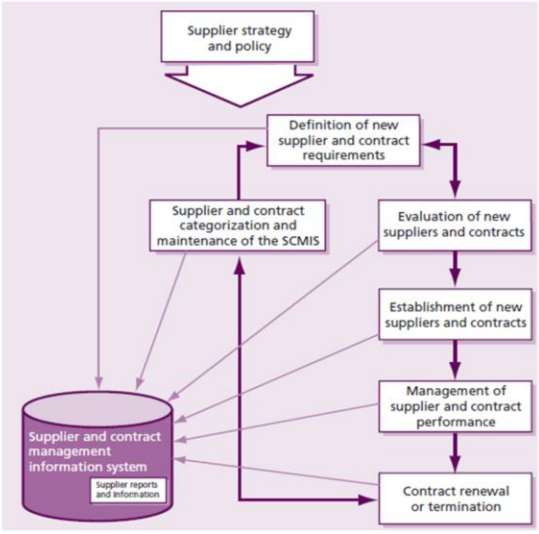
•Identification of improvement opportunities for inclusion in the CSI register, and the implementation of service and supplier improvement plans

•Maintenance of standard contracts, terms and conditions

•Management of contractual dispute resolution

•Management of sub-contracted suppliers.

Supplier Management Process



The activities of supplier management can be summarized in this way:

- Definition of new supplier and contract requirements:
  - •Identification of business need and preparation of the business case, including options (internal and external), costs, timescales, targets, benefits, risk assessment
  - •Produce a statement of requirement (SoR) and/or invitation to tender (ITT)
  - •Ensure conformance to strategy/policy

- Evaluation of new suppliers and contracts:
  - •Identify method of purchase or procurement
  - •Establish evaluation criteria – for example, services, capability (both personnel and organization), quality and cost
  - •Evaluate alternative options
  - •Select
  - •Negotiate contracts, targets and the terms and conditions, including responsibilities, closure, renewal, extension, dispute, transfer
  - •Agree and award the contract

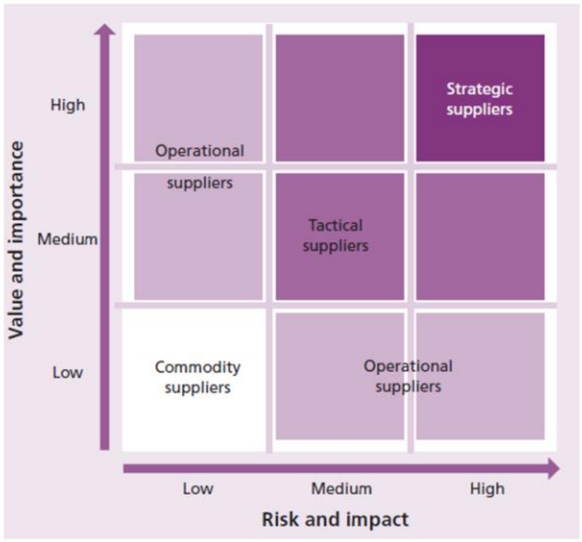
- Supplier and contract categorization and maintenance of the SCMIS:
  - Assessment or reassessment of the supplier and contract
  - Ensure changes progressed through service transition
  - Categorization of the supplier
  - Update of SCMIS
  - Ongoing maintenance of the SCMIS

- Establishment of new suppliers and contracts:
  - Set up the supplier service and contract, within the SCMIS and any other associated corporate systems
  - Transition of service
  - Establish contacts and relationships

- Supplier, contract and performance management:
  - Management and control of the operation and delivery of service/products
  - Monitor and report (service, quality and costs)
  - Review and improve (service, quality and costs)
  - Management of the supplier and the relationship (communication, risks, changes, failures, improvements, contacts, interfaces)
  - Review, at least annually, service scope against business need, targets and agreements
  - Plan for possible closure/renewal/extension

- Contract renewal or termination:
  - Review (determine benefits delivered, ongoing requirement)
  - Renegotiate and renew or terminate and/or transfer
  - Transition to new supplier(s) or to internal resources.

Supplier Categorizes



Strategic: significant 'partnering' relationships that involve senior managers sharing confidential strategic information to facilitate long-term plans
Tactical: relationships involving significant commercial activity and business interaction.
Operational: suppliers of operational products or services
Commodity: suppliers providing low-value and/or readily available products and services

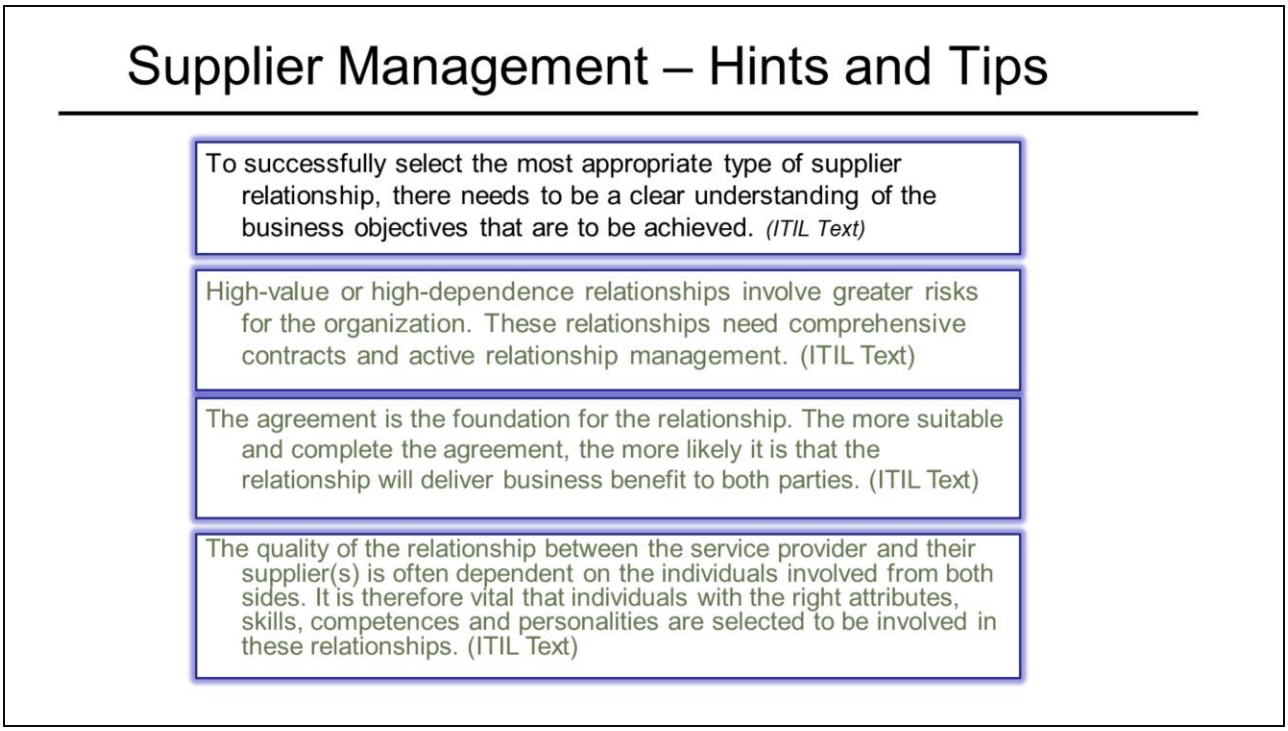
The supplier management process should be adaptive and spend more time and effort managing key suppliers than less important suppliers. This means that some form of categorization scheme should exist within the supplier management process to categorize the supplier and their importance to the service provider and the services provided to the business. Suppliers can be categorized in many ways, but one of the best methods for categorizing suppliers is based on assessing the risk and impact associated with using the supplier, and the value and importance of the supplier and its services to the business.

A number of factors, from the nature of the service to the overall cost, determine the importance of a supplier from a business perspective. As shown later, the greater the business significance of a supplier relationship, the more the business needs to be involved in the management and development of a relationship. A formal categorization approach can help to establish this importance.

Strategically important supplier relationships are given the greatest focus. It is in these cases that supplier managers have to ensure that the culture of the service provider organization is extended into the supplier domain so that the relationship works beyond the initial contract. The rise in popularity of outsourcing, and the increase in the scope and complexity of some sourcing arrangements, has resulted in a diversification of types of supplier relationship. At a strategic level, it is important to understand the options that are available so that the most suitable type of supplier relationship can be established to gain maximum business benefit and evolves in line with business needs.

The amount of time and effort spent managing the supplier and the relationship can then be appropriate to its categorization:

- **Strategic** For significant ‘partnering’ relationships that involve senior managers sharing confidential strategic information to facilitate long-term plans. These relationships would normally be managed and owned at a senior management level within the service provider organization, and would involve regular and frequent contact and performance reviews. These relationships would probably require involvement of service strategy and service design resources, and would include ongoing specific improvement programmes (e.g. a network service provider supplying worldwide networks service and their support).
- **Tactical** For relationships involving significant commercial activity and business interaction. These relationships would normally be managed by middle management and would involve regular contact and performance reviews, often including ongoing improvement programmes (e.g. a hardware maintenance organization providing resolution of server hardware failures).
- **Operational** For suppliers of operational products or services. These relationships would normally be managed by junior operational management and would involve infrequent but regular contact and performance reviews (e.g. an internet hosting service provider, supplying hosting space for a low-usage, low-impact website or internally used IT service).
- **Commodity** For suppliers providing low-value and/or readily available products and services, which could be alternatively sourced relatively easily (e.g. paper or printer cartridge suppliers).



The more customized those services are, the greater the difficulty in moving to an alternative supplier. Customization may benefit the business, contributing to competitive advantage through differentiated service, or may be the result of operational evolution. Tailored services increase the dependence on the supplier, increase risk and can result in increased cost. From a supplier perspective, tailored services may decrease their ability to achieve economies of scale through common operations, resulting in narrowed margins, and reduced capital available for future investment. Standard products and services are the preferred approach unless a clear business advantage exists, in which case a strategic supplier delivers the tailored service.

Having established the type of supplier, the relationship then needs to be formalized. In the discussion below, the term ‘agreement’ is used generically to refer to any formalization of a relationship between customer and supplier organizations, and may range from the informal to comprehensive legally binding contracts.

Reducing the number of direct suppliers reduces the number of relationships that need to be managed, the number of peer-to-peer supplier issues that need to be resolved, and reduces the complexity of the supplier management activities. Some organizations may successfully reduce or collapse the whole supply chain around a single service provider, often referred to as a ‘prime’ supplier. Facilities management is often outsourced to a single specialist partner or supplier, who may in turn sub-contract restaurant services, vending machine maintenance and cleaning.

Outsourcing entire business services to a single ‘prime supplier’ may run additional risks. For these reasons, organizations need to consider carefully their supply chain strategies ahead of major outsourcing activity. The scope of outsourced services needs to be considered to reduce the number of suppliers, while ensuring that risk is managed and it fits with typical competencies in the supply market.

Service Design Processes

Capacity Management

Capacity Management– Purpose and Objectives

- **Purpose:** ensure that the capacity of IT services and the IT infrastructure meets the agreed capacity- and performance-related requirements in a cost-effective and timely manner.

- **Objectives:**
  - Produce and maintain an appropriate capacity plan
  - Provide advice and guidance to other areas on all capacity- and performance-related issues
  - Ensure that service performance achievements meet all of their agreed targets
  - Assist with the diagnosis and resolution of performance- and capacity-related incidents and problems
  - Assess the impact of all changes on the capacity plan
  - Ensure that proactive measures to improve the performance of services are implemented wherever it is cost-justifiable to do so

The purpose of the capacity management process is to ensure that the capacity of IT services and the IT infrastructure meets the agreed capacity- and performance-related requirements in a cost-effective and timely manner. Capacity management is concerned with meeting both the current and future capacity and performance needs of the business.

The objectives of capacity management are to:

•Produce and maintain an appropriate and up-to-date capacity plan, which reflects the current and future needs of the business

•Provide advice and guidance to all other areas of the business and IT on all capacity- and performance-related issues

•Ensure that service performance achievements meet all of their agreed targets by managing the performance and capacity of both services and resources

•Assist with the diagnosis and resolution of performance- and capacity-related incidents and problems

•Assess the impact of all changes on the capacity plan, and the performance and capacity of all services and resources

•Ensure that proactive measures to improve the performance of services are

implemented wherever it is cost-justifiable to do so.

Capacity Management– Scope

- Monitoring patterns of business activity
- Tuning activities to make the most efficient use of existing IT resources
- Understanding the agreed current and future demands and producing forecasts for future requirements
- Influencing demand in conjunction with the financial management for IT services and demand management processes
- Producing a capacity plan
- Assisting with the identification and resolution of any incidents and problems associated with capacity or performance
- Proactive improvement of service or component performance

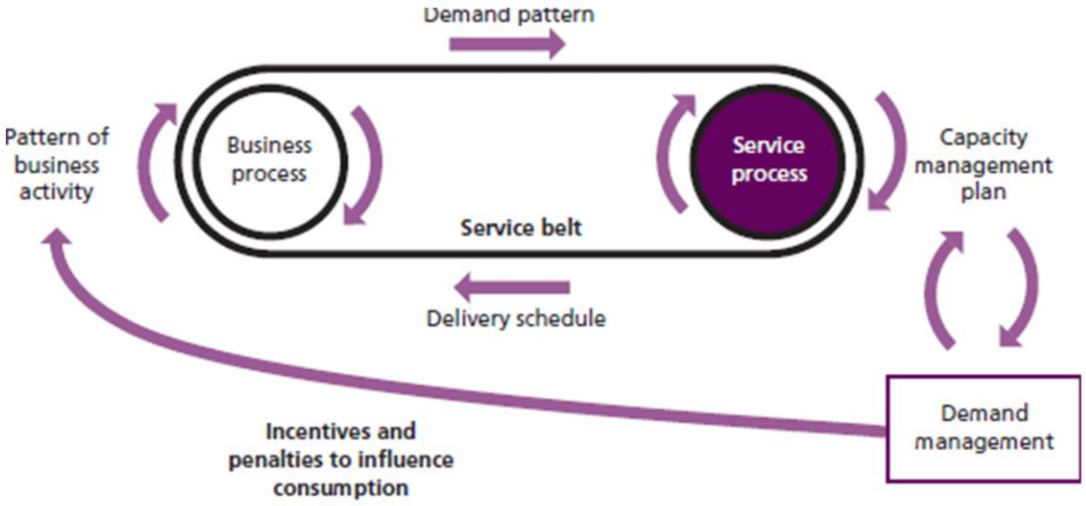
The capacity management process should be the focal point for all IT performance and capacity issues. Capacity management considers all resources required to deliver the IT service, and plans for short-, medium- and long-term business requirements. Capacity management should also consider space planning and environmental systems capacity. Capacity management could consider **human resource capacity** where a lack of human resources could result in a breach of SLA or OLA targets, a delay in the end-to-end performance or service response time, or an inability to meet future commitments and plans (e.g. overnight data backups not completed in time because no operators were present to load tapes).

The capacity management process should include:

- Monitoring patterns of business activity through performance, utilization and throughput of IT services and the supporting infrastructure, environmental, data and applications components and the production of regular and ad hoc reports on service and component capacity and performance
- Undertaking tuning activities to make the most efficient use of existing IT resources
- Understanding the agreed current and future demands being made by the customer for IT resources, and producing forecasts for future requirements
- Influencing demand in conjunction with the financial management for IT services and demand management processes
- Producing a capacity plan that enables the service provider to continue to provide services of the quality defined in SLAs and that covers a sufficient planning timeframe to meet future service levels required as defined in the service portfolio and SLRs
- Assisting with the identification and resolution of any incidents and problems associated with service or component capacity or performance
- The proactive improvement of service or component performance, wherever it is cost-justifiable and meets the needs of the business.

Capacity management is responsible for ensuring that IT resources are planned and scheduled to provide a consistent level of service that is matched to the current and future needs of the business, as agreed and documented within SLAs and OLAs.

Capacity Management and Demand Management



Capacity Plan

- The capacity plan contains:
  - Information on the current usage of service and components
  - plans for the development of IT capacity to meet the needs in the growth of both existing service and any agreed new services
- The plan should be actively used as a basis for decision-making as it provides planning input to many other areas of IT and the business
- The plan should be acted on by the IT service provider and senior management of the organization to plan the capacity of the IT infrastructure

Service Design Processes

IT Service Continuity Management (ITSCM)

ITSCM– Purpose and Objectives

- **Purpose:** support the overall business continuity management (BCM) process by ensuring that, by managing the risks that could seriously affect IT services, the IT service provider can always provide minimum agreed business continuity-related service levels

- **Objectives:**
  - Produce and maintain a set of IT service continuity plans
  - Complete regular BIA exercises
  - Conduct regular risk assessment and management exercises in conjunction with the availability and ISM processes
  - Provide advice and guidance on all continuity-related issues
  - Ensure that appropriate continuity mechanisms are used
  - Assess the impact of all changes on the IT service continuity plans
  - Ensure that proactive measures to improve the availability of services are implemented wherever it is cost-justifiable to do so
  - Negotiate and agree contracts with suppliers for the provision of the necessary recovery capability in conjunction with the supplier management process

In support of and alignment with the BCM process, ITSCM uses formal risk assessment and management techniques to:

•Reduce risks to IT services to agreed acceptable levels

•Plan and prepare for the recovery of IT services.

For a definition of BCM, please see the glossary at the end of this publication.

The objectives of ITSCM are to:

•Produce and maintain a set of IT service continuity plans that support the overall business continuity plans of the organization

•Complete regular BIA exercises to ensure that all continuity plans are maintained in line with changing business impacts and requirements

•Conduct regular risk assessment and management exercises to manage IT services within an agreed level of business risk in conjunction with the business and the availability management and information security management processes

•Provide advice and guidance to all other areas of the business and IT on all continuity-related issues

•Ensure that appropriate continuity mechanisms are put in place to meet or exceed the agreed business continuity targets

•Assess the impact of all changes on the IT service continuity plans and supporting methods and procedures

•Ensure that proactive measures to improve the availability of services are implemented wherever it is cost-justifiable to do so

•Negotiate and agree contracts with suppliers for the provision of the necessary recovery capability to support all continuity plans in conjunction with the supplier management process.

ITSCM– Scope

- The agreement of the scope of the ITSCM process and the policies adopted
- BIA to quantify the impact loss of IT service would have on the business
- Risk assessment and management
- Production of an overall ITSCM strategy and plan that must be integrated into the BCM strategy and plan
- Testing of the plans
- Ongoing operation and maintenance of the plans

ITSCM focuses on those events that the business considers significant enough to be treated as a 'disaster'. Less significant events will be dealt with as part of the incident management process. What constitutes a disaster will vary from organization to organization. The impact of a loss of a business process, such as financial loss, damage to reputation or regulatory breach, is measured through a BIA exercise, which determines the minimum critical requirements.

ITSCM does not usually directly cover longer-term risks such as those from changes in business direction, diversification, restructuring, major competitor failure, and so on. There is usually time to identify and evaluate the risk and include risk mitigation through changes or shifts in business and IT strategies. ITSCM also does not usually cover minor technical faults (for example, non-critical disk failure), unless there is a possibility that the impact could have a major impact on the business. These risks would be expected to be covered mainly through the service desk and the incident management process, or resolved through the planning associated with other processes (availability, problem, change management, etc.)

The ITSCM process includes:

•The agreement of the scope of the ITSCM process and the policies adopted

•BIA to quantify the impact loss of IT service would have on the business

•Risk assessment and management – the risk identification and risk assessment to identify potential threats to continuity and the likelihood of the threats becoming reality. This also includes taking measures to manage the identified threats where this can be cost-justified. The approach to managing these threats will form the core of the ITSCM strategy and plans

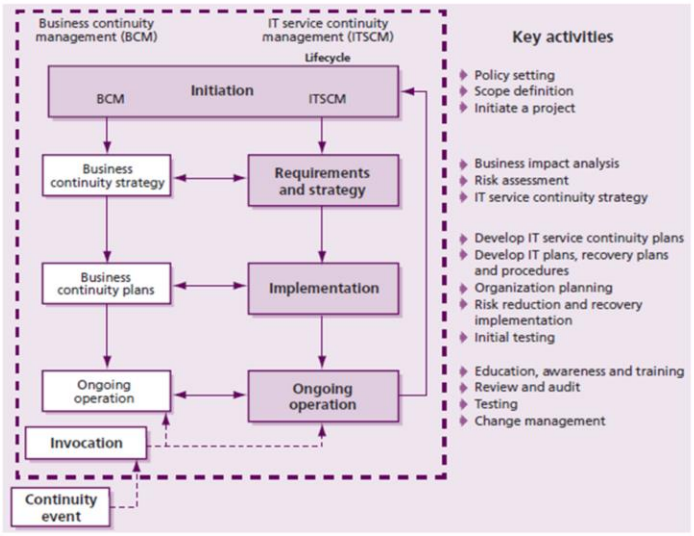
•Production of an overall ITSCM strategy that must be integrated into the BCM strategy. This can be produced following the two steps identified above, and is likely to include elements of risk reduction as well as selection of appropriate and comprehensive recovery options

•Production of an ITSCM plan, which again must be integrated with the overall BCM plans

•Testing of the plans

•Ongoing operation and maintenance of the plans.

ITSCM– Lifecycle



Stage 1 – Initiation: The initiation process covers the whole of the organization and consists of the following activities.

• Policy setting: This should be established and communicated as soon as possible so that all members of the organization involved in, or affected by, business continuity issues are aware of their responsibilities to comply with and support ITSCM. As a minimum, the policy should set out management intention and objectives.

• Define scope and specify terms of reference: This includes defining the scope and responsibilities of all staff in the organization. It covers such tasks as undertaking a risk assessment and business impact analysis and determination of the command and control structure required to support a business interruption.

• Initiate a project: The initiation of formal IT service continuity management is best organized into a project. The project can be used to bring ITSCM to the 'ongoing operation' stage.

Stage 2 – Requirements and strategy: Ascertaining the business requirements for IT service continuity is a critical component in order to determine how well an organization will survive a business interruption or disaster and the costs that will be incurred. This stage can effectively be split into two sections:

•**Requirements** Perform BIA and risk assessment

•**Strategy** Following the requirements analysis, the strategy should document how the risks will be managed through risk reduction measures and recovery options required to support the business.

Stage 3 – Implementation: Once the strategy has been approved, the detailed IT service continuity plans need to be produced in line with the business continuity plans and the measures to implement the strategy need to be put in place. The measures to implement the strategy will include putting in place both the defined risk reduction and recovery option arrangements and performing initial testing to ensure that what was planned has been achieved.

• Develop IT service continuity plans and procedures: ITSCM plans need to be developed to enable the necessary information for critical systems, services and facilities to either continue to be provided or to be reinstated within an acceptable period to the business.

• Organization planning: During the disaster recovery process, the organizational structure will inevitably be different from normal operation and will be based around: executive, coordination, and recovery

• Risk reduction/recovery arrangement implementation: Risk reduction arrangements are usually undertaken in conjunction with availability management.

• Initial testing: Experience has shown that recovery plans that have not been fully tested do not work as intended, if at all. Testing is therefore a critical part of the overall ITSCM process and the only way of ensuring that the selected strategy, standby arrangements, logistics, business recovery plans and procedures will actually work in practice.

Stage 4 – Ongoing operation: This stage consists of the activities necessary to firmly establish the ITSCM capabilities and maintain them in an accurate and reliable state as time goes on. The activities of ongoing operation include the following,

•Education, awareness and training: should cover the organization and, in particular, the IT organization, for service continuity-specific items.

• Review and audit: Regular review of all of the deliverables from the ITSCM process needs to be undertaken to ensure that they remain current. With service providers struggling to do everything they must to serve their customers, it may be difficult to set aside the time needed for reviews and audits, but the work is necessary.

• Testing: Following the initial testing, it is necessary to establish a programme of regular testing to ensure that the critical components of the strategy are tested, preferably at least annually, although testing of IT service continuity plans should be arranged in line with business needs and the needs of the business continuity plans. All plans should also be tested after every major business change. It is important that any changes to the IT technology are also included in the strategy, implemented in an appropriate fashion and tested to ensure that they function correctly within the overall provision of IT following a disaster.

• Change management: The change management process should ensure that all changes are assessed for their potential impact on the ITSCM plans. If the planned change will invalidate the plans, then the plan must be updated before the change is implemented, and it should be tested as part of the change testing.

The plans themselves must be under very strict change management and service asset and configuration management control. Inaccurate plans and inadequate recovery capabilities may result in the failure of business continuity plans. Also, on an ongoing basis, whenever there are new services or where services have major changes, it is essential that a BIA and a risk assessment is conducted on the new or changed service and the strategy and plans updated accordingly.

Business Impact Analysis (BIA)

- The purpose of a BIA is to quantify the impact to the business that loss of service would have
  - 'hard' impact that can be precisely identified (e.g., financial loss)
  - 'soft' impact (e.g., public relations, moral, health and safety)
- The BIA is a key input to the strategy as it helps in identifying the most important services to the organization

The BIA identifies:

•The form that the damage or loss may take – for example:

•Lost income

•Additional costs

•Damaged reputation

•Loss of goodwill

•Loss of competitive advantage

•Breach of law, health and safety

•Risk to personal safety

•Immediate and long-term loss of market share

•Political, corporate or personal embarrassment

•Loss of operational capability, for example, in a command and control environment

•How the degree of damage or loss is likely to escalate after a service disruption, and the times of the day, week, month or year when disruption will be most severe

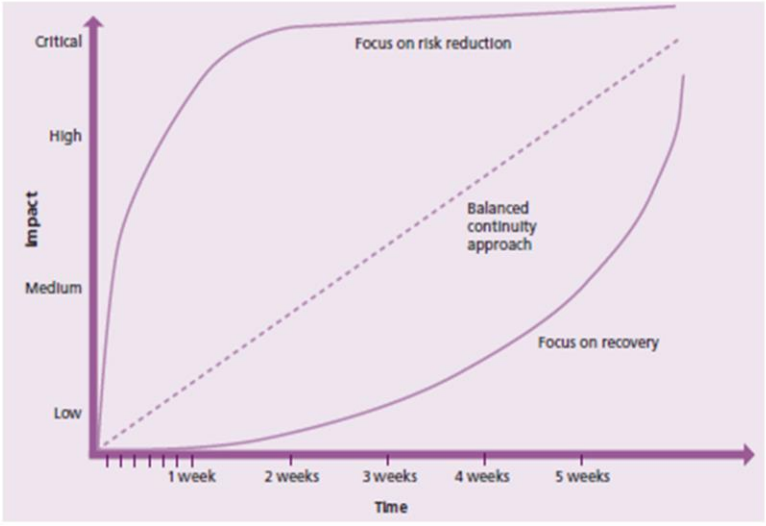
•The staffing, skills, facilities and services (including the IT services) necessary to enable critical and essential business processes to continue operating at a minimum acceptable level

•The time within which minimum levels of staffing, facilities and services should be recovered

•The time within which all required business processes and supporting staff, facilities and services should be fully recovered

•The relative business recovery priority for each of the IT services.

Graphical Representation of BIA



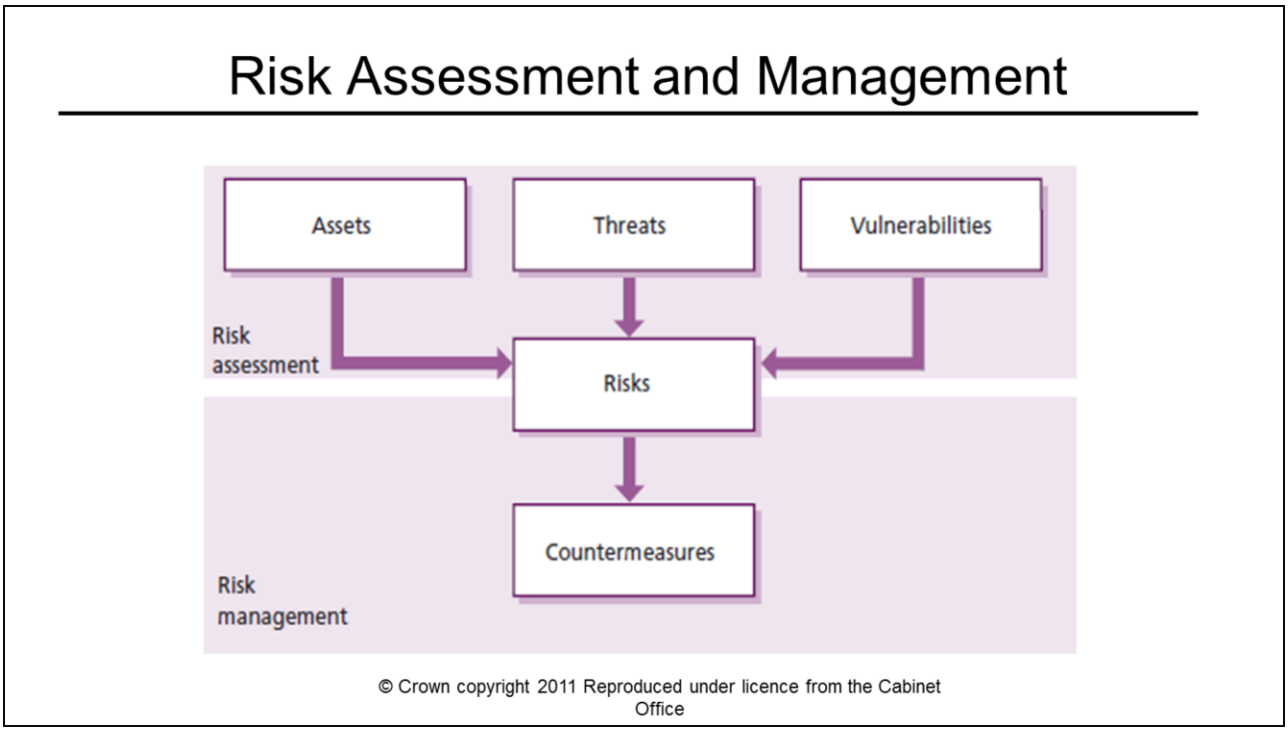
One of the key outputs from a BIA exercise is a graph of the anticipated business impact caused by the loss of a business process or the loss of an IT service over time. This graph can then be used to drive the business and IT continuity strategies and plans. More preventive measures need to be adopted with regard to those processes and services with earlier and higher impacts, whereas greater emphasis should be placed on continuity and recovery measures for those where the impact is lower and takes longer to develop. A balanced approach of both measures should be adopted to those in between.

These items provide the drivers for the level of ITSCM mechanisms that need to be considered or deployed. Once presented with these options, the business may decide that lower levels of service or increased delays are more acceptable, based on a cost benefit analysis, or it may be that comprehensive disaster prevention measures will need to be implemented.

These assessments enable the mapping of critical service, application and technology components to critical business processes, thus helping to identify the ITSCM elements that need to be provided. The business requirements are ranked and the associated ITSCM elements confirmed and prioritized in terms of risk reduction and recovery planning. The results of the BIA, discussed earlier, are invaluable input to several areas of process design including SLM to understand the required service levels.

Impacts should be measured against particular scenarios for each business process, such as an inability to settle trades in a money market dealing process, or an inability to invoice for a period of days.

Example of BIA: money market dealing environment where loss of market data information could mean that the organization starts to lose money immediately as trading cannot continue. In addition, customers may go to another organization, which would mean potential loss of core business. Loss of the settlement system does not prevent trading from taking place, but if trades already conducted cannot be settled within a specified period of time, the organization may be in breach of regulatory rules or settlement periods and suffer fines and damaged reputation. This may actually be a more significant impact than the inability to trade because of an inability to satisfy customer expectations.



Risk assessment involves the identification and assessment of the level (measure) of the risks calculated from the assessed values of assets and the assessed levels of threats to, and vulnerabilities of, those assets. Risk is also determined to a certain extent by its acceptance. Some organizations and businesses may be more willing to accept risk whereas others are not.

Risk management involves the identification, selection and adoption of countermeasures justified by the identified risks to assets in terms of their potential impact on services if failure occurs, and the reduction of those risks to an acceptable level. Risk management is an activity that is associated with many other activities, especially the IT service continuity management and information security management processes and the service transition lifecycle stage. All of these risk assessment exercises should be coordinated.

Conducting a formal risk assessment will typically result in a risk profile that can be used to determine appropriate risk responses or risk reduction measures (ITSCM mechanisms) to manage the risks, i.e. reduce the risk to an acceptable level or mitigate the risk.

Examples:

Risk: Loss of data

Threat: Technology failure- Human error- Viruses, malicious software, e.g. attack applets

Risk: Unavailability of key technical and support staff

Threat: Industrial action - Denial of access to premises -Resignation- Sickness/injury-Transport difficulties

A number of risk assessment and management methods are available for both the commercial and government sectors. Risk assessment is the assessment of the risks that may give rise to service disruption or security violation. Risk management is concerned with identifying appropriate risk responses or cost-justifiable countermeasures to combat those risks. A standard methodology, such as the Management of Risk (M_o_R), should be used to assess and manage risks within an organization.