[Template:Use British English](/wiki/Template:Use_British_English" \o "Template:Use British English) [Template:Refimprove](/wiki/Template:Refimprove)

**ITIL**, formerly an acronym for **Information Technology Infrastructure Library**, is a set of practices for [IT service management](/wiki/IT_service_management) (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITIL 2011 edition), ITIL is published as a series of five core volumes, each of which covers a different ITSM lifecycle stage. Although ITIL underpins [ISO/IEC 20000](/wiki/ISO/IEC_20000) (previously BS 15000), the International Service Management Standard for IT service management, there are some differences between the ISO 20000 standard and the ITIL framework.

ITIL describes processes, procedures, tasks, and checklists which are not organization-specific, but can be applied by an organization for establishing integration with the organization's strategy, delivering value, and maintaining a minimum level of competency. It allows the organization to establish a baseline from which it can plan, implement, and measure. It is used to demonstrate compliance and to measure improvement.

Since July 2013, ITIL has been owned by [AXELOS](/wiki/AXELOS), a [joint venture](/wiki/Joint_venture) between [Capita](/wiki/Capita) and the [Cabinet Office](/wiki/Cabinet_Office). AXELOS licenses organisations to use the ITIL intellectual property, accredits licensed examination institutes, and manages updates to the framework.

## Contents

* 1 History[[edit](/index.php?title=(none)&action=edit&section=1)]
* 2 Service strategy[[edit](/index.php?title=(none)&action=edit&section=4)]
  + 2.1 Service Portfolio Management[[edit](/index.php?title=(none)&action=edit&section=5)]
  + 2.2 Financial management for IT services[[edit](/index.php?title=(none)&action=edit&section=6)]
* 3 Service design[[edit](/index.php?title=(none)&action=edit&section=7)]
  + 3.1 Service catalogue management[[edit](/index.php?title=(none)&action=edit&section=8)]
  + 3.2 Service-level management[[edit](/index.php?title=(none)&action=edit&section=9)]
  + 3.3 Availability management[[edit](/index.php?title=(none)&action=edit&section=10)]
  + 3.4 Capacity management[[edit](/index.php?title=(none)&action=edit&section=11)]
  + 3.5 IT service continuity management[[edit](/index.php?title=(none)&action=edit&section=12)]
  + 3.6 Security management[[edit](/index.php?title=(none)&action=edit&section=13)]
  + 3.7 Supplier management[[edit](/index.php?title=(none)&action=edit&section=14)]
* 4 Service transition[[edit](/index.php?title=(none)&action=edit&section=15)]
  + 4.1 Change management[[edit](/index.php?title=(none)&action=edit&section=16)]
  + 4.2 Service asset and configuration management[[edit](/index.php?title=(none)&action=edit&section=17)]
  + 4.3 Release and deployment management[[edit](/index.php?title=(none)&action=edit&section=18)]
* 5 Service operation[[edit](/index.php?title=(none)&action=edit&section=19)]
  + 5.1 Processes[[edit](/index.php?title=(none)&action=edit&section=20)]
  + 5.2 Functions[[edit](/index.php?title=(none)&action=edit&section=21)]
    - 5.2.1 Service desk[[edit](/index.php?title=(none)&action=edit&section=22)]
    - 5.2.2 Application management[[edit](/index.php?title=(none)&action=edit&section=23)]
    - 5.2.3 IT Operations management[[edit](/index.php?title=(none)&action=edit&section=24)]
    - 5.2.4 Technical management[[edit](/index.php?title=(none)&action=edit&section=25)]
  + 5.3 Event management[[edit](/index.php?title=(none)&action=edit&section=26)]
  + 5.4 Incident management[[edit](/index.php?title=(none)&action=edit&section=27)]
  + 5.5 Request fulfillment[[edit](/index.php?title=(none)&action=edit&section=28)]
  + 5.6 Problem management[[edit](/index.php?title=(none)&action=edit&section=29)]
    - 5.6.1 Root-cause analysis[[edit](/index.php?title=(none)&action=edit&section=30)]
  + 5.7 Identity management[[edit](/index.php?title=(none)&action=edit&section=31)]
* 6 Continual service improvement (CSI)[[edit](/index.php?title=(none)&action=edit&section=32)]
* 7 Overview of ITIL v2[[edit](/index.php?title=(none)&action=edit&section=33)]
  + 7.1 Service support[[edit](/index.php?title=(none)&action=edit&section=34)]
  + 7.2 Service delivery[[edit](/index.php?title=(none)&action=edit&section=35)]
  + 7.3 ICT infrastructure management[[edit](/index.php?title=(none)&action=edit&section=36)]
    - 7.3.1 ICT design and planning[[edit](/index.php?title=(none)&action=edit&section=37)]
    - 7.3.2 ICT deployment management[[edit](/index.php?title=(none)&action=edit&section=38)]
    - 7.3.3 ICT operations management[[edit](/index.php?title=(none)&action=edit&section=39)]
    - 7.3.4 ICT technical support[[edit](/index.php?title=(none)&action=edit&section=40)]
  + 7.4 Planning to implement service management[[edit](/index.php?title=(none)&action=edit&section=41)]
  + 7.5 Small-scale implementation[[edit](/index.php?title=(none)&action=edit&section=42)]
* 8 Related frameworks[[edit](/index.php?title=(none)&action=edit&section=43)]
  + 8.1 Descendants[[edit](/index.php?title=(none)&action=edit&section=44)]
    - 8.1.1 Microsoft Operations Framework[[edit](/index.php?title=(none)&action=edit&section=45)]
    - 8.1.2 FITS[[edit](/index.php?title=(none)&action=edit&section=46)]
  + 8.2 Other frameworks[[edit](/index.php?title=(none)&action=edit&section=47)]
* 9 Certification[[edit](/index.php?title=(none)&action=edit&section=48)]
  + 9.1 Individuals[[edit](/index.php?title=(none)&action=edit&section=49)]

## History[[edit](/index.php?title=(none)&action=edit&section=1)]

Responding to growing dependence on IT, the UK Government's [Central Computer and Telecommunications Agency](/wiki/Central_Computer_and_Telecommunications_Agency) (CCTA) in the 1980s developed a set of recommendations. It recognized that, without standard practices, government agencies and private sector contracts had started independently creating their own IT management practices.

The IT Infrastructure Library originated as a collection of books, each covering a specific practice within [IT service management](/wiki/IT_service_management). ITIL was built around a process model-based view of controlling and managing operations often credited to [W. Edwards Deming](/wiki/W._Edwards_Deming) and his [plan-do-check-act (PDCA)](/wiki/PDCA) cycle.[[1]](#cite_note-1) After the initial publication in 1989–96, the number of books quickly grew within ITIL v1 to more than 30 volumes.

In 2000/2001, to make ITIL more accessible (and affordable), ITIL v2 consolidated the publications into nine logical "sets" that grouped related process-guidelines to match different aspects of IT management, applications and services. The Service Management sets (Service Support and Service Delivery) were by far the most widely used, circulated, and understood of the ITIL v2 publications.[Template:Citation needed](/wiki/Template:Citation_needed)

* In April 2001, the CCTA was merged into the [OGC](/wiki/Office_of_Government_Commerce), an office of the [UK Treasury](/wiki/HM_Treasury).[[2]](#cite_note-2)# ITIL Service Transition: *develops and improves capabilities for introducing new services into supported environments.*<ref name=service\_transition>[Template:Cite book](/wiki/Template:Cite_book)</ref>

1. ITIL Service Operation: *manages services in supported environments.*<ref name=service\_operation>[Template:Cite book](/wiki/Template:Cite_book)</ref>
2. ITIL Continual Service Improvement: *achieves services incremental and large-scale improvements.*<ref name=csi>[Template:Cite book](/wiki/Template:Cite_book)</ref>

Due to the similarity between ITIL v3 of 2007 and ITIL 2011, no bridge examinations for ITIL v3 certification holders were created or made available for ITIL 2011 certification.

## Service strategy[[edit](/index.php?title=(none)&action=edit&section=4)]

The center and origin point of the ITIL Service Lifecycle, the ITIL Service Strategy (SS) volume,<ref name=service\_strategy/> provides guidance on clarification and prioritization of service-provider investments in services. More generally, Service Strategy focuses on helping IT organizations improve and develop over the long term. In both cases, Service Strategy relies largely upon a market-driven approach. The Service Strategy lifecycle stage is often considered as the core of the service lifecycle. In Service Strategy stage, the strategic approach for the whole lifecycle is identified to provide values to the customers through IT service management. Key topics covered include service value definition, [business-case](/wiki/Business_case) development, service assets, market analysis, and service provider types. List of covered processes:

* Strategy management for IT Services
* [Service portfolio management](/wiki/Service_portfolio_management)
* [Financial management for IT services](/wiki/Financial_management_for_IT_services)
* [Demand management](/wiki/Demand_management)
* [Business relationship management](/wiki/Business_relationship_management)

For candidates in the ITIL Intermediate Capability stream, the Service Offerings and Agreements (SOA) Qualification course and exam are most closely aligned to the Service Strategy (SS) Qualification course and exam in the Lifecycle stream.

### Service Portfolio Management[[edit](/index.php?title=(none)&action=edit&section=5)]

The customer needs services to achieve their objectives. The service provider should ensure they can provide these services. The purpose of Service Portfolio Management is ensuring these services are offered.

The service portfolio contains the services managed by the service provider. The service portfolio comprises: the pipeline section, which contains the services that are yet to be offered; the [service catalog](/wiki/Service_catalog) section, which contains the details of operational services; and the retired section, which contains details of the services that are no longer offered.

### Financial management for IT services[[edit](/index.php?title=(none)&action=edit&section=6)]

[Template:Main](/wiki/Template:Main) IT Financial Management comprises the discipline of ensuring that the IT infrastructure is obtained at the most effective price (which does not necessarily mean cheapest) and calculating the cost of providing IT services so that an organization can understand the costs of its IT services. These costs may then be recovered from the customer of the service. This is the 2nd component of service delivery process.

## Service design[[edit](/index.php?title=(none)&action=edit&section=7)]

The Service Design (SD) volume<ref name=service\_design/> provides good-practice guidance on the design of IT services, processes, and other aspects of the service management effort. Significantly, design within ITIL is understood to encompass all elements relevant to technology service delivery, rather than focusing solely on design of the technology itself. As such, service design addresses how a planned service solution interacts with the larger business and technical environments, service management systems required to support the service, processes which interact with the service, technology, and architecture required to support the service, and the supply chain required to support the planned service. Within ITIL, design work for an IT service is aggregated into a single [Service Design Package](/wiki/ITIL/service_design_package) ([SDP](/wiki/ITIL/service_design_package)). Service design packages, along with other information about services, are managed within the service catalogues.

List of covered processes:

1. Design coordination
2. [Service catalogue](/wiki/Service_catalog) management
3. [Service-level](/wiki/Service-level_agreement) management
4. [Availability](/wiki/Availability) management
5. [Capacity management](/wiki/Capacity_management)
6. [IT service continuity management](/wiki/IT_service_continuity)
7. [Security management](/wiki/ITIL#Security_management)
8. [Supplier](/wiki/Vendor_(supply_chain)) management

A model used to help define roles and responsibilities in service design is a [RACI matrix](/wiki/RACI_matrix) (Responsible, Accountable, Consulted and Informed).

### Service catalogue management[[edit](/index.php?title=(none)&action=edit&section=8)]

Service catalogue management maintains and produces the [service catalogue](/wiki/Service_catalog) and ensures that it contains accurate details, dependencies and interfaces of all services made available to customers. Service catalogue information includes:

* ordering and requesting processes
* prices
* deliverables
* contract points

### Service-level management[[edit](/index.php?title=(none)&action=edit&section=9)]

Service-level management provides for continual identification, monitoring and review of the levels of IT services specified in the [service-level agreements](/wiki/Service-level_agreement) (SLAs). Service-level management ensures that arrangements are in place with internal IT support-providers and external suppliers in the form of operational level agreements (OLAs) and [underpinning contracts](/wiki/Underpinning_contract) (UCs), respectively. The process involves assessing the impact of change on service quality and SLAs. The service-level management process is in close relation with the operational processes to control their activities. The central role of service-level management makes it the natural place for [metrics](/wiki/Software_metric) to be established and monitored against a [benchmark](/wiki/Benchmarking).

Service-level management is the primary interface with the customer (as opposed to the user serviced by the [service desk](/wiki/#Service_desk)). Service-level management is responsible for:

* ensuring that the agreed IT services are delivered when and where they are supposed to be;
* liaising with [availability management](/wiki/#Availability_management), [capacity management](/wiki/#Capacity_management), [incident management](/wiki/Incident_management_(ITSM)) and [problem management](/wiki/#Problem_management) to ensure that the required levels and quality of service are achieved within the resources agreed with [financial management](/wiki/#Financial_management_for_IT_services);
* ensuring that appropriate [IT service continuity](/wiki/#IT_service_continuity_management) plans exist to support the business and its continuity requirements.

The service-level manager relies on the other areas of the service delivery process to provide the necessary support which ensures the agreed services are provided in a cost-effective, secure and efficient manner.

### Availability management[[edit](/index.php?title=(none)&action=edit&section=10)]

Availability management allows organizations to sustain IT service-availability in order to support the business at a justifiable cost. High-level activities are realizing availability requirements, compiling availability plans, monitoring availability, and monitoring maintenance obligations.

Availability management addresses the ability of an IT component to perform at an agreed level over a period of time.

* Reliability: Ability of an IT component to perform at an agreed level at described conditions.
* Maintainability: The ability of an IT component to remain in, or be restored to an operational state.
* [Serviceability](/wiki/Serviceability_(computer)): The ability for an external supplier to maintain the availability of component or function under a third-party contract.
* Resilience: A measure of freedom from operational failure and a method of keeping services reliable. One popular method of resilience is redundancy.
* [Security](/wiki/Computer_security): A service may have associated data. Security refers to the confidentiality, integrity, and availability of that data. Availability gives a clear overview of the end-to-end availability of the system.

### Capacity management[[edit](/index.php?title=(none)&action=edit&section=11)]

[Capacity management](/wiki/Capacity_management) supports the optimum and cost-effective provision of IT services by helping organizations match their IT resources to business demands. The high-level activities include:

* application sizing
* workload management
* demand management
* modelling
* capacity planning
* resource management
* performance management

Capacity management is focused on strategic capacity, including capacity of personnel (e.g., human resources, staffing and training), system capacity, and component (or tactical) capacity.

### IT service continuity management[[edit](/index.php?title=(none)&action=edit&section=12)]

IT service continuity management (ITSCM) covers the processes by which plans are put in place and managed to ensure that IT services can recover and continue even after a serious incident occurs. It is not just about reactive measures, but also about proactive measures – reducing the risk of a disaster in the first instance.

ITSCM is regarded by the application owners as the recovery of the IT infrastructure used to deliver IT services, but [Template:As of](/wiki/Template:As_of) many businesses practice the much further-reaching process of business continuity planning ([BCP](/wiki/Business_continuity_planning)), to ensure that the whole end-to-end business process can continue should a serious incident occur (at primary support level).

ITSCM involves the following basic steps:

* prioritising the activities to be recovered by conducting a [business impact analysis](/wiki/Business_impact_analysis) (BIA)
* performing a risk assessment (aka [risk analysis](/wiki/Risk_analysis_(business))) for each of the IT services to identify the assets, threats, vulnerabilities and countermeasures for each service.
* evaluating the options for recovery
* producing the contingency plan
* testing, reviewing, and revising the plan on a regular basis.

### Security management[[edit](/index.php?title=(none)&action=edit&section=13)]

[Template:Main](/wiki/Template:Main) The ITIL-process Security Management[[5]](#cite_note-5)describes the structured fitting of information security in the management organization. It is based on the code of practice for *information security management system* (ISMS) now known as [ISO/IEC 27002](/wiki/ISO/IEC_27002).

A basic goal of security management is to ensure adequate [information security](/wiki/Information_security). The primary goal of information security, in turn, is to protect information assets against [risks](/wiki/Risk), and thus to maintain their value to the organization. This is commonly expressed in terms of ensuring their [confidentiality](/wiki/Information_security#Confidentiality), [integrity](/wiki/Information_security#Integrity) and [availability](/wiki/Information_security#Availability), along with related properties or goals such as [authenticity](/wiki/Information_security#Authenticity), [accountability](/wiki/Accountability), [non-repudiation](/wiki/Information_security#Non-repudiation) and reliability.

Mounting pressure for many organizations to structure their information security management systems in accordance with [ISO/IEC 27001](/wiki/ISO/IEC_27001) requires revision of the ITIL v2 security management volume, which culminated in the release of the 2007 edition.

### Supplier management[[edit](/index.php?title=(none)&action=edit&section=14)]

The purpose of supplier management is to obtain value for money from suppliers and contracts. It ensures that underpinning contracts and agreements align with business needs, [Service Level Agreements](/wiki/Service_Level_Agreement) and [Service Level Requirements](/wiki/Service_level_requirement). Supplier Management oversees process of identification of business needs, evaluation of suppliers, establishing contracts, their categorization, management and termination.

## Service transition[[edit](/index.php?title=(none)&action=edit&section=15)]

Service transition (ST), as described by the ITIL service transition volume,<ref name=service\_transition/> relates to the delivery of services required by a business into live/operational use, and often encompasses the "project" side of IT rather than [business as usual](/wiki/Wikt:business_as_usual) (BAU). This area also covers topics such as managing changes to the BAU environment.

List of ITIL processes in service transition:

1. Transition planning and support
2. [Change management](/wiki/Change_management_(ITSM))
3. Service asset and configuration management
4. [Release and deployment management](/wiki/Release_management)
5. Service validation and testing
6. [Change evaluation](/wiki/Change_management_(ITSM))
7. [Knowledge management](/wiki/Knowledge_management)

### Change management[[edit](/index.php?title=(none)&action=edit&section=16)]

[Template:Main](/wiki/Template:Main) Change management aims to ensure that standardised methods and procedures are used for efficient handling of all changes. A change is an event that results in a new status of one or more [configuration items](/wiki/Configuration_item) (CIs), and which is approved by management, is cost-effective, enhances business process changes (fixes) – all with a minimum risk to IT infrastructure.

The main aims of change management include:

* Minimal disruption of services
* Reduction in back-out activities
* Economic use of resources involved in the change

Common change management terminology includes:

* *Change*: the addition, modification or removal of CIs
* *Request For Change* (*RFC*) or, in older terminology, [*Change Request*](/wiki/Change_request) (*CR*): a form used to record details of a request for a change and is sent as an input to Change Management by the Change Requestor
* *ITIL v2 - Forward Schedule of Changes (FSC)*: schedule that contains details of all forthcoming Changes.
* *ITIL 2007 - Change Schedule (CS)*: schedule that contains details of all forthcoming Changes, and references historical data. Many people still refer to the known term FSC.

There are three types of changes: Standard Change,Normal Change,Urgent/Emergency Change

### Service asset and configuration management[[edit](/index.php?title=(none)&action=edit&section=17)]

Service asset and configuration management is primarily focused on maintaining information (i.e., configurations) about Configuration Items (i.e., assets) required to deliver an IT service, including their relationships. Configuration management is the management and traceability of every aspect of a configuration from beginning to end and it includes the following key process areas under its umbrella:

* Identification
* Planning
* Change control
* Change management
* Release management
* Maintenance

### Release and deployment management[[edit](/index.php?title=(none)&action=edit&section=18)]

[Release and deployment management](/wiki/Release_management) is used by the software migration team for platform-independent and automated distribution of software and hardware, including license controls across the entire IT infrastructure. Proper software and hardware control ensures the availability of licensed, tested, and version-certified software and hardware, which functions as intended when introduced into existing infrastructure. Quality control during the development and implementation of new hardware and software is also the responsibility of Release Management. This guarantees that all software meets the demands of the business processes. Release management utilizes [Definitive Media Library](/wiki/Definitive_Media_Library) for storage of software.

The goals of release management include:

* Planning the rollout of software
* Designing and implementing procedures for the distribution and installation of changes to IT systems
* Effectively communicating and managing expectations of the customer during the planning and rollout of new releases
* Controlling the distribution and installation of changes to IT systems

Release management focuses on the protection of the live environment and its services through the use of formal procedures and checks.

A Release consists of the new or changed software and/or hardware required to implement approved changes. *Release categories* include:

* Major software releases and major hardware upgrades, normally containing large amounts of new functionality, some of which may make intervening fixes to problems redundant. A major upgrade or release usually supersedes all preceding minor upgrades, releases and emergency fixes.
* Minor software releases and hardware upgrades, normally containing small enhancements and fixes, some of which may have already been issued as emergency fixes. A minor upgrade or release usually supersedes all preceding emergency fixes.
* Emergency software and hardware fixes, normally containing the corrections to a small number of known problems.

Releases can be divided based on the release unit into:

* Delta release: a release of only that part of the software which has been changed. For example, security patches.
* Full release: the entire software program is deployed—for example, a new version of an existing application.
* Packaged release: a combination of many changes—for example, an operating system image which also contains specific applications.

## Service operation[[edit](/index.php?title=(none)&action=edit&section=19)]

Service Operation (SO) aims to provide [best practice](/wiki/Best_practice) for achieving the delivery of agreed levels of services both to end-users and the customers (where "customers" refer to those individuals who pay for the service and negotiate the [SLAs](/wiki/Service-level_agreement)). Service operation, as described in the ITIL Service Operation volume,<ref name=service\_operation/> is the part of the [lifecycle](/wiki/Enterprise_life_cycle) where the services and value is actually directly delivered. Also the monitoring of problems and balance between service reliability and cost etc. are considered. The functions include technical management, application management, operations management and [service desk](/wiki/Service_desk) as well as, responsibilities for staff engaging in Service Operation.

### Processes[[edit](/index.php?title=(none)&action=edit&section=20)]

1. Event Management
2. [Access Management](/wiki/Access_Management)
3. [Request Fulfillment](/wiki/Request_Fulfillment)
4. [Problem Management](/wiki/Problem_Management)
5. [Incident Management](/wiki/Incident_Management)

### Functions[[edit](/index.php?title=(none)&action=edit&section=21)]

1. [Service Desk](/wiki/Service_Desk)
2. [Technical Management](/wiki/Technical_Management)
3. [Application Management](/wiki/Application_Management)
4. [IT Operations Management](/wiki/IT_Operations_Management)

#### Service desk[[edit](/index.php?title=(none)&action=edit&section=22)]

The *service desk* is one of four ITIL functions and is primarily associated with the Service Operation lifecycle stage. Tasks include handling incidents and requests, and providing an interface for other ITSM processes. Features include:

* single [point of contact](/wiki/Point_of_contact) (SPOC) and not necessarily the first point of contact (FPOC)
* single point of entry
* single point of exit
* easier for customers
* streamlined communication channel

Primary purposes of a service desk include:

* incident control: life-cycle management of all service requests
* communication: keeping a customer informed of progress and advising on workarounds

The service desk function can have various names, such as:

* [*Call center*](/wiki/Call_center): main emphasis on professionally handling large call volumes of telephone-based transactions
* [*Help desk*](/wiki/Help_desk): manage, co-ordinate and resolve incidents as quickly as possible at [primary support level](/wiki/Primary_support_level)
* *Service desk*: not only handles incidents, problems and questions but also provides an interface for other activities such as change requests, maintenance contracts, software licenses, service-level management, configuration management, availability management, financial management and IT services continuity management

The three *types* of structure for consideration:

* *Local service desk*: to meet local business needs – practical only until multiple locations requiring support services are involved
* *Central service desk*: for organizations having multiple locations – reduces operational costs[Template:Citation needed](/wiki/Template:Citation_needed) and improves usage of available resources
* *Virtual service desk*: for organizations having multi-country locations – can be situated and accessed from anywhere in the world due to advances[Template:When](/wiki/Template:When) in network performance and telecommunications, reducing operational costs[Template:Citation needed](/wiki/Template:Citation_needed) and improving usage of available resources

#### Application management[[edit](/index.php?title=(none)&action=edit&section=23)]

ITIL *application management*[[6]](#cite_note-6) encompasses a set of best practices proposed to improve the overall quality of IT software development and support through the life-cycle of software development projects, with particular attention to gathering and defining requirements that meet business objectives.

[Software asset management](/wiki/Software_asset_management) (SAM) is a primary topic of ITILv2 and is closely associated with the ITIL Application Management function. SAM is the practice of integrating people, processes, and technology to allow software licenses and usage to be systematically tracked, evaluated, and managed. The goal of SAM is to reduce IT expenditures, human resource overhead and risks inherent in owning and managing software assets.

SAM practices include:

* maintaining software license compliance
* tracking inventory and software asset use
* maintaining standard policies and procedures surrounding definition, deployment, configuration, use, and retirement of software assets and the [definitive software library](/wiki/Definitive_software_library).

SAM represents the software component of IT asset management. This includes hardware asset management because effective hardware inventory controls are critical to efforts to control software. This means overseeing software and hardware that constitute an organization's computers and [network](/wiki/Computer_network).

#### IT Operations management[[edit](/index.php?title=(none)&action=edit&section=24)]

Refer to [ICT infrastructure management](/wiki/#ICT_infrastructure_management) for more details.

#### Technical management[[edit](/index.php?title=(none)&action=edit&section=25)]

Refer to [ICT infrastructure management](/wiki/#ICT_infrastructure_management) for more details.

### Event management[[edit](/index.php?title=(none)&action=edit&section=26)]

An event may indicate that something is not functioning correctly, leading to an incident being logged. Events may also indicate normal activity, or a need for routine intervention such as changing a tape. Event management depends on monitoring, but it is different. Event management generates and detects notifications, while monitoring checks the status of components even when no events are occurring. Events may be detected by a CI sending a message, or by a management tool polling the CI. After an event has been detected it may lead to an Incident, Problem or Change, or it may simply be logged in case the information is needed. Response to an event may be automated or may require manual intervention. If actions are needed then a trigger, such as an SMS message or an incident being automatically logged, can alert support staff.

### Incident management[[edit](/index.php?title=(none)&action=edit&section=27)]

[Template:Main](/wiki/Template:Main) Incident management aims to restore normal service operation as quickly as possible and minimise the adverse effect on business operations, thus ensuring that the best possible levels of service quality and availability are maintained. 'Normal service operation' is defined here as service operation within service-level agreement ([SLA](/wiki/Service-level_agreement)) limits.

An incident is defined as:

2007: An unplanned interruption to an IT service or a reduction in the quality of an IT service. Failure of a configuration item that has not yet impacted service is also an incident. For example, failure of one disk from a mirror set.

V2: An event which is not part of the standard operation of a service and which causes or may cause disruption to or a reduction in the quality of services and customer productivity.

The objective of incident management is to restore normal operations as quickly as possible with the least possible impact on either the business or the user, at a cost-effective price. The transformation between event-to-incident is the critical junction where [Application Performance Management](/wiki/Application_Performance_Management) (APM) and ITIL come together to provide tangible value back to the business.[[7]](#cite_note-7)

### Request fulfillment[[edit](/index.php?title=(none)&action=edit&section=28)]

Request fulfillment (or request management) focuses on fulfilling Service Requests, which are often minor (standard) *changes* (e.g., requests to change a password) or requests for information.

The term "standard change" means pre-approved, repeatable, pre-defined, low risk changes. If the change does not meet these criteria then it is not a standard change and should be defined as a request for change.

### Problem management[[edit](/index.php?title=(none)&action=edit&section=29)]

[Template:Main](/wiki/Template:Main) Problem management aims to resolve the root causes of incidents and thus to minimise the adverse impact of incidents caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors. A "problem" in this context is the unknown underlying cause of one or more incidents, and a 'known error' is a problem that is successfully diagnosed and for which either a [work-around](/wiki/Work-around) or a permanent resolution has been identified. The CCTA (Central Computer and Telecommunications Agency) defines problems and known errors as follows:

A *problem* is a condition often identified as a result of multiple incidents that exhibit common symptoms. Problems can also be identified from a single significant incident, indicative of a single error, for which the cause is unknown, but for which the impact is significant.

A *known error* is a condition identified by successful diagnosis of the root cause of a problem, and the subsequent development of a work-around.

*Problem management* differs from *incident management*. *Problem management* aims primarily to find and resolve the root cause of a problem and thus prevent further incidents; the purpose of *incident management* is to return the service to normal level as soon as possible, with smallest possible business impact.

The problem-management process reduces the number and severity of incidents and problems on the business, and documents the details of the problem and resolution to be available for the first-line and second-line of the help desk. The proactive process identifies and resolves problems before incidents occur. Such processes include:

* Trend analysis
* Targeting support action
* Providing information to the organization

The *error control process* iteratively diagnoses known errors until they are eliminated by the successful implementation of a change under the control of the Change Management process.

The *problem control process* aims to handle problems in an efficient way. Problem control identifies the root cause of incidents and reports it to the service desk. Other activities are:

* Problem identification and recording
* Problem classification
* Problem investigation and diagnosis

#### Root-cause analysis[[edit](/index.php?title=(none)&action=edit&section=30)]

Root-cause analysis is a formal problem-solving process and a critical component of Problem Management. Once a problem (or potential problem) has been identified, the root cause analysis process begins. The purpose of a root cause analysis is two-fold:

1. develop a thorough understanding of the problem and its causes
2. identify corrective/preventive actions that will reduce the risk of recurrence to an acceptable level

Classic root-cause analysis methods include the [5-whys](/wiki/5_Whys) and [*Ishikawa diagram*](/wiki/Ishikawa_diagram) or [fishbone diagram](/wiki/Fishbone_diagram). Others have since developed more advanced root cause analysis methodologies, some with corresponding software applications.

Benefits from employing a standard, structured root-cause analysis methodology include:

* common terms, language, and structure with respect to root cause analysis
* problem identification, including actual and potential impact
* identification of the problem's causes, their interactions, and the supporting evidence
* identification of corrective/preventive actions ([CAPA](/wiki/Corrective_and_preventive_action)) that will prevent recurrence of the problem
* development of a knowledge base which others can use as a resource

### Identity management[[edit](/index.php?title=(none)&action=edit&section=31)]

[Template:Main](/wiki/Template:Main) [Identity management](/wiki/Identity_management) (IdM) less commonly called [Access and Identity Management](/wiki/Access_and_Identity_Management) (AIM) as a process focuses on granting authorised users the right to use a service, while preventing access to non-authorised users. Certain identity management processes executes policies defined in [Security Management](/wiki/ITIL#Security_management).

## Continual service improvement (CSI)[[edit](/index.php?title=(none)&action=edit&section=32)]

Continual service improvement, defined in the ITIL continual service improvement volume,<ref name=csi/> aims to align and realign IT services to changing business needs by identifying and implementing improvements to the IT services that support the business processes. It incorporates many of the same concepts articulated in the [Deming Cycle](/wiki/Deming_Cycle) of *Plan-Do-Check-Act*. The perspective of CSI on improvement is the business perspective of service quality, even though CSI aims to improve process effectiveness, [efficiency](/wiki/Economic_efficiency) and cost effectiveness of the IT processes through the whole lifecycle. To manage improvement, CSI should clearly define what should be controlled and measured.

CSI needs upfront planning, training and awareness, ongoing scheduling, roles created, ownership assigned,and activities identified to be successful. CSI must be planned and scheduled as process with defined activities, inputs, outputs, roles and reporting. Continual Service Improvement and [Application Performance Management](/wiki/Application_Performance_Management) (APM) are two sides of the same coin. They both focus on improvement with APM tying together *service design*, *service transition*, and *service operation* which in turn helps raise the bar of operational excellence for IT.[[8]](#cite_note-8) Improvement initiatives typically follow a seven-step process:

1. Identify the strategy for improvement
2. Define what you will measure
3. Gather the data
4. Process the data
5. Analyse the information and data
6. Present and use the information
7. Implement improvement

## Overview of ITIL v2[[edit](/index.php?title=(none)&action=edit&section=33)]

The eight ITIL version 2 books and their disciplines are:

The IT service management sets

1. [Service Support](/wiki/Information_Technology_Infrastructure_Library#Service_support)

2. [Service Delivery](/wiki/Information_Technology_Infrastructure_Library#Service_delivery)

Other operational guidance

3. [ICT infrastructure management](/wiki/ICT_infrastructure)

4. [Security management](/wiki/Information_Technology_Infrastructure_Library#Security_management)

5. [Application management](/wiki/Information_Technology_Infrastructure_Library#Application_management)

6. [Software asset management](/wiki/Information_Technology_Infrastructure_Library#Software_asset_management)

To assist with the implementation of ITIL practices a further book was published (Apr 9, 2002) providing guidance on implementation (mainly of Service Management):

7. [Planning to implement service management](/wiki/Information_Technology_Infrastructure_Library#Planning_to_implement_service_management)

And this has more recently (Jan 26, 2006) been supplemented with guidelines for smaller IT units, not included in the original eight publications:

8. ITIL [small-scale implementation](/wiki/Information_Technology_Infrastructure_Library#Small-scale_implementation)

### Service support[[edit](/index.php?title=(none)&action=edit&section=34)]

The Service Support[[9]](#cite_note-9)ITIL discipline focuses on the *User* of the [ICT](/wiki/Information_and_communication_technologies) services and is primarily concerned with ensuring that they have access to the appropriate services to support the business functions.

To a business, customers and users are the entry point to the process model. They get involved in service support by:

* Asking for changes
* Needing communication, updates
* Having difficulties, queries
* Real process delivery

The service desk functions are the single contact-point for [end-users'](/wiki/End-user) incidents. Its first function is always to document ("create") an incident. If there is a direct solution, it attempts to resolve the incident at the first level. If the service desk cannot solve the incident then it is passed to a 2nd/3rd level group within the incident management system. Incidents can initiate a chain of processes: incident management, [problem management](/wiki/Problem_management), [change management](/wiki/Change_management), [release management](/wiki/Release_management) and [configuration management](/wiki/Configuration_management). This chain of processes is tracked using the [configuration management database](/wiki/Configuration_management_database) ([CMDB](/wiki/Configuration_management_database)), - ITIL refers to configuration management system ([CMS](/wiki/Configuration_management_system)), which records each process, and creates output documents for traceability (quality management). Note - CMDB/CMS does not have to be a single database. The solution can be Federated.

### Service delivery[[edit](/index.php?title=(none)&action=edit&section=35)]

The service delivery[[10]](#cite_note-10)discipline concentrates on the proactive services the ICT must deliver to provide adequate support to business users. It focuses on the business as the *customer* of the ICT services (compare with: [service support](/wiki/#Service_support)). The discipline consisted of the following processes:

* [Service level](/wiki/Service_level) management
* [Capacity management](/wiki/Capacity_management)
* IT service continuity management
* [Availability](/wiki/Availability) management
* Financial management

### ICT infrastructure management[[edit](/index.php?title=(none)&action=edit&section=36)]

[Information and Communication Technology](/wiki/Information_and_Communication_Technology) (ICT) management[[11]](#cite_note-11) processes recommend best practice for requirements analysis, planning, design, deployment and ongoing operations management and technical support of an ICT infrastructure.

The infrastructure management processes describe those processes within ITIL that directly relate to the ICT equipment and software that is involved in providing ICT services to customers.

* ICT design and planning
* ICT deployment
* ICT operations
* ICT technical support

These disciplines are less well understood than those of service management and therefore often some of their content is believed to be covered 'by implication' in service management disciplines.

#### ICT design and planning[[edit](/index.php?title=(none)&action=edit&section=37)]

ICT design and planning provides a framework and approach for the strategic and technical design and planning of ICT infrastructures. It includes the necessary combination of business (and overall IS) strategy, with technical design and architecture. ICT design and planning drives both the procurement of new ICT solutions through the production of statements of requirement ("SOR") and invitations to [tender](/wiki/Call_for_bids) ("ITT") and is responsible for the initiation and management of ICT Programmes for strategic business change. Key outputs from design and planning are:

* ICT strategies, policies and plans
* the ICT overall architecture & management architecture
* feasibility studies, ITTs and SORs
* business cases

#### ICT deployment management[[edit](/index.php?title=(none)&action=edit&section=38)]

ICT deployment provides a framework for the successful management of design, build, test and roll-out (deploy) projects within an overall ICT [programme](/wiki/Program_management). It includes many [project management](/wiki/Project_management) disciplines in common with [PRINCE2](/wiki/PRINCE2), but has a broader focus to include the necessary integration of release management and both functional and non functional testing.

#### ICT operations management[[edit](/index.php?title=(none)&action=edit&section=39)]

ICT operations management provides the day-to-day technical supervision of the ICT infrastructure. Often confused with the role of incident management from service support, operations has a more technical bias and is concerned not solely with incidents reported by users, but with events generated by or recorded by the infrastructure. ICT operations may often work closely alongside incident management and the service desk, which are not-necessarily technical, to provide an 'operations bridge'. Operations, however should primarily work from documented processes and procedures and should be concerned with a number of specific sub-processes, such as: output management, job scheduling, backup and restore, network monitoring/management, system monitoring/management, database monitoring/management storage monitoring/management. Operations are responsible for the following:

* a stable, secure ICT infrastructure
* a current, up to date operational documentation library ("ODL")
* a log of all operational events
* maintenance of operational monitoring and management tools.
* operational scripts
* operational procedures

[thumb|ITIL Framework](/wiki/File:ItilstructWiki.png)

#### ICT technical support[[edit](/index.php?title=(none)&action=edit&section=40)]

ICT technical support is the specialist technical function for infrastructure within ICT. Primarily as a support to other processes, both in infrastructure management and service management, technical support provides a number of specialist functions: research and evaluation, market intelligence (particularly for design and planning and capacity management), proof of concept and pilot engineering, specialist technical expertise (particularly to operations and problem management), creation of documentation (perhaps for the operational documentation library or known error database). There are different levels of support under the ITIL structure, these being primary support level, [secondary support level](/wiki/Secondary_support_level) and [tertiary support level](/wiki/Tertiary_support_level), higher-level administrators being responsible for support at primary level.

The Known Error Database (KEDB) database contains all known error records. This database is created by problem management and used by incident management and problem management, and as part of service knowledge management systems.[[12]](#cite_note-12)

### Planning to implement service management[[edit](/index.php?title=(none)&action=edit&section=41)]

The ITIL discipline – planning to implement service management[[13]](#cite_note-13)attempts to provide practitioners with a framework for the alignment of business needs and IT provision requirements. The processes and approaches incorporated within the guidelines suggest the development of a continuous service improvement program (CSIP) as the basis for implementing other ITIL disciplines as projects within a controlled program of work. Planning to implement service management focuses mainly on the service management processes, but also applies generically to other ITIL disciplines. Components include:

* creating vision
* analysing organization
* [setting goals](/wiki/Goal_setting)
* implementing IT service management

### Small-scale implementation[[edit](/index.php?title=(none)&action=edit&section=42)]

ITIL *Small-scale implementation*[[14]](#cite_note-14) provides an approach to ITIL framework implementation for smaller IT units or departments. It is primarily an auxiliary work that covers many of the same best practice guidelines as *planning to implement service management, service support, and service delivery* but provides additional guidance on the combination of roles and responsibilities, and avoiding conflict between ITIL priorities. The typical IT Organizational structure that maps to ITIL framework. [thumb|IT organizational Structure](/wiki/File:ITOrgWiki.png)

## Related frameworks[[edit](/index.php?title=(none)&action=edit&section=43)]

A number of frameworks exist in the field of IT Service Management alongside ITIL.

### Descendants[[edit](/index.php?title=(none)&action=edit&section=44)]

#### Microsoft Operations Framework[[edit](/index.php?title=(none)&action=edit&section=45)]

The [Microsoft Operations Framework](/wiki/Microsoft_Operations_Framework) (MOF) is based on ITIL v2. While ITIL deliberately aims to be platform-agnostic, MOF is designed by Microsoft to provide a common management framework for *its* products. Microsoft has mapped MOF to ITIL as part of their documentation of the framework.[[15]](#cite_note-15)

#### FITS[[edit](/index.php?title=(none)&action=edit&section=46)]

The British Educational Communications and Technology Agency ([BECTA](/wiki/BECTA)) used ITIL as the basis for their development of [Framework for ICT Technical Support](http://www.thefitsfoundation.org) (FITS). Their aim was to develop a framework appropriate for British schools, which often have very small IT departments. FITS became independent from [BECTA](/wiki/BECTA) in 2009 and is now maintained and supported by The FITS Foundation. FITS is now used in excess of a thousand schools in the UK, Australia and Norway as the standard for ICT Service Management in the Education sector (Video: [What people are saying](http://www.youtube.com/watch?v=ast-ZPLaMkU&feature=youtu.be))

### Other frameworks[[edit](/index.php?title=(none)&action=edit&section=47)]

The process framework of the [ISO/IEC 20000](/wiki/ISO/IEC_20000) standard (previously BS 15000) is largely equivalent that of the *Service Support* and *Service Delivery* parts of ITIL Version 2.[[16]](#cite_note-16) While it is not possible for an organization to be certified as being ITIL compliant, certification of an organization is available for ISO/IEC 20000.[[17]](#cite_note-17) [COBIT](/wiki/COBIT) is an [IT governance framework](/wiki/Corporate_governance_of_information_technology) and supporting toolset developed by [ISACA](/wiki/ISACA). [ISACA](/wiki/ISACA) view ITIL as being complementary to COBIT. They see COBIT as providing a governance and assurance role while ITIL providing guidance for service management.[[18]](#cite_note-18) The [Business Process Framework (eTOM)](/wiki/Business_Process_Framework_(eTOM)) published by the TeleManagement Forum offers a framework aimed at telecommunications service providers. In a joined effort, [TM Forum](/wiki/TM_Forum) and [itSMF](/wiki/ItSMF) developed an Application Note to eTOM (GB921) that shows how the two frameworks can be mapped to each other. It addresses how eTom process elements and flows can be used to support the processes identified in ITIL.[[19]](#cite_note-19)[[20]](#cite_note-20) [IBM Tivoli Unified Process (ITUP)](/wiki/IBM_Tivoli_Unified_Process_(ITUP)) is aligned with ITIL, but is presented as a complete, integrated process model compatible with IBM's products.

[FitSM](/wiki/FitSM) [[21]](#cite_note-21) is a standard for lightweight service management. Its process framework is quite similar to that of ISO/IEC 20000 and the *Service Support* and *Service Delivery* parts of ITIL version 2, but adopts *Service Portfolio Management* from later ITIL versions. FitSM contains several parts, including samples and templates for core ITSM documents, that are published under [Creative Common licenses](/wiki/Creative_Commons_license).

## Certification[[edit](/index.php?title=(none)&action=edit&section=48)]

### Individuals[[edit](/index.php?title=(none)&action=edit&section=49)]

[thumb|An ITILv2 Foundation Badge.](/wiki/File:Wearer_of_an_ITIL_Foundation_Certificate_pin.jpg) The certification scheme differs between ITIL v2 and ITIL 2007/2011, and bridge examinations (now retired) allowed owners of v2 certificates to transfer to the new program.[Template:Citation needed](/wiki/Template:Citation_needed) **ITIL v2** offers three certification levels: *Foundation*, *Practitioner* and *Manager*. These were progressively discontinued in favor of the new scheme introduced along with the publication of the 2007 Edition. ITIL certification levels are now: *Foundation*, *Intermediate*, *Expert* and *Master*. In addition, the single-process practitioner certifications that were offered by OGC for version 2 have now been replaced and the offering expanded by what are known as complementary certifications.[[22]](#cite_note-22) The ITIL certification scheme now offers a modular approach. Each qualification is assigned a credit value; so that upon successful completion of the module, the candidate is rewarded with both a certification and a number of credits. At the lowest level – Foundation – candidates are awarded a certification and two credits. At the Intermediate level, a total of additional 15 credits have to be earned. These credits may be accumulated in either a "Lifecycle" stream<ref group=note>The Lifecycle stream follows the ITIL core volumes; there are therefore 5 modules also called *Service Strategy*, *Service Design*, *Service Transition*, *Service Operation* and *Continual Service Improvement*.</ref> or a "Capability" stream;<ref group=note>The Capability stream is more focused on process activities; the 4 modules available in 2013 are *Operational support and analysis* (OSA), *Service offerings and agreements* (SOA), *Planning protection and optimization* (PPO) and *Release, control and validation* (RCV).</ref> or combination thereof. Each Lifecycle module and exam is three credits. Each Capability module and corresponding exam is four credits. A candidate wanting to achieve the Expert level will have, among other requirements, to gain the required number of credits (22). That is accomplished with two from Foundations, then at least 15 from Intermediate, and finally five credits from the "Managing Across the Lifecycle" exam. Together, the total of 22 earned credits allows a person to request designation as an ITIL Expert. Advancing from the expert to the master level does not require additional credits, but does require at least five years of IT domain work experience and an extensive usage of ITIL practices.[[23]](#cite_note-23) The complementary certifications also have point values, ranging from 0.5 to 1.5 credits, which can be applied towards ITIL Expert certification. However, only a maximum of six credits from complementary certifications can be applied towards the Expert certification.[[24]](#cite_note-24) The ITIL Certification Management Board (ICMB) manages ITIL certification. The Board includes representatives from interested parties within the community around the world. Members of the Board include (though are not limited to) representatives from the UK [Office of Government Commerce](/wiki/Office_of_Government_Commerce) (OGC), APM Group (APMG), [The Stationery Office](/wiki/The_Stationery_Office) (TSO), ITIL Examination Panel, Examination Institutes (EIs) and the [IT Service Management Forum International](/wiki/ItSMF) (*it*SMF) as the recognised user group.[[25]](#cite_note-25) Since the early 1990s, EXIN and ISEB had been setting up the ITIL based certification program, developing and providing ITIL exams at three different levels: Foundation, Practitioner and Manager. EXIN<ref name=exin>[Template:Cite web](/wiki/Template:Cite_web)</ref> and BCS/ISEB[[26]](#cite_note-26) (the British Computer Society) had from that time onwards been the only two examination providers in the world to develop formally acknowledged ITIL certifications, provide ITIL exams and accredit ITIL training providers worldwide. These rights were obtained from OGC, the British government institution and owner of the ITIL trademark.[Template:Citation needed](/wiki/Template:Citation_needed) OGC signed over the management of the ITIL trademark and the accreditation of examination providers to APM Group in 2006. Now, after signing a contract with EXIN,<ref name=exin/> BCS/ISEB, Loyalist Certification Services <http://www.loyalistexams.com>,[PeopleCert Group](http://www.peoplecert.org) and other certification bodies, APM Group has accredited them as official examination bodies, to offer ITIL exams and accredit ITIL training providers.[Template:Citation needed](/wiki/Template:Citation_needed)

On July 20, 2006, the OGC signed a contract with the [APM Group](http://www.apmgroupltd.com/) to become its commercial partner for ITIL accreditation from January 1, 2007.[[27]](#cite_note-27) APMG manage the ITIL Version 3 exams. APMG maintains a voluntary register of ITIL certified practitioners at their Successful Candidate Register.[[28]](#cite_note-28)