ITIL is published in a series of books, each of which covers an IT management topic. The names ITIL and IT Infrastructure Library are registered trademarks of the United Kingdom's Office of Government Commerce (OGC). ITIL gives a detailed description of a number of important IT practices with comprehensive checklists, tasks and procedures that can be tailored to any IT organization.

### Certification

ITIL Certifications are managed by the ITIL Certification Management Board (ICMB). The Board includes representatives from all interested parties within the community from around the world. Members of the Board include (though are not limited to) representatives from the UK Office of Government Commerce (OGC), APM Group (APMG), The Stationery Office (TSO), V3 Examination Panel, Examination Institutes (EIs) and the IT Service Management Forum International (iSMF) as the recognized user group.\(^1\)

On July 20, 2006, the OGC signed a contract with the APM Group to be its commercial partner for ITIL accreditation from January 1, 2007.\(^2\)

APMG manage the ITIL Version 3 exams and award qualifications at Foundation, Intermediate and Expert level (with a new Masters level under development).

APMG maintains a voluntary register of ITIL Version 3-certified practitioners at their Successful Candidate Register. A voluntary registry of ITIL Version 2-certified practitioners is operated by the ITIL Certification Register.
Outside of ITIL, other IT Service Management approaches and frameworks exist, including the Support Service Management (SSM), IT Service Management (ITSM), and the Capability Maturity Model (CMM/CMMI), and is often linked with Dynamic Systems Development Method (DSDM). The combination of the ISO/IEC 20000 standard and the Capability Maturity Model (CMM/CMMI), is often linked with Dynamic Systems Development Method (DSDM), the Capability Maturity Model (CMM/CMMI), and is often linked with Dynamic Systems Development Method (DSDM). It is an international standard covering the Information Services Procurement Library, the Application Services Library (ASL), the Information Services Procurement Library (ISPL), and the Application Services Library (ASL). It is considered essential ITIL.

ITIL History

Precursors

The raison d'être for building the library was rooted in the fact that the Central Computer and Telecommunications Agency (CCTA) Procurement had been buying Mainframes and Minis from IBM/DEC/HP Sperry Univac et al for decades. Maintenance and on site care was usually outsourced to the Mainframe and Mini support teams - who typically just replaced dumb terminals for users. Support calls were answered on site by low level vendor engineers doing swap outs of dumb terminals. The CCTA looked to stem their budget and started buying PCs however found that users had local hardware and software (MS DOS and Dr.DOS) issues. Government departments had to start their own IT Departments, and turned to the CCTA for advice and guidance. Peter Skinner and the CCTA procurement department approached vendors and PC/Network resellers for advice which was freely given and latterly developed. The reason that there were 6 books originally (and not one big book) was that Government departments came in all sizes and may have just wanted a single element from one of the books (i.e. how to start and man a help desk) and not want to buy the complete suite (hence Library).

Many of the concepts did not originate within the original UK Government's Central Computer and Telecommunications Agency (CCTA) project to develop ITIL. According to IBM:

"The primary author of the IBM yellow books was Edward A. Van Schaik, who compiled them into the 1985 book A Management System for Information Systems. These widely accepted "yellow books,"... were key inputs to the original set of ITIL books."[^2]

The publications were retitled primarily as a result of the desire (by Roy Dibble of CCTA) that the publications be seen as guidance and not as a formal method and as a result of growing interest from outside of the UK Government.

During the late 1980s the CCTA was under sustained attack, both from IT companies who wanted to take over the central Government consultancy service it provided and from other Government departments who wanted to break free of its oversight.[^citation needed] Eventually CCTA succumbed and the concept of a central driving IT authority for the UK Government was lost. This meant that adoption of CCTA guidance such as ITIL was delayed, as various other departments fought to take over new responsibilities.

In some cases this guidance was lost permanently. The CCTA IT Security and Privacy group, for instance, provided the CCTA IT Security Library input to GITMM, but when CCTA was broken up the security service appropriated this work and suppressed it as part of their turf war over security responsibilities.

Though ITIL was developed during the 1980s, it was not widely adopted until the mid 1990s for the reasons mentioned above. This wider adoption and awareness has led to a number of standards, including ISO/IEC 20000 which is an international standard covering the IT Service Management elements of ITIL. ITIL is often considered alongside other best practice frameworks such as the Information Services Procurement Library (ISPL), the Application Services Library (ASL), the Dynamic Systems Development Method (DSDM), and the Capability Maturity Model (CMM/CMMI), and is often linked with IT governance through Control Objectives for Information and related Technology (COBIT).

In December 2005, the OGC issued notice of an ITIL refresh[^9], commonly known as ITIL v3, which became available in May 2007. ITIL v3 initially includes five core texts:

1. Service Strategy
2. Service Design
3. Service Transition
4. Service Operation
5. Continual Service Improvement

These publications update much of the current v2 and extend the scope of ITIL in the domain of service management.

ITIL alternatives

ITIL Service Management as a concept is related but not equivalent to ITIL which, in Version 2, contained a subsection specifically entitled IT Service Management (ITSM). (The five volumes of version 3 have no such demarcated subsection). The combination of the Service Support and Service Delivery volumes are generally equivalent to the scope of the ISO/IEC 20000 standard (previously BS 15000).

Outside of ITIL, other IT Service Management approaches and frameworks exist, including the Enterprise Computing Institute's library covering general issues of large scale IT management, including various Service Management subjects. COBIT is perceived as an audit framework but the supporting body of knowledge (such as COBIT's books Control Practices, IT Assurance...
The design of IT services conforming to best practice, and including design of Service Design responsibilities of staff engaging in service strategy.

Service Strategy

Service strategy is shown at the core of the ITIL v3.1 lifecycle but cannot exist in isolation to the other parts of the IT structure. It encompasses a framework to build best practice in developing a long term service strategy. It covers many topics including: general strategy, competition and market space, service provider types, service management as a strategic asset, organization design and development, process activities, financial management, service portfolio management, demand management, and key roles and responsibilities of staff engaging in service strategy.

Service Design

The design of IT services conforming to best practice, and including design of architecture, processes, policies, documentation, and allowing
for future business requirements. This also encompasses topics such as Service Design Package (SDP), service catalog management, service level management, designing for capacity management, IT service continuity, Information Security, supplier management, and key roles and responsibilities for staff engaging in service design.

**Service Transition**
Service transition relates to the delivery of services required by the business into live/operational use, and often encompasses the "project" side of IT rather than "BAU" (Business As Usual). This area also covers topics such as managing changes to the "BAU" environment. Topics include Service Asset and Configuration Management, Transition Planning and Support, Release and deployment management, Change Management, Knowledge Management, as well as the key roles of staff engaging in Service Transition.

**Service Operation**
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). Service Operations is the part of the lifecycle where the services and value is actually directly delivered. Also the monitoring of problems and balance between service reliability and cost etc are considered. Topics include balancing conflicting goals (e.g. reliability v cost etc), Event management, incident management, problem management, request fulfillment, asset management, service desk, technical and application management, as well as key roles and responsibilities for staff engaging in Service Operation.

**Continual Service Improvement (CSI)**

**Short Description**
Aligning and realigning IT services to changing business needs (because standstill implies decline).

The goal of Continual Service Improvement is to align and realign IT Services to changing business needs by identifying and implementing improvements to the IT services that support the Business Processes. The perspective of CSI on improvement is the business perspective of service quality, even though CSI aims to improve process effectiveness, efficiency and cost effectiveness of the IT processes through the whole lifecycle. In order to manage improvement, CSI should clearly define what should be controlled and measured.

CSI needs to be treated just like any other service practice. There needs to be upfront planning, training and awareness, ongoing scheduling, roles created, ownership assigned, and activities identified in order to be successful. CSI must be planned and scheduled as process with defined activities, inputs, outputs, roles and reporting.

**Long Description**
Once an organization has gone through the process of identifying what its Services are, as well as developing and implementing the IT Service Management (ITSM) processes to enable those services, many incorrectly believe that the hard work is done. The real work is only just beginning. How do organizations get buy-in for using the new processes? How do organizations measure, report and use the data to improve not only the new processes but to continually improve the Services being provided? This requires a conscious decision to adopt CSI with clearly defined goals, documented procedures, inputs, outputs and identified roles and responsibilities. To be successful, CSI must be embedded within each organization's culture.

The Service Lifecycle is a comprehensive approach to Service Management: seeking to understand its structure, the interconnections between all its components, and how changes in any area will affect the whole system and its constituent parts over time. It is an organizing framework designed for sustainable performance.

The Service Lifecycle can be viewed in a graphical manner, where it is easy to demonstrate the value provided, both in terms of "business contribution" and "profit". The **business contribution** is the ability for an IT organization to support a business process, managing the IT service at the requested performance. The **profit** is the ability to manage cost of service in relations to the business revenue.

The Service Lifecycle can be viewed as a phased life cycle, where the phases are:

- Defining strategy for the IT Service Management (Service Strategy or SS)
- Designing the services to support the strategy (Service Design or SD)
- Implement the services in order to meet the designed requirements (Service Transition or ST)
- Support the services managing the operational activities (Service Operation or SO)

The interaction between phases are managed through the Continual Service Improvement approach, which is responsible for measuring and improving service and process maturity level. After comparison of all phases, a service period is concluded and another service period begins.

The Continual Service Improvement phase is involved during all phases of the service lifecycle. It is responsible for measuring the service and the processes, (Service Measurement), and to document the results (Service Reporting) in order to improve the services quality and the processes maturity (Service Improvement). These improvements will be implemented in the next period of Service Lifecycle, starting again with Service Strategy, and following with Service Design and Transition, the Service Operation phase of course continue to manages operations during all service periods.

With the evolution of service periods, the "effort" for each phase will be reduced concerning the strategic and tactical phases (SS, SD and ST), here the SO phase is optimized and takes the primary role. At each cycle of the service (service period) the service will be improved with results of increasing of the value of business and maximizing of profits.

In terms of Business Contribution, the IT Service begins to be valuable when in the first step the Service Transition starts.

In terms of profits, the major investments are required with the big implementation projects (ST), when the transition is complete and the Operations start, the service begins to support business process and the new revenues balance the costs. After some periods of service optimization the "Profit & Loss" start to be profitable and reach the "break even point".

After a number of periods (depending on the complexity of the service and the flexibility of the business), the business contribution and the profit will be stabilized, which means that the IT organization has reached the right level of maturity in managing processes and the service has reached the right level of performance in meeting the service level requirements.
Service Support
The Service Support ITIL discipline is focused on the User of the ICT 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.

The service desk is the single contact point for the customers to record their problems. It will try to resolve it, if there is a direct solution. If not, it will create an incident. Incidents initiate a chain of processes: Incident Management, Problem Management, Change Management, Release Management and Configuration Management (see following sections for details). This chain of processes is tracked using the Configuration Management Database (CMDB), which records each process, and creates output documents for traceability (Quality Management).

Service Desk / Service Request Management
Tasks include handling incidents and requests, and providing an interface for other ITSM processes.

- Single Point of Contact (SPOC) and not necessarily the First Point of Contact (FPOC)
- There is a single point of entry and exit
- Easier for Customers
- Data Integrity
- Communication channel is streamlined

The primary functions of the Service Desk are:

- Incident Control: life cycle management of all Service Requests
- Communication: keeping the customer informed of progress and advising on workarounds

The Service Desk function is known under various names.

- Call Center: main emphasis on professionally handling large call volumes of telephone-based transactions
- Help Desk: manage, co-ordinate and resolve incidents as quickly as possible
- 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 that can be considered are:

- Local Service Desk: to meet local business needs - is practical only until multiple locations requiring support services are involved
- Central Service Desk: for organizations having multi-country locations - can be situated and accessed from anywhere in the world due to advances in network performance and telecommunications, reducing operational costs and improving usage of available resources
- Virtual Service Desk: for organizations having multiple locations - reduces operational costs and improves usage of available resources

Incident Management
The goal of Incident Management is to restore normal service operation as quickly as possible and minimize 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) limits.

Main article: Incident Management (ITSM)

Problem Management
The goal of ‘Problem Management’ is to resolve the root cause of incidents and thus to minimize the adverse impact of incidents and problems on business that are caused by errors within the IT infrastructure, and to prevent recurrence of incidents related to these errors. A ‘problem’ is an 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 or a permanent resolution has been identified. The CCTA 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 is different from incident management. The principal purpose of problem management is to find and resolve the root cause of a problem and prevention of 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 is intended to reduce the number and severity of incidents and problems on the business, and report it in documentation to be available for the first-line and second line of the help desk. The proactive process identifies and resolves problems before incidents occur. These activities are:

- Trend analysis;
- Targeting support action;
- Providing information to the organization.

The Error Control Process is an iterative process to diagnose 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.

The standard technique for identifying the root cause of a problem is to use an Ishikawa diagram, also referred to as a cause-and-effect diagram, tree diagram, or fishbone diagram. An Ishikawa diagram is typically the result of a brainstorming session in which members of a group offer ideas to improve a product. For problem-solving, the goal will be to find the cause and effect of the problem.

Ishikawa diagrams can be defined in a meta-model.

First there is the main subject, which is the backbone of the diagram that we are trying to solve or improve. The main subject is derived from a cause. The relationship between a cause and an effect is a double relation: an effect is a result of a cause, and the cause is the root of an effect. But there is just one effect for several causes and one cause for several effects.

Change Management

The goal of Change Management is to ensure that standardized methods and procedures are used for efficient handling of all changes,

Main article: Change Management (ITSM)

A change is “an event that results in a new status of one or more configuration items (CI’s)” approved by management, cost effective, enhances business process changes (fixes) - with a minimum risk to IT infrastructure.

The main aims of Change Management are:

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

Change Management Terminology

- Change: the addition, modification or removal of CIs
- Request for Change (RFC): form used to record details of a request for a change and is sent as an input to Change Management by the Change Requestor
- Forward Schedule of Changes (FSC): schedule that contains details of all the forthcoming Changes

Release Management

Release Management is used 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 will function as intended when introduced into the 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. The goals of release management are:

- Plan the rollout of software
- Design and implement procedures for the distribution and installation of changes to IT systems
- Effectively communicate and manage expectations of the customer during the planning and rollout of new releases
- Control the distribution and installation of changes to IT systems

The focus of release management is the protection of the live environment and its services through the use of formal procedures and checks.

Release Categories

A Release consists of the new or changed software and/or hardware required to implement approved changes

Releases are categorized as:

- Major software releases and 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: means that the entire software program will be deployed. For example, a new version of an existing application.
- Packaged Release: is a combination of many changes. For example, an operating system image which also contains specific applications.

Configuration Management

Configuration Management is a process that tracks all of the individual Configuration Items (CI) in a system.

Main article: Configuration Management (ITSM)

Service Delivery

The Service Delivery discipline is primarily concerned with the proactive and forward-looking services that the business requires of its ICT provider in order to provide adequate support to the business users. It is focused on the business as the customer of the ICT services (compare with: Service Support). The discipline consists of the following processes, explained in subsections below:

- Service Level Management
- Capacity Management
Service Level Management

Service Level Management provides for continual identification, monitoring and review of the levels of IT services specified in the service level agreements (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 (UCs). The process involves assessing the impact of change upon 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 to be established and monitored against a benchmark.

Service Level Management is the primary interface with the customer (as opposed to the user, who is serviced by the 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, Capacity Management, Incident Management and Problem Management to ensure that the required levels and quality of service are achieved within the resources agreed with Financial Management
- producing and maintaining a Service Catalog (a list of standard IT service options and agreements made available to customers)
- ensuring that appropriate IT Service Continuity plans have been made to support the business and its continuity requirements.

The Service Level Manager relies on all 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.

Capacity Management

Capacity Management supports the optimum and cost effective provision of IT services by helping organizations match their IT resources to the business demands. The high-level activities are Application Sizing, Workload Management, Demand Management, Modeling, Capacity Planning, Resource Management, and Performance Management.

Availability Management

Availability Management allows organizations to sustain the IT service availability in order to support the business at a justifiable cost. The high-level activities are Realize Availability Requirements, Compile Availability Plan, Monitor Availability, and Monitor Maintenance Obligations.

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

- **Reliability**: how reliable is the service? 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**: 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**: A service may have associated data. Security refers to the confidentiality, integrity, and availability of that data. Availability gives us the clear overview of the end to end availability of the system.

Financial Management for IT Services

Main article: Financial Management

Planning to implement service management

Main article: ITIL Planning to implement service management

The ITIL discipline - Planning To Implement Service Management [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 Programme (CSIP) as the basis for implementing other ITIL disciplines as projects within a controlled programme of work. Planning To Implement Service Management is mainly focused on the Service Management processes, but is also generically applicable to other ITIL disciplines.

- create vision
- analyze organization
- set goals
- implement IT service management

Security Management

Main article: ITIL Security Management

The ITIL-process Security Management [14] describes the structured fitting of information security in the management organization. ITIL Security Management is based on the code of practice for information security management also known as ISO/IEC 17799.

A basic concept of the Security Management is the information security. The primary goal of information security is to guarantee safety of the information. Safety is to be protected against risks. Security is the means to be safe against risks. When protecting information it is the value of the information that has to be protected. These values are stipulated by the confidentiality, integrity and availability. Infered aspects are privacy, anonymity and verifiability.

The current move towards ISO/IEC 27001 may require some revision to the ITIL Security Management best practices which are often claimed to be rich in content for physical security but weak in areas such as software/application security and logical security in the ICT infrastructure.

ICT Infrastructure Management

ICT Infrastructure Management [19] processes recommend best practice for requirements analysis, planning, design, deployment and
ongoing operations management and technical support of an ICT Infrastructure. ("ICT" is an acronym for "Information and Communication Technology").

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.

ICIT Design and Planning

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 ("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

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

ICT Operations Management

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 is more technical 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 in order 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:

- 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

ICT Technical Support

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).

The Business Perspective

The Business Perspective is the name given to the collection of best practices [16] that is suggested to address some of the issues often encountered in understanding and improving IT service provision, as a part of the entire business requirement for high IS quality management. These issues are:

- Business Continuity Management describes the responsibilities and opportunities available to the business manager to improve what is, in most organizations one of the key contributing services to business efficiency and effectiveness.
- Surviving Change. IT infrastructure changes can impact the manner in which business is conducted or the continuity of business operations. It is important that business managers take notice of these changes and ensure that steps are taken to safeguard the business from adverse side effects.
- Transformation of business practice through radical change helps to control IT and to integrate it with the business.
- Partnerships and outsourcing

This volume is related to the topics of IT Governance and IT Portfolio Management.

Application Management

ITIL Application Management[17] set 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.

This volume is related to the topics of Software Engineering and IT Portfolio Management.

Software Asset Management
Software Asset Management (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 includes maintaining software license compliance; tracking the inventory and usage of software assets; and maintaining standard policies and procedures surrounding the definition, deployment, configuration, use and retirement of software assets and the Definitive Software Library. SAM represents the software component of IT asset management, which also includes hardware asset management (to which SAM is intrinsically linked by the concept that without effective inventory hardware controls, efforts to control the software thereon will be significantly inhibited) which includes overseeing both software and hardware that comprise an organization’s computers and network.

Small-Scale Implementation

ITIL Small-Scale Implementation [18] provides an approach to the implementation of the ITIL framework for those with smaller IT units or departments. It is primarily an auxiliary work, covering 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.

Criticisms of ITIL

ITIL has been criticized on several fronts, including:

- The books are not affordable for non-commercial users
- Accusations that many ITIL advocates think ITIL is “a holistic, all-encompassing framework for IT governance”;
- Accusations that proponents of ITIL indoctrinate the methodology with ‘religious zeal’ at the expense of pragmatism.
- Implementation and credentialing requires specific training
- Debate over ITIL falling under BSM or ITSIM frameworks

As Jan van Bon (author and editor of many IT Service Management publications) notes, "There is a lot of confusion about ITIL, stemming from all kinds of misunderstandings about its nature. ITIL is, as the OGC states, a set of best practices. The OGC doesn’t claim that ITIL’s best practices describe pure processes. The OGC also doesn’t claim that ITIL is a framework, designed as one coherent model. That is what most of its users make of it, probably because they have such a great need for such a model." [19]

CIO Magazine columnist Dean Meyer has also presented some cautionary views of ITIL, [20] including five pitfalls such as “becoming a slave to outdated definitions” and “Letting ITIL become religion.” As he notes, “...it doesn’t describe the complete range of processes needed to be world class. It's focused on ... managing ongoing services.”

The quality of the library’s volumes is seen to be uneven. For example, van Herwaarden and Grift note, “the consistency that characterized the service support processes … is largely missing in the service delivery books.” [21]

In a 2004 survey designed by Noel Bruton (author of ‘How to Manage the IT Helpdesk’ and ‘Managing the IT Services Process’), ITIL adopting organizations were asked to relate their actual experiences in having implemented ITIL. Seventy-seven percent of survey respondents either agreed or strongly agreed that “ITIL does not have all the answers”. ITIL exponents accept this, citing ITIL’s stated intention to be non-prescriptive, expecting that organizations will have to engage ITIL processes with their existing overall process model. Bruton notes that the claim to non-prescriptiveness must be at best one of scale rather than absolute intention, for the very description of a certain set of processes is in itself a form of prescription. (Survey “The ITIL Experience - Has It Been Worth It”, author Bruton Consultancy 2004, published by Helpdesk Institute Europe, The Helpdesk and IT Support Show and Hornbill Software.)

While ITIL addresses in depth the various aspects of Service Management, it does not address enterprise architecture in such depth. Many of the shortcomings in the implementation of ITIL do not necessarily come about because of flaws in the design or implementation of the Service Management aspects of the business, but rather the wider architectural framework in which the business is situated. Because of its primary focus on Service Management, ITIL has limited utility in managing poorly designed enterprise architectures, or how to feed back into the design of the enterprise architecture.

Some researchers have placed ITIL in relation with Lean, Six Sigma and Agile IT operations management. [citation needed] Applying Six Sigma techniques to ITIL brings the engineering approach to ITIL’s framework. Applying Lean techniques promotes continuous improvement of the ITIL’s best practices.

See also

- Business Application Optimization (BAO, Macro 4)
- Business Information Services Library
- Enterprise Architecture
- IT Governance
- IT Service Management
- PRINCE2
- IBM Tivoli Unified Process (ITUP)
- enhanced Telecom Operations Map (eTOM)
- Run Book Automation (RBA)
- Performance engineering
- Microsoft Operations Framework (MOF)
- Grey Area Diagnosis
- RPR Problem Diagnosis

References

The English Wikipedia is the English-language edition of the free online encyclopedia Wikipedia. Founded on 15 January 2001, it is the first edition of Wikipedia and, as of November 2017, has the most articles of any of the editions. As of February 2019, 12% of articles in all Wikipedias belong to the English-language edition. This share has gradually declined from more than 50 percent in 2003, due to the growth of Wikipedias in other languages. As of 13 February 2019, there are 5,802,434 articles on


External links

- Official ITIL Website
- The OGC website
- IT Service Management Forum (International)
- The ITIL definition site
- The ITIL Forum
- The ITIL Open Guide
- American ITIL
- IT Business Edge - ITIL Resources

Categories: Information technology management | Standards | Method engineering

This page was last modified on 15 May 2009, at 17:59 (UTC). All text is available under the terms of the GNU Free Documentation License. (See Copyrights for details.) Wikipedia® is a registered trademark of the Wikimedia Foundation, Inc., a U.S. registered 501(c)(3)-tax-deductible nonprofit charity. Privacy policy About Wikipedia Disclaimers

The English Wikipedia is the English-language edition of the free online encyclopedia Wikipedia. Founded on 15 January 2001, it is the first edition of Wikipedia and, as of November 2017, has the most articles of any of the editions. As of February 2019, 12% of articles in all Wikipedias belong to the English-language edition. This share has gradually declined from more than 50 percent in 2003, due to the growth of Wikipedias in other languages. As of 13 February 2019, there are 5,802,434 articles on