ITIL® V3 Foundation Course Glossary

Term	Definition
Acceptance	Formal agreement that an IT Service, Process, Plan, or other Deliverable is complete, accurate, Reliable and meets its specified Requirements. Acceptance is usually preceded by Evaluation or Testing and is often required before proceeding to the next stage of a Project or Process. See Service Acceptance Criteria.
Access Management	The Process responsible for allowing Users to make use of IT Services, data, or other Assets. Access Management helps to protect the Confidentiality, Integrity and Availability of Assets by ensuring that only authorized Users are able to access or modify the Assets. Access Management is sometimes referred to as Rights Management or Identity Management.
Account Manager	A Role that is very similar to Business Relationship Manager, but includes more commercial aspects. Most commonly used when dealing with External Customers.
Accounting	The Process responsible for identifying actual Costs of delivering IT Services, comparing these with budgeted costs, and managing variance from the Budget.
Accredited	Officially authorized to carry out a Role. For example an Accredited body may be authorized to provide training or to conduct Audits.
Agreed Service Time	A synonym for Service Hours, commonly used in formal calculations of Availability. See Downtime.
Alert	A warning that a threshold has been reached, something has changed, or a Failure has occurred. Alerts are often created and managed by System Management tools and are managed by the Event Management Process.
Application	Software that provides Functions that are required by an IT Service. Each Application may be part of more than one IT Services. An Application runs on one or more Servers or Clients. See Application Management, Application Portfolio.
Application Management	The Function responsible for managing Applications throughout their Lifecycle.
Application Service Provider (ASP)	An External Service Provider that provides IT Services using Applications running at the Service Provider's premises. Users access the Applications by network connections to the Service Provider.
Application Sizing	The Activity responsible for understanding the Resource Requirements needed to support a new Application, or a major Change to an existing Application. Application Sizing helps to ensure that the IT Service can meet its agreed Service Level Targets for Capacity and Performance.

ITIL® V3 Foundation Course Glossary

Term	Definition
Architecture	The structure of a System or IT Service, including the Relationships of Components to each other and to the environment they are in. Architecture also includes the Standards and Guidelines which guide the design and evolution of the System.
Assessment	Inspection and analysis to check whether a Standard or set of Guidelines is being followed, that Records are accurate, or that Efficiency and Effectiveness targets are being met. See Audit.
Asset	Any Resource or Capability. Assets of a Service Provider include anything that could contribute to the delivery of a Service. Assets can be one of the following types: Management, Organization, Process, Knowledge, People, Information, Applications, Infrastructure, and Financial Capital.
Asset Management	Asset Management is the Process responsible for tracking and reporting the value and ownership of financial Assets throughout their Lifecycle. Asset Management is part of an overall Service Asset and Configuration Management Process. See Asset Register.
Attribute	A piece of information about a Configuration Item. Examples are name, location, Version number, and Cost. Attributes of CIs are recorded in the Configuration Management Database (CMDB). See Relationship.
Audit	Formal inspection and verification to check whether a Standard or set of Guidelines is being followed, that Records are accurate, or that Efficiency and Effectiveness targets are being met. An Audit may be carried out by internal or external groups. See Certification, Assessment.
Authority Matrix	Synonym for RACI.
Availability	Ability of a Configuration Item or IT Service to perform its agreed Function when required. Availability is determined by Reliability, Maintainability, Serviceability, Performance, and Security. Availability is usually calculated as a percentage. This calculation is often based on Agreed Service Time and Downtime. It is Best Practice to calculate Availability using measurements of the Business output of the IT Service.
Availability Management	The Process responsible for defining, analyzing, Planning, measuring and improving all aspects of the Availability of IT Services. Availability Management is responsible for ensuring that all IT Infrastructure, Processes, Tools, Roles etc are appropriate for the agreed Service Level Targets for Availability.

ITIL® V3 Foundation Course Glossary

Term	Definition
Availability Management Information System (AMIS)	A virtual repository of all Availability Management data, usually stored in multiple physical locations. See Service Knowledge Management System.
Availability Plan	A Plan to ensure that existing and future Availability Requirements for IT Services can be provided Cost Effectively.
Back-out	Synonym for Remediation.
Backup	Copying data to protect against loss of Integrity or Availability of the original.
Baseline	A Benchmark used as a reference point. For example: • An ITSM Baseline can be used as a starting point to measure the effect of a Service Improvement Plan • A Performance Baseline can be used to measure changes in Performance over the lifetime of an IT Service • A Configuration Management Baseline can be used to enable the IT Infrastructure to be restored to a known Configuration if a Change or Release fails
Best Practice	Proven Activities or Processes that have been successfully used by multiple Organizations. ITIL is an example of Best Practice.
Business Capacity Management (BCM)	In the context of ITSM, Business Capacity Management is the Activity responsible for understanding future Business Requirements for use in the Capacity Plan. See Service Capacity Management.
Business Case	Justification for a significant item of expenditure. Includes information about Costs, benefits, options, issues, Risks, and possible problems. See Cost Benefit Analysis.
Business Continuity Management (BCM)	The Business Process responsible for managing Risks that could seriously impact the Business. BCM safeguards the interests of key stakeholders, reputation, brand and value creating activities. The BCM Process involves reducing Risks to an acceptable level and planning for the recovery of Business Processes should a disruption to the Business occur. BCM sets the Objectives, Scope and Requirements for IT Service Continuity Management.
Business Continuity Plan (BCP)	A Plan defining the steps required to Restore Business Processes following a disruption. The Plan will also identify the triggers for Invocation, people to be involved, communications etc. IT Service Continuity Plans form a significant part of Business Continuity Plans.

ITIL® V3 Foundation Course Glossary

Term	Definition
Business Impact Analysis (BIA)	BIA is the Activity in Business Continuity Management that identifies Vital Business Functions and their dependencies. These dependencies may include Suppliers, people, other Business Processes, IT Services etc. BIA defines the recovery requirements for IT Services. These requirements include Recovery Time Objectives, Recovery Point Objectives and minimum Service Level Targets for each IT Service.
Business Relationship Manager (BRM)	A Role responsible for maintaining the Relationship with one or more Customers. This Role is often combined with the Service Level Manager Role. See Account Manager.
Business Unit	A segment of the Business which has its own Plans, Metrics, income and Costs. Each Business Unit owns Assets and uses these to create value for Customers in the form of goods and Services.
Capability	The ability of an Organization, person, Process, Application, Configuration Item or IT Service to carry out an Activity. Capabilities are intangible Assets of an Organization. See Resource.
Capability Maturity Model (CMM)	The Capability Maturity Model for Software (also known as the CMM and SW-CMM) is a model used to identify Best Practices to help increase Process Maturity. CMM was developed at the Software Engineering Institute (SEI) of Carnegie Mellon University. In 2000, the SW-CMM was upgraded to CMMI® (Capability Maturity Model Integration). The SEI no longer maintains the SW-CMM model, its associated appraisal methods, or training materials.
Capacity	The maximum Throughput that a Configuration Item or IT Service can deliver whilst meeting agreed Service Level Targets. For some types of CI, Capacity may be the size or volume, for example a disk drive.
Capacity Management	The Process responsible for ensuring that the Capacity of IT Services and the IT Infrastructure is able to deliver agreed Service Level Targets in a Cost Effective and timely manner. Capacity Management considers all Resources required to deliver the IT Service, and plans for short, medium and long term Business Requirements.
Capacity Management Information System (CMIS)	A virtual repository of all Capacity Management data, usually stored in multiple physical locations. See Service Knowledge Management System.
Capacity Plan	A Capacity Plan is used to manage the Resources required to deliver IT Services. The Plan contains scenarios for different predictions of Business demand, and costed options to deliver the agreed Service Level Targets.

ITIL® V3 Foundation Course Glossary

Term	Definition
Category	A named group of things that have something in common. Categories are used to group similar things together. For example Cost Types are used to group similar types of Cost. Incident Categories are used to group similar types of Incident, CI Types are used to group similar types of Configuration Item.
Certification	Issuing a certificate to confirm Compliance to a Standard. Certification includes a formal Audit by an independent and Accredited body. The term Certification is also used to mean awarding a certificate to verify that a person has achieved a qualification.
Change	The addition, modification or removal of anything that could have an effect on IT Services. The Scope should include all IT Services, Configuration Items, Processes, Documentation etc.
Change Advisory Board (CAB)	A group of people that advises the Change Manager in the Assessment, prioritisation and scheduling of Changes. This board is usually made up of representatives from all areas within the IT Service Provider, the Business, and Third Parties such as Suppliers.
Change Management	The Process responsible for controlling the Lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to IT Services.
Change Model	A repeatable way of dealing with a particular Category of Change. A Change Model defines specific pre-defined steps that will be followed for a Change of this Category. Change Models may be very simple, with no requirement for approval (e.g. Password Reset) or may be very complex with many steps that require approval (e.g. major software Release). See Standard Change, Change Advisory Board.
Change Record	A Record containing the details of a Change. Each Change Record documents the Lifecycle of a single Change. A Change Record is created for every Request for Change that is received, even those that are subsequently rejected. Change Records should reference the Configuration Items that are affected by the Change. Change Records are stored in the Configuration Management System.
Change Request	Synonym for Request for Change.
Change Schedule	A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.
CI Type	A Category that is used to Classify CIs. The CI Type identifies the required Attributes and Relationships for a Configuration Record. Common CI Types include: hardware, Document, User etc.

ITIL® V3 Foundation Course Glossary

Term	Definition
Classification	The act of assigning a Category to something. Classification is used to ensure consistent management and reporting. CIs, Incidents, Problems, Changes etc. are usually classified.
COBIT	Control Objectives for Information and related Technology (COBIT) provides guidance and Best Practice for the management of IT Processes. COBIT is published by the IT Governance Institute. See http://www.isaca.org/ for more information.
Compliance	Ensuring that a Standard or set of Guidelines is followed, or that proper, consistent accounting or other practices are being employed.
Component CI	A Configuration Item that is part of an Assembly. For example, a CPU or Memory CI may be part of a Server CI.
Confidentiality	A security principle that requires that data should only be accessed by authorized people.
Configuration	A generic term, used to describe a group of Configuration Items that work together to deliver an IT Service, or a recognizable part of an IT Service. Configuration is also used to describe the parameter settings for one or more CIs.
Configuration Baseline	A Baseline of a Configuration that has been formally agreed and is managed through the Change Management process. A Configuration Baseline is used as a basis for future Builds, Releases and Changes.
Configuration Control	The Activity responsible for ensuring that adding, modifying or removing a CI is properly managed, for example by submitting a Request for Change or Service Request.
Configuration Item (CI)	Any Component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs.
Configuration Management	The Process responsible for maintaining information about Configuration Items required to deliver an IT Service, including their Relationships. This information is managed throughout the Lifecycle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process.
Configuration Management Database (CMDB)	A database used to store Configuration Records throughout their Lifecycle. The Configuration Management System maintains one or more CMDBs, and each CMDB stores Attributes of CIs, and Relationships with other CIs.

ITIL® V3 Foundation Course Glossary

Term	Definition
Configuration Management System (CMS)	A set of tools and databases that are used to manage an IT Service Provider's Configuration data. The CMS also includes information about Incidents, Problems, Known Errors, Changes and Releases; and may contain data about employees, Suppliers, locations, Business Units, Customers and Users. The CMS includes tools for collecting, storing, managing, updating, and presenting data about all Configuration Items and their Relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management Processes. See Configuration Management Database, Service Knowledge Management System.
Continual Service Improvement (CSI)	A stage in the Lifecycle of an IT Service and the title of one of the Core ITIL publications. Continual Service Improvement is responsible for managing improvements to IT Service Management Processes and IT Services. The Performance of the IT Service Provider is continually measured and improvements are made to Processes, IT Services and IT Infrastructure in order to increase Efficiency, Effectiveness, and Cost Effectiveness. See Plan-Do-Check-Act.
Control Processes	The ISO/IEC 20000 Process group that includes Change Management and Configuration Management.
Cost Benefit Analysis	An Activity that analyses and compares the Costs and the benefits involved in one or more alternative courses of action. See Business Case, Net Present Value, Internal Rate of Return, Return on Investment, Value on Investment.
Critical Success Factor (CSF)	Something that must happen if a Process, Project, Plan, or IT Service is to succeed. KPIs are used to measure the achievement of each CSF. For example a CSF of "protect IT Services when making Changes" could be measured by KPIs such as "percentage reduction of unsuccessful Changes", "percentage reduction in Changes causing Incidents" etc.
Customer	Someone who buys goods or Services. The Customer of an IT Service Provider is the person or group who defines and agrees the Service Level Targets. The term Customers is also sometimes informally used to mean Users, for example "this is a Customer focussed Organization".
Dashboard	A graphical representation of overall IT Service Performance and Availability. Dashboard images may be updated in real-time, and can also be included in management reports and web pages. Dashboards can be used to support Service Level Management, Event Management or Incident Diagnosis.
Data-to-Information-to-Knowledge-to-Wisdom (DIKW)	A way of understanding the relationships between data, information, knowledge, and wisdom. DIKW shows how each of these builds on the others.

ITIL® V3 Foundation Course Glossary

Term	Definition
Definitive Media Library (DML)	One or more locations in which the definitive and approved versions of all software Configuration Items are securely stored. The DML may also contain associated CIs such as licenses and documentation. The DML is a single logical storage area even if there are multiple locations. All software in the DML is under the control of Change and Release Management and is recorded in the Configuration Management System. Only software from the DML is acceptable for use in a Release.
Demand Management	Activities that understand and influence Customer demand for Services and the provision of Capacity to meet these demands. At a Strategic level Demand Management can involve analysis of Patterns of Business Activity and User Profiles. At a Tactical level it can involve use of Differential Charging to encourage Customers to use IT Services at less busy times. See Capacity Management.
Deming Cycle	Synonym for Plan Do Check Act.
Detection	A stage in the Incident Lifecycle. Detection results in the Incident becoming known to the Service Provider. Detection can be automatic, or can be the result of a User logging an Incident.
Differential Charging	A technique used to support Demand Management by charging different amounts for the same IT Service Function at different times.
Direct Cost	A cost of providing an IT Service which can be allocated in full to a specific Customer, Cost Centre, Project etc. For example cost of providing non-shared servers or software licenses. See Indirect Cost.
Directory Service	An Application that manages information about IT Infrastructure available on a network, and corresponding User access Rights.
Downtime	The time when a Configuration Item or IT Service is not Available during its Agreed Service Time. The Availability of an IT Service is often calculated from Agreed Service Time and Downtime.
Effectiveness	A measure of whether the Objectives of a Process, Service or Activity have been achieved. An Effective Process or Activity is one that achieves its agreed Objectives. See KPI.
Efficiency	A measure of whether the right amount of resources have been used to deliver a Process, Service or Activity. An Efficient Process achieves its Objectives with the minimum amount of time, money, people or other resources. See KPI.

ITIL® V3 Foundation Course Glossary

Term	Definition
Emergency Change	A Change that must be introduced as soon as possible. For example to resolve a Major Incident or implement a Security patch. The Change Management Process will normally have a specific Procedure for handling Emergency Changes. See Emergency Change Advisory Board (ECAB).
Emergency Change Advisory Board (ECAB)	A sub-set of the Change Advisory Board who make decisions about high impact Emergency Changes. Membership of the ECAB may be decided at the time a meeting is called, and depends on the nature of the Emergency Change.
Error	A design flaw or malfunction that causes a Failure of one or more Configuration Items or IT Services. A mistake made by a person or a faulty Process that impacts a CI or IT Service is also an Error.
Escalation	An Activity that obtains additional Resources when these are needed to meet Service Level Targets or Customer expectations. Escalation may be needed within any IT Service Management Process, but is most commonly associated with Incident Management, Problem Management and the management of Customer complaints. There are two types of Escalation, Functional Escalation and Hierarchic Escalation.
Event	A change of state which has significance for the management of a Configuration Item or IT Service. The term Event is also used to mean an Alert or notification created by any IT Service, Configuration Item or Monitoring tool. Events typically require IT Operations personnel to take actions, and often lead to Incidents being logged.
Event Management	The Process responsible for managing Events throughout their Lifecycle. Event Management is one of the main Activities of IT Operations.
Exception Report	A Document containing details of one or more KPIs or other important targets that have exceeded defined Thresholds. Examples include SLA targets being missed or about to be missed, and a Performance Metric indicating a potential Capacity problem.
External Service Provider	An IT Service Provider which is part of a different Organization to their Customer. An IT Service Provider may have both Internal Customers and External Customers. See Type III Service Provider.
Facilities Management	The Function responsible for managing the physical Environment where the IT Infrastructure is located. Facilities Management includes all aspects of managing the physical Environment, for example power and cooling, building Access Management, and environmental Monitoring.
Fault	Synonym for Error.

ITIL® V3 Foundation Course Glossary

Term	Definition
Fault Tree Analysis (FTA)	A technique that can be used to determine the chain of Events that leads to a Problem. Fault Tree Analysis represents a chain of Events using Boolean notation in a diagram.
Financial Management	The Function and Processes responsible for managing an IT Service Provider's Budgeting, Accounting and Charging Requirements.
Fishbone Diagram	Synonym for Ishikawa Diagram.
Fit for Purpose	An informal term used to describe a Process, Configuration Item, IT Service etc. that is capable of meeting its Objectives or Service Levels. Being Fit for Purpose requires suitable Design, implementation, Control and maintenance.
Fixed Cost	A Cost that does not vary with IT Service usage. For example the cost of Server hardware. See Variable Cost.
Follow the Sun	A methodology for using Service Desks and Support Groups around the world to provide seamless 24 * 7 Service. Calls, Incidents, Problems and Service Requests are passed between groups in different time zones.
Function	A team or group of people and the tools they use to carry out one or more Processes or Activities. For example the Service Desk. The term Function also has two other meanings • An intended purpose of a Configuration Item, Person, Team, Process, or IT Service. For example one Function of an Email Service may be to store and forward outgoing mails, one Function of a Business Process may be to dispatch goods to Customers. • To perform the intended purpose correctly, "The computer is Functioning"
Gap Analysis	An Activity which compares two sets of data and identifies the differences. Gap Analysis is commonly used to compare a set of Requirements with actual delivery. See Benchmarking.
Governance	Ensuring that Policies and Strategy are actually implemented, and that required Processes are correctly followed. Governance includes defining Roles and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.
Hierarchic Escalation	Informing or involving more senior levels of management to assist in an Escalation.
Impact	A measure of the effect of an Incident, Problem or Change on Business Processes. Impact is often based on how Service Levels will be affected. Impact and Urgency are used to assign Priority.

ITIL® V3 Foundation Course Glossary

Term	Definition
Incident	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.
Incident Management	The Process responsible for managing the Lifecycle of all Incidents. The primary Objective of Incident Management is to return the IT Service to Users as quickly as possible.
Incident Record	A Record containing the details of an Incident. Each Incident record documents the Lifecycle of a single Incident.
Indirect Cost	A Cost of providing an IT Service which cannot be allocated in full to a specific Customer. For example Cost of providing shared Servers or software licenses. Also known as Overhead. See Direct Cost.
Information Security Management (ISM)	The Process that ensures the Confidentiality, Integrity and Availability of an Organization's Assets, information, data and IT Services. Information Security Management usually forms part of an Organizational approach to Security Management which has a wider scope than the IT Service Provider, and includes handling of paper, building access, phone calls etc., for the entire Organization.
Information Security Management System (ISMS)	The framework of Policy, Processes, Standards, Guidelines and tools that ensures an Organization can achieve its Information Security Management Objectives.
Information Security Policy	The Policy that governs the Organization’s approach to Information Security Management.
Information Technology (IT)	The use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, Applications and other software. The information may include Business data, voice, images, video, etc. Information Technology is often used to support Business Processes through IT Services.
Integrity	A security principle that ensures data and Configuration Items are only modified by authorized personnel and Activities. Integrity considers all possible causes of modification, including software and hardware Failure, environmental Events, and human intervention.
Internal Service Provider	An IT Service Provider which is part of the same Organization as their Customer. An IT Service Provider may have both Internal Customers and External Customers. See Type I Service Provider, Type II Service Provider, Insource.

ITIL® V3 Foundation Course Glossary

Term	Definition
International Organization for Standardization (ISO)	The International Organization for Standardization (ISO) is the world's largest developer of Standards. ISO is a non-governmental organization which is a network of the national standards institutes of 156 countries. Further information about ISO is available from http://www.iso.org/
Ishikawa Diagram	A technique that helps a team to identify all the possible causes of a Problem. Originally devised by Kaoru Ishikawa, the output of this technique is a diagram that looks like a fishbone.
ISO 9000	A generic term that refers to a number of international Standards and Guidelines for Quality Management Systems. See http://www.iso.org/ for more information. See ISO.
ISO 9001	An international Standard for Quality Management Systems. See ISO 9000, Standard.
ISO/IEC 17799	ISO Code of Practice for Information Security Management. See Standard.
ISO/IEC 20000	ISO Specification and Code of Practice for IT Service Management. ISO/IEC 20000 is aligned with ITIL Best Practice.
ISO/IEC 27001	ISO Specification for Information Security Management. The corresponding Code of Practice is ISO/IEC 17799. See Standard.
IT Infrastructure	All of the hardware, software, networks, facilities etc. that are required to Develop, Test, deliver, Monitor, Control or support IT Services. The term IT Infrastructure includes all of the Information Technology but not the associated people, Processes and documentation.
IT Operations	Activities carried out by IT Operations Control, including Console Management, Job Scheduling, Backup and Restore, and Print and Output Management. IT Operations is also used as a synonym for Service Operation.
IT Operations Control	The Function responsible for Monitoring and Control of the IT Services and IT Infrastructure. See Operations Bridge.
IT Operations Management	The Function within an IT Service Provider which performs the daily Activities needed to manage IT Services and the supporting IT Infrastructure. IT Operations Management includes IT Operations Control and Facilities Management.
IT Service	A Service provided to one or more Customers by an IT Service Provider. An IT Service is based on the use of Information Technology and supports the Customer's Business Processes. An IT Service is made up from a combination of people, Processes and technology and should be defined in a Service Level Agreement.

ITIL® V3 Foundation Course Glossary

Term	Definition
IT Service Continuity Management (ITSCM)	The Process responsible for managing Risks that could seriously impact IT Services. ITSCM ensures that the IT Service Provider can always provide minimum agreed Service Levels, by reducing the Risk to an acceptable level and Planning for the Recovery of IT Services. ITSCM should be designed to support Business Continuity Management.
IT Service Continuity Plan	A Plan defining the steps required to Recover one or more IT Services. The Plan will also identify the triggers for Invocation, people to be involved, communications etc. The IT Service Continuity Plan should be part of a Business Continuity Plan.
IT Service Management (ITSM)	The implementation and management of Quality IT Services that meet the needs of the Business. IT Service Management is performed by IT Service Providers through an appropriate mix of people, Process and Information Technology. See Service Management.
IT Service Management Forum (itSMF)	The IT Service Management Forum is an independent Organization dedicated to promoting a professional approach to IT Service Management. The itSMF is a not-for-profit membership Organization with representation in many countries around the world (itSMF Chapters). The itSMF and its membership contribute to the development of ITIL and associated IT Service Management Standards. See http://www.itsmf.com/ for more information.
ITIL	A set of Best Practice guidance for IT Service Management. ITIL is owned by the OGC and consists of a series of publications giving guidance on the provision of Quality IT Services, and on the Processes and facilities needed to support them. See http://www.itil.co.uk/ for more information.
Kepner & Tregoe Analysis	A structured approach to Problem solving. The Problem is analysed in terms of what, where, when and extent. Possible causes are identified. The most probable cause is tested. The true cause is verified.
Key Performance Indicator (KPI)	A Metric that is used to help manage a Process, IT Service or Activity. Many Metrics may be measured, but only the most important of these are defined as KPIs and used to actively manage and report on the Process, IT Service or Activity. KPIs should be selected to ensure that Efficiency, Effectiveness, and Cost Effectiveness are all managed. See Critical Success Factor.
Knowledge Base	A logical database containing the data used by the Service Knowledge Management System.
Knowledge Management	The Process responsible for gathering, analyzing, storing and sharing knowledge and information within an Organization. The primary purpose of Knowledge Management is to improve Efficiency by reducing the need to rediscover knowledge. See Data-to-Information-to-Knowledge-to-Wisdom, Service Knowledge Management System.

ITIL® V3 Foundation Course Glossary

Term	Definition
Known Error	A Problem that has a documented Root Cause and a Workaround. Known Errors are created and managed throughout their Lifecycle by Problem Management. Known Errors may also be identified by Development or Suppliers.
Known Error Database (KEDB)	A database containing all Known Error Records. This database is created by Problem Management and used by Incident and Problem Management. The Known Error Database is part of the Service Knowledge Management System.
Known Error Record	A Record containing the details of a Known Error. Each Known Error Record documents the Lifecycle of a Known Error, including the Status, Root Cause and Workaround. In some implementations a Known Error is documented using additional fields in a Problem Record.
Lifecycle	The various stages in the life of an IT Service, Configuration Item, Incident, Problem, Change etc. The Lifecycle defines the Categories for Status and the Status transitions that are permitted. For example: • The Lifecycle of an Application includes Requirements, Design, Build, Deploy, Operate, Optimise. • The Expanded Incident Lifecycle includes Detect, Respond, Diagnose, Repair, Recover, Restore. • The lifecycle of a Server may include: Ordered, Received, In Test, Live, Disposed etc.
Maintainability	A measure of how quickly and Effectively a Configuration Item or IT Service can be restored to normal working after a Failure. Maintainability is often measured and reported as MTRS. Maintainability is also used in the context of Software or IT Service Development to mean ability to be Changed or Repaired easily.
Major Incident	The highest Category of Impact for an Incident. A Major Incident results in significant disruption to the Business.
Management of Risk (MoR)	The OGC methodology for managing Risks. MoR includes all the Activities required to identify and Control the exposure to Risk which may have an impact on the achievement of an Organization's Business Objectives. See http://www.m-o-r.org/ for more details.
Manual Workaround	A Workaround that requires manual intervention. Manual Workaround is also used as the name of a Recovery Option in which The Business Process Operates without the use of IT Services. This is a temporary measure and is usually combined with another Recovery Option.
Maturity Level	A named level in a Maturity model such as the Carnegie Mellon Capability Maturity Model Integration.
Mean Time Between Failures (MTBF)	A Metric for measuring and reporting Reliability. MTBF is the average time that a Configuration Item or IT Service can perform its agreed Function without interruption. This is measured from when the CI or IT Service starts working, until it next fails.

ITIL® V3 Foundation Course Glossary

Term	Definition
Mean Time Between Service Incidents (MTBSI)	A Metric used for measuring and reporting Reliability. MTBSI is the mean time from when a System or IT Service fails, until it next fails. MTBSI is equal to MTBF + MTRS.
Mean Time To Repair (MTTR)	The average time taken to repair a Configuration Item or IT Service after a Failure. MTTR is measured from when the CI or IT Service fails until it is Repaired. MTTR does not include the time required to Recover or Restore. MTTR is sometimes incorrectly used to mean Mean Time to Restore Service.
Mean Time to Restore Service (MTRS)	The average time taken to Restore a Configuration Item or IT Service after a Failure. MTRS is measured from when the CI or IT Service fails until it is fully Restored and delivering its normal functionality. See Maintainability, Mean Time to Repair.
Metric	Something that is measured and reported to help manage a Process, IT Service or Activity. See KPI.
Mission Statement	The Mission Statement of an Organization is a short but complete description of the overall purpose and intentions of that Organization. It states what is to be achieved, but not how this should be done.
Notional Charging	An approach to Charging for IT Services. Charges to Customers are calculated and Customers are informed of the charge, but no money is actually transferred. Notional Charging is sometimes introduced to ensure that Customers are aware of the Costs they incur, or as a stage during the introduction of real Charging.
Office of Government Commerce (OGC)	OGC owns the ITIL brand (copyright and trademark). OGC is a UK Government department that supports the delivery of the government's procurement agenda through its work in collaborative procurement and in raising levels of procurement skills and capability with departments. It also provides support for complex public sector projects.
Operational Level Agreement (OLA)	An Agreement between an IT Service Provider and another part of the same Organization. An OLA supports the IT Service Provider's delivery of IT Services to Customers. The OLA defines the goods or Services to be provided and the responsibilities of both parties. For example there could be an OLA • between the IT Service Provider and a procurement department to obtain hardware in agreed times • between the Service Desk and a Support Group to provide Incident Resolution in agreed times. See Service Level Agreement.
Outsourcing	Using an External Service Provider to manage IT Services. See Service Sourcing, Type III Service Provider.
Overhead	Synonym for Indirect cost

Term	Definition
Pain Value Analysis	A technique used to help identify the Business Impact of one or more Problems. A formula is used to calculate Pain Value based on the number of Users affected, the duration of the Downtime, the Impact on each User, and the cost to the Business (if known).
Pareto Principle	A technique used to prioritise Activities. The Pareto Principle says that 80% of the value of any Activity is created with 20% of the effort. Pareto Analysis is also used in Problem Management to prioritise possible Problem causes for investigation.
Partnership	A relationship between two Organizations which involves working closely together for common goals or mutual benefit. The IT Service Provider should have a Partnership with the Business, and with Third Parties who are critical to the delivery of IT Services. See Value Network.
Pattern of Business Activity (PBA)	A Workload profile of one or more Business Activities. Patterns of Business Activity are used to help the IT Service Provider understand and plan for different levels of Business Activity. See User Profile.
Performance Management	The Process responsible for day-to-day Capacity Management Activities. These include Monitoring, Threshold detection, Performance analysis and Tuning, and implementing Changes related to Performance and Capacity.
Pilot	A limited Deployment of an IT Service, a Release or a Process to the Live Environment. A Pilot is used to reduce Risk and to gain User feedback and Acceptance. See Test, Evaluation.
Plan-Do-Check-Act	A four stage cycle for Process management, attributed to Edward Deming. Plan-Do-Check-Act is also called the Deming Cycle. PLAN: Design or revise Processes that support the IT Services. DO: Implement the Plan and manage the Processes. CHECK: Measure the Processes and IT Services, compare with Objectives and produce reports ACT: Plan and implement Changes to improve the Processes.
Policy	Formally documented management expectations and intentions. Policies are used to direct decisions, and to ensure consistent and appropriate development and implementation of Processes, Standards, Roles, Activities, IT Infrastructure etc.
Post Implementation Review (PIR)	A Review that takes place after a Change or a Project has been implemented. A PIR determines if the Change or Project was successful, and identifies opportunities for improvement.
Priority	A Category used to identify the relative importance of an Incident, Problem or Change. Priority is based on Impact and Urgency, and is used to identify required times for actions to be taken. For example the SLA may state that Priority2 Incidents must be resolved within 12 hours.

Term	Definition
Proactive Problem Management	Part of the Problem Management Process. The Objective of Proactive Problem Management is to identify Problems that might otherwise be missed. Proactive Problem Management analyses Incident Records, and uses data collected by other IT Service Management Processes to identify trends or significant Problems.
Problem	A cause of one or more Incidents. The cause is not usually known at the time a Problem Record is created, and the Problem Management Process is responsible for further investigation.
Problem Management	The Process responsible for managing the Lifecycle of all Problems. The primary Objectives of Problem Management are to prevent Incidents from happening, and to minimise the Impact of Incidents that cannot be prevented.
Problem Record	A Record containing the details of a Problem. Each Problem Record documents the Lifecycle of a single Problem.
Procedure	A Document containing steps that specify how to achieve an Activity. Procedures are defined as part of Processes. See Work Instruction.
Process	A structured set of Activities designed to accomplish a specific Objective. A Process takes one or more defined inputs and turns them into defined outputs. A Process may include any of the Roles, responsibilities, tools and management Controls required to reliably deliver the outputs. A Process may define Policies, Standards, Guidelines, Activities, and Work Instructions if they are needed.
Process Control	The Activity of planning and regulating a Process, with the Objective of performing the Process in an Effective, Efficient, and consistent manner.
Process Manager	A Role responsible for Operational management of a Process. The Process Manager's responsibilities include Planning and co-ordination of all Activities required to carry out, monitor and report on the Process. There may be several Process Managers for one Process, for example regional Change Managers or IT Service Continuity Managers for each data centre. The Process Manager Role is often assigned to the person who carries out the Process Owner Role, but the two Roles may be separate in larger Organizations.
Process Owner	A Role responsible for ensuring that a Process is Fit for Purpose. The Process Owner’s responsibilities include sponsorship, Design, Change Management and continual improvement of the Process and its Metrics. This Role is often assigned to the same person who carries out the Process Manager Role, but the two Roles may be separate in larger Organizations.

ITIL® V3 Foundation Course Glossary

Term	Definition
Project	A temporary Organization, with people and other Assets required to achieve an Objective or other Outcome. Each Project has a Lifecycle that typically includes initiation, Planning, execution, Closure etc. Projects are usually managed using a formal methodology such as PRINCE2.
Quality Assurance (QA)	The Process responsible for ensuring that the Quality of a product, Service or Process will provide its intended Value.
Quality Management System (QMS)	The set of Processes responsible for ensuring that all work carried out by an Organization is of a suitable Quality to reliably meet Business Objectives or Service Levels. See ISO 9000.
RACI	A Model used to help define Roles and Responsibilities. RACI stands for Responsible, Accountable, Consulted and Informed. See Stakeholder.
Release	A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, Tested, and Deployed as a single entity.
Release and Deployment Management	The Process responsible for both Release Management and Deployment.
Release Management	The Process responsible for Planning, scheduling and controlling the movement of Releases to Test and Live Environments. The primary Objective of Release Management is to ensure that the integrity of the Live Environment is protected and that the correct Components are released. Release Management is part of the Release and Deployment Management Process.
Release Unit	Components of an IT Service that are normally Released together. A Release Unit typically includes sufficient Components to perform a useful Function. For example one Release Unit could be a Desktop PC, including Hardware, Software, Licenses, Documentation etc. A different Release Unit may be the complete Payroll Application, including IT Operations Procedures and User training.
Reliability	A measure of how long a Configuration Item or IT Service can perform its agreed Function without interruption. Usually measured as MTBF or MTBSI. The term Reliability can also be used to state how likely it is that a Process, Function etc. will deliver its required outputs. See Availability.
Request for Change (RFC)	A formal proposal for a Change to be made. An RFC includes details of the proposed Change, and may be recorded on paper or electronically. The term RFC is often misused to mean a Change Record, or the Change itself.

Term	Definition
Request Fulfilment	The Process responsible for managing the Lifecycle of all Service Requests.
Requirement	A formal statement of what is needed. For example a Service Level Requirement, a Project Requirement or the required Deliverables for a Process. See Statement of Requirements.
Resilience	The ability of a Configuration Item or IT Service to resist Failure or to Recover quickly following a Failure. For example, an armoured cable will resist failure when put under stress. See Fault Tolerance.
Resource	A generic term that includes IT Infrastructure, people, money or anything else that might help to deliver an IT Service. Resources are considered to be Assets of an Organization. See Capability, Service Asset.
Response Time	A measure of the time taken to complete an Operation or Transaction. Used in Capacity Management as a measure of IT Infrastructure Performance, and in Incident Management as a measure of the time taken to answer the phone, or to start Diagnosis.
Restore	Taking action to return an IT Service to the Users after Repair and Recovery from an Incident. This is the primary Objective of Incident Management.
Retire	Permanent removal of an IT Service, or other Configuration Item, from the Live Environment. Retired is a stage in the Lifecycle of many Configuration Items.
Return on Investment (ROI)	A measurement of the expected benefit of an investment. In the simplest sense it is the net profit of an investment divided by the net worth of the assets invested. See Net Present Value, Value on Investment.
Rights	Entitlements, or permissions, granted to a User or Role. For example the Right to modify particular data, or to authorize a Change.
Risk	A possible Event that could cause harm or loss, or affect the ability to achieve Objectives. A Risk is measured by the probability of a Threat, the Vulnerability of the Asset to that Threat, and the Impact it would have if it occurred.
Risk Assessment	The initial steps of Risk Management. Analyzing the value of Assets to the business, identifying Threats to those Assets, and evaluating how Vulnerable each Asset is to those Threats. Risk Assessment can be quantitative (based on numerical data) or qualitative.
Risk Management	The Process responsible for identifying, assessing and controlling Risks. See Risk Assessment.

ITIL® V3 Foundation Course Glossary

Term	Definition
Role	A set of responsibilities, Activities and authorities granted to a person or team. A Role is defined in a Process. One person or team may have multiple Roles, for example the Roles of Configuration Manager and Change Manager may be carried out by a single person.
Rollout	Synonym for Deployment. Most often used to refer to complex or phased Deployments or Deployments to multiple locations.
Root Cause	The underlying or original cause of an Incident or Problem.
Root Cause Analysis (RCA)	An Activity that identifies the Root Cause of an Incident or Problem. RCA typically concentrates on IT Infrastructure failures. See Service Failure Analysis.
Service	A means of delivering value to Customers by facilitating Outcomes Customers want to achieve without the ownership of specific Costs and Risks.
Service Acceptance Criteria (SAC)	A set of criteria used to ensure that an IT Service meets its functionality and Quality Requirements and that the IT Service Provider is ready to Operate the new IT Service when it has been Deployed. See Acceptance.
Service Asset and Configuration Management (SACM)	The Process responsible for both Configuration Management and Asset Management.
Service Capacity Management (SCM)	The Activity responsible for understanding the Performance and Capacity of IT Services. The Resources used by each IT Service and the pattern of usage over time are collected, recorded, and analysed for use in the Capacity Plan. See Business Capacity Management, Component Capacity Management.
Service Catalogue	A database or structured Document with information about all Live IT Services, including those available for Deployment. The Service Catalogue is the only part of the Service Portfolio published to Customers, and is used to support the sale and delivery of IT Services. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request Processes. See Contract Portfolio.
Service Continuity Management	Synonym for IT Service Continuity Management.
Service Contract	A Contract to deliver one or more IT Services. The term Service Contract is also used to mean any Agreement to deliver IT Services, whether this is a legal Contract or an SLA. See Contract Portfolio.

Term	Definition
Service Design	A stage in the Lifecycle of an IT Service. Service Design includes a number of Processes and Functions and is the title of one of the Core ITIL publications. See Design.
Service Design Package	Document(s) defining all aspects of an IT Service and its Requirements through each stage of its Lifecycle. A Service Design Package is produced for each new IT Service, major Change, or IT Service Retirement.
Service Desk	The Single Point of Contact between the Service Provider and the Users. A typical Service Desk manages Incidents and Service Requests, and also handles communication with the Users.
Service Improvement Plan (SIP)	A formal Plan to implement improvements to a Process or IT Service.
Service Knowledge Management System (SKMS)	A set of tools and databases that are used to manage knowledge and information. The SKMS includes the Configuration Management System, as well as other tools and databases. The SKMS stores, manages, updates, and presents all information that an IT Service Provider needs to manage the full Lifecycle of IT Services.
Service Level	Measured and reported achievement against one or more Service Level Targets. The term Service Level is sometimes used informally to mean Service Level Target.
Service Level Agreement (SLA)	An Agreement between an IT Service Provider and a Customer. The SLA describes the IT Service, documents Service Level Targets, and specifies the responsibilities of the IT Service Provider and the Customer. A single SLA may cover multiple IT Services or multiple Customers. See Operational Level Agreement.
Service Level Management (SLM)	The Process responsible for negotiating Service Level Agreements, and ensuring that these are met. SLM is responsible for ensuring that all IT Service Management Processes, Operational Level Agreements, and Underpinning Contracts, are appropriate for the agreed Service Level Targets. SLM monitors and reports on Service Levels, and holds regular Customer reviews.
Service Level Package (SLP)	A defined level of Utility and Warranty for a particular Service Package. Each SLP is designed to meet the needs of a particular Pattern of Business Activity. See Line of Service.
Service Level Requirement (SLR)	A Customer Requirement for an aspect of an IT Service. SLRs are based on Business Objectives and are used to negotiate agreed Service Level Targets.

ITIL® V3 Foundation Course Glossary

Term	Definition
Service Management	Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services.
Service Management Lifecycle	An approach to IT Service Management that emphasizes the importance of coordination and Control across the various Functions, Processes, and Systems necessary to manage the full Lifecycle of IT Services. The Service Management Lifecycle approach considers the Strategy, Design, Transition, Operation and Continuous Improvement of IT Services.
Service Manager	A manager who is responsible for managing the end-to-end Lifecycle of one or more IT Services. The term Service Manager is also used to mean any manager within the IT Service Provider. Most commonly used to refer to a Business Relationship Manager, a Process Manager, an Account Manager or a senior manager with responsibility for IT Services overall.
Service Operation	A stage in the Lifecycle of an IT Service. Service Operation includes a number of Processes and Functions and is the title of one of the Core ITIL publications. See Operation.
Service Owner	A Role which is accountable for the delivery of a specific IT Service.
Service Package	A detailed description of an IT Service that is available to be delivered to Customers. A Service Package includes a Service Level Package and one or more Core Services and Supporting Services.
Service Pipeline	A database or structured Document listing all IT Services that are under consideration or Development, but are not yet available to Customers. The Service Pipeline provides a Business view of possible future IT Services and is part of the Service Portfolio which is not normally published to Customers.
Service Portfolio	The complete set of Services that are managed by a Service Provider. The Service Portfolio is used to manage the entire Lifecycle of all Services, and includes three Categories: Service Pipeline (proposed or in Development); Service Catalogue (Live or available for Deployment); and Retired Services. See Service Portfolio Management, Contract Portfolio.
Service Portfolio Management (SPM)	The Process responsible for managing the Service Portfolio. Service Portfolio Management considers Services in terms of the Business value that they provide.
Service Potential	The total possible value of the overall Capabilities and Resources of the IT Service Provider.

ITIL® V3 Foundation Course Glossary

Term	Definition
Service Provider	An Organization supplying Services to one or more Internal Customers or External Customers. Service Provider is often used as an abbreviation for IT Service Provider. See Type I Service Provider, Type II Service Provider, Type III Service Provider.
Service Request	A request from a User for information, or advice, or for a Standard Change or for Access to an IT Service. For example to reset a password, or to provide standard IT Services for a new User. Service Requests are usually handled by a Service Desk, and do not require an RFC to be submitted. See Request Fulfilment.
Service Strategy	The title of one of the Core ITIL publications. Service Strategy establishes an overall Strategy for IT Services and for IT Service Management.
Service Transition	A stage in the Lifecycle of an IT Service. Service Transition includes a number of Processes and Functions and is the title of one of the Core ITIL publications. See Transition.
Service Utility	The Functionality of an IT Service from the Customer's perspective. The Business value of an IT Service is created by the combination of Service Utility (what the Service does) and Service Warranty (how well it does it). See Utility.
Service Validation and Testing	The Process responsible for Validation and Testing of a new or Changed IT Service. Service Validation and Testing ensures that the IT Service matches its Design Specification and will meet the needs of the Business.
Service Valuation	A measurement of the total Cost of delivering an IT Service, and the total value to the Business of that IT Service. Service Valuation is used to help the Business and the IT Service Provider agree on the value of the IT Service.
Service Warranty	Assurance that an IT Service will meet agreed Requirements. This may be a formal Agreement such as a Service Level Agreement or Contract, or may be a marketing message or brand image. The Business value of an IT Service is created by the combination of Service Utility (what the Service does) and Service Warranty (how well it does it). See Warranty.
Serviceability	The ability of a Third Party Supplier to meet the terms of their Contract. This Contract will include agreed levels of Reliability, Maintainability or Availability for a Configuration Item.
Single Point of Contact	Providing a single consistent way to communicate with an Organization or Business Unit. For example, a Single Point of Contact for an IT Service Provider is usually called a Service Desk.

Term	Definition
SLAM Chart	A Service Level Agreement Monitoring Chart is used to help monitor and report achievements against Service Level Targets. A SLAM Chart is typically colour coded to show whether each agreed Service Level Target has been met, missed, or nearly missed during each of the previous 12 months.
Stakeholder	All people who have an interest in an Organization, Project, IT Service etc. Stakeholders may be interested in the Activities, targets, Resources, or Deliverables. Stakeholders may include Customers, Partners, employees, shareholders, owners, etc. See RACI.
Standard	A mandatory Requirement. Examples include ISO/IEC 20000 (an international Standard), an internal security Standard for Unix configuration, or a government Standard for how financial Records should be maintained. The term Standard is also used to refer to a Code of Practice or Specification published by a Standards Organization such as ISO or BSI. See Guideline.
Standard Change	A pre-approved Change that is low Risk, relatively common and follows a Procedure or Work Instruction. For example password reset or provision of standard equipment to a new employee. RFCs are not required to implement a Standard Change, and they are logged and tracked using a different mechanism, such as a Service Request. See Change Model.
Status	The name of a required field in many types of Record. It shows the current stage in the Lifecycle of the associated Configuration Item, Incident, Problem etc.
Status Accounting	The Activity responsible for recording and reporting the Lifecycle of each Configuration Item.
Strategic	The highest of three levels of Planning and delivery (Strategic, Tactical, Operational). Strategic Activities include Objective setting and long term Planning to achieve the overall Vision.
Supplier	A Third Party responsible for supplying goods or Services that are required to deliver IT services. Examples of suppliers include commodity hardware and software vendors, network and telecom providers, and Outsourcing Organizations. See Underpinning Contract, Supply Chain.
Supplier and Contract Database (SCD)	A database or structured Document used to manage Supplier Contracts throughout their Lifecycle. The SCD contains key Attributes of all Contracts with Suppliers, and should be part of the Service Knowledge Management System.
Supplier Management	The Process responsible for ensuring that all Contracts with Suppliers support the needs of the Business, and that all Suppliers meet their contractual commitments.

ITIL® V3 Foundation Course Glossary

Term	Definition
System	A number of related things that work together to achieve an overall Objective. For example: • A computer System including hardware, software and Applications. • A management System, including multiple Processes that are planned and managed together. For example a Quality Management System. • A Database Management System or Operating System that includes many software modules that are designed to perform a set of related Functions.
Tactical	The middle of three levels of Planning and delivery (Strategic, Tactical, Operational). Tactical Activities include the medium term Plans required to achieve specific Objectives, typically over a period of weeks to months.
Technical Management	The Function responsible for providing technical skills in support of IT Services and management of the IT Infrastructure. Technical Management defines the Roles of Support Groups, as well as the tools, Processes and Procedures required.
Third-line Support	The third level in a hierarchy of Support Groups involved in the resolution of Incidents and investigation of Problems. Each level contains more specialist skills, or has more time or other Resources.
Threat	Anything that might exploit a Vulnerability. Any potential cause of an Incident can be considered to be a Threat. For example a fire is a Threat that could exploit the Vulnerability of flammable floor coverings. This term is commonly used in Information Security Management and IT Service Continuity Management, but also applies to other areas such as Problem and Availability Management.
Threshold	The value of a Metric which should cause an Alert to be generated, or management action to be taken. For example "Priority1 Incident not solved within 4 hours", "more than 5 soft disk errors in an hour", or "more than 10 failed changes in a month".
Total Cost of Ownership (TCO)	A methodology used to help make investment decisions. TCO assesses the full Lifecycle Cost of owning a Configuration Item, not just the initial Cost or purchase price. See Total Cost of Utilization.
Trend Analysis	Analysis of data to identify time related patterns. Trend Analysis is used in Problem Management to identify common Failures or fragile Configuration Items, and in Capacity Management as a Modelling tool to predict future behaviour. It is also used as a management tool for identifying deficiencies in IT Service Management Processes.
Tuning	The Activity responsible for Planning Changes to make the most efficient use of Resources. Tuning is part of Performance Management, which also includes Performance Monitoring and implementation of the required Changes.

ITIL® V3 Foundation Course Glossary

Term	Definition
Type I Service Provider	An Internal Service Provider that is embedded within a Business Unit. There may be several Type I Service Providers within an Organization.
Type II Service Provider	An Internal Service Provider that provides shared IT Services to more than one Business Unit.
Type III Service Provider	A Service Provider that provides IT Services to External Customers.
Underpinning Contract (UC)	A Contract between an IT Service Provider and a Third Party. The Third Party provides goods or Services that support delivery of an IT Service to a Customer. The Underpinning Contract defines targets and responsibilities that are required to meet agreed Service Level Targets in an SLA.
Urgency	A measure of how long it will be until an Incident, Problem or Change has a significant Impact on the Business. For example a high Impact Incident may have low Urgency, if the Impact will not affect the Business until the end of the financial year. Impact and Urgency are used to assign Priority.
User	A person who uses the IT Service on a day-to-day basis. Users are distinct from Customers, as some Customers do not use the IT Service directly.
User Profile (UP)	A pattern of User demand for IT Services. Each User Profile includes one or more Patterns of Business Activity.
Utility	Functionality offered by a Product or Service to meet a particular need. Utility is often summarised as "what it does". See Service Utility.
Value on Investment (VOI)	A measurement of the expected benefit of an investment. VOI considers both financial and intangible benefits. See Return on Investment.
Variable Cost	A Cost that depends on how much the IT Service is used, how many products are produced, the number and type of Users, or something else that cannot be fixed in advance. See Variable Cost Dynamics.
Vision	A description of what the Organization intends to become in the future. A Vision is created by senior management and is used to help influence Culture and Strategic Planning.
Vulnerability	A weakness that could be exploited by a Threat. For example an open firewall port, a password that is never changed, or a flammable carpet. A missing Control is also considered to be a Vulnerability.
Warranty	A promise or guarantee that a product or Service will meet its agreed Requirements. See Service Validation and Testing, Service Warranty.

Term	Definition
Work Instruction	A Document containing detailed instructions that specify exactly what steps to follow to carry out an Activity. A Work Instruction contains much more detail than a Procedure and is only created if very detailed instructions are needed.
Workaround	Reducing or eliminating the Impact of an Incident or Problem for which a full Resolution is not yet available. For example by restarting a failed Configuration Item. Workarounds for Problems are documented in Known Error Records. Workarounds for Incidents that do not have associated Problem Records are documented in the Incident Record.
Workload	The Resources required to deliver an identifiable part of an IT Service. Workloads may be Categorised by Users, groups of Users, or Functions within the IT Service. This is used to assist in analyzing and managing the Capacity, Performance and Utilisation of Configuration Items and IT Services. The term Workload is sometimes used as a synonym for Throughput.