

# ITIL – Service operation glossary

Term	Description
<b>Access management</b>	(Service operation) 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.
<b>Active monitoring</b>	(Service operation) Monitoring of a configuration item or an IT service that uses automated regular checks to discover the current status. See <i>passive monitoring</i> .
<b>Activity</b>	A set of actions designed to achieve a particular result. Activities are usually defined as part of processes or plans, and are documented in procedures.
<b>Alert</b>	(Service operation) 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.
<b>Application</b>	Software that provides functions that are required by an IT service. Each application may be part of more than one IT service. An application runs on one or more servers or clients. See <i>application management</i> , <i>application portfolio</i> .
<b>Application management</b>	(Service design) (Service operation) The function responsible for managing applications throughout their lifecycle.
<b>Assessment</b>	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 <i>audit</i> .
<b>Audit</b>	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 <i>certification</i> , <i>assessment</i> .
<b>Authority matrix</b>	Synonym for RACI.
<b>Automatic Call Distribution (ACD)</b>	(Service operation) Use of information technology to direct an incoming telephone call to the most appropriate person in the shortest possible time. ACD is sometimes called Automated Call Distribution.
<b>Backup</b>	(Service design) (Service operation) Copying data to protect against loss of Integrity or availability of the original.
<b>Best practice</b>	Proven activities or processes that have been successfully used by multiple organisations. ITIL is an example of Best Practice.
<b>British Standards Institution (BSI)</b>	The UK National Standards body, responsible for creating and maintaining British Standards. See <a href="http://www.bsi-global.com">http://www.bsi-global.com</a> for more information. See <i>ISO</i> .
<b>Business process</b>	A process that is owned and carried out by the business. A business process contributes to the delivery of a product or service to a business customer. For example, a retailer may have a purchasing process which helps to deliver services to their business customers. Many business processes rely on IT services.
<b>Business service</b>	An IT service that directly supports a business process, as opposed to an infrastructure service which is used internally by the IT service provider and is not usually visible to the business.  The term business service is also used to mean a service that is delivered to business customers by business units. For example, delivery of financial services to customers of a bank, or goods to the customers of a retail store. Successful delivery of business services often depends on one or more IT services.

Term	Description
<b>Call</b>	(Service operation) A telephone call to the service desk from a user. A call could result in an incident or a service request being logged.
<b>Call centre</b>	(Service operation) An organisation or business unit which handles large numbers of incoming and outgoing telephone calls. See <i>service desk</i> .
<b>Call type</b>	(Service operation) A category that is used to distinguish incoming requests to a service desk. Common call types are incident, service request and complaint.
<b>Change case</b>	(Service operation) A technique used to predict the impact of proposed changes. Change cases use specific scenarios to clarify the scope of proposed changes and to help with cost benefit analysis. See <i>use case</i> .
<b>Chronological analysis</b>	(Service operation) A technique used to help identify possible causes of problems. All available data about the problem is collected and sorted by date and time to provide a detailed timeline. This can make it possible to identify which events may have been triggered by others.
<b>Closed</b>	(Service operation) The final status in the lifecycle of an incident, problem, change etc. When the status is closed, no further action is taken.
<b>Closure</b>	(Service operation) The act of changing the status of an incident, problem, change etc. to closed.
<b>Compliance</b>	Ensuring that a standard or set of guidelines is followed, or that proper, consistent accounting or other practices are being employed.
<b>Component</b>	A general term that is used to mean one part of something more complex. For example, a computer system may be a component of an IT service, an application may be a component of a release unit. Components that need to be managed should be configuration items.
<b>Computer Telephony Integration (CTI)</b>	(Service operation) CTI is a general term covering any kind of integration between computers and telephone systems. It is most commonly used to refer to systems where an application displays detailed screens relating to incoming or outgoing telephone calls. See <i>automatic call distribution, interactive voice response</i> .
<b>Concurrency</b>	A measure of the number of users engaged in the same operation at the same time.
<b>Contract</b>	A legally binding agreement between two or more parties.
<b>Control</b>	A means of managing a risk, ensuring that a business objective is achieved, or ensuring that a process is followed. Example controls include policies, procedures, roles, RAID, door locks etc. A control is sometimes called a countermeasure or safeguard. Control also means to manage the utilization or behaviour of a configuration item, system or IT service.
<b>Control processes</b>	The ISO/IEC 20000 process group that includes change management and configuration management.
<b>Cost</b>	The amount of money spent on a specific activity, IT service, or business unit. Costs consist of real cost (money), notional cost such as people's time, and depreciation.
<b>Cost benefit analysis</b>	An activity that analyses and compares the costs and the benefits involved in one or more alternative courses of action. See <i>business case, net present value, internal rate of return, return on investment, value on investment</i> .
<b>Cost effectiveness</b>	A measure of the balance between the effectiveness and cost of a service, process or activity, a cost effective process is one which achieves its objectives at minimum cost. See <i>KPI, return on investment, value for money</i> .
<b>CRAMM</b>	A methodology and tool for analysing and managing risks. CRAMM was developed by the UK Government, but is now privately owned. Further information is available from <a href="http://www.cramm.com/">http://www.cramm.com/</a> .

Term	Description
<b>Crisis management</b>	The process responsible for managing the wider implications of business continuity. A crisis management team is responsible for strategic issues such as managing media relations and shareholder confidence, and decides when to invoke business continuity plans.
<b>Critical Success Factor (CSF)</b>	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.
<b>Culture</b>	A set of values that is shared by a group of people, including expectations about how people should behave, ideas, beliefs, and practices. See <i>vision</i> .
<b>Customer</b>	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 organisation.
<b>Dashboard</b>	(Service operation) 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.
<b>Data-to-Information-to-Knowledge-to-Wisdom (DIKW)</b>	A way of understanding the relationships between data, information, knowledge, and wisdom. DIKW shows how each of these builds on the others.
<b>Deliverable</b>	Something that must be provided to meet a commitment in a service Level Agreement or a contract. Deliverable is also used in a more informal way to mean a planned output of any process.
<b>Demand management</b>	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 <i>capacity management</i> .
<b>Deming cycle</b>	Synonym for Plan Do Check Act.
<b>Dependency</b>	The direct or indirect reliance of one process or activity upon another.
<b>Detection</b>	(Service operation) 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.
<b>Diagnosis</b>	(Service operation) A stage in the incident and problem lifecycles. The purpose of diagnosis is to identify a workaround for an incident or the root cause of a problem.
<b>Diagnostic script</b>	(Service operation) A structured set of questions used by service desk staff to ensure they ask the correct questions, and to help them classify, resolve and assign incidents. Diagnostic scripts may also be made available to users to help them diagnose and resolve their own incidents.
<b>Directory service</b>	(Service operation) An application that manages information about IT infrastructure available on a network, and corresponding user access rights.
<b>Document</b>	Information in readable form. A document may be paper or electronic. For example, a policy statement, Service Level Agreement, incident record, diagram of computer room layout. See <i>record</i> .
<b>Downtime</b>	(Service design) (Service operation) 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.
<b>Driver</b>	Something that influences strategy, objectives or requirements. For example, new legislation or the actions of competitors.

<b>Error</b>	(Service operation) 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.
<b>Escalation</b>	(Service operation) 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.
<b>Estimation</b>	The use of experience to provide an approximate value for a metric or cost. Estimation is also used in capacity and availability management as the cheapest and least accurate modelling method.
<b>Event</b>	(Service operation) 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.
<b>Event management</b>	(Service operation) The process responsible for managing events throughout their lifecycle. event management is one of the main activities of IT operations.
<b>Exception report</b>	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.
<b>Expanded incident lifecycle</b>	(Availability management) Detailed stages in the lifecycle of an incident. The stages are detection, diagnosis, repair, recovery, restoration. The expanded incident lifecycle is used to help understand all contributions to the impact of incidents and to plan how these could be controlled or reduced.
<b>External customer</b>	A customer who works for a different business to the IT service provider. See <i>external service provider</i> , <i>internal customer</i> .
<b>External metric</b>	A metric that is used to measure the delivery of IT service to a customer. External metrics are usually defined in SLAs and reported to customers. See <i>internal metric</i> .
<b>Facilities management</b>	(Service operation) 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.
<b>Failure</b>	(Service operation) Loss of ability to operate to specification, or to deliver the required output. The term failure may be used when referring to IT services, processes, activities, configuration items etc. A failure often causes an incident.
<b>Fault</b>	Synonym for <i>error</i> .
<b>First line support</b>	(Service operation) The first level in a hierarchy of support groups involved in the resolution of incidents. Each level contains more specialist skills, or has more time or other resources. See <i>escalation</i> .
<b>Fishbone diagram</b>	Synonym for <i>Ishikawa diagram</i> .
<b>Fit for purpose</b>	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.
<b>Follow the sun</b>	(Service operation) 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.
<b>Fulfilment</b>	Performing activities to meet a need or requirement. For example, by providing a new IT service, or meeting a service request.

Term	Description
<b>Function</b>	<p>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.</p> <p>The term function also has two other meanings:</p> <ul style="list-style-type: none"> <li>■ 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.</li> <li>■ To perform the intended purpose correctly, the computer is functioning.</li> </ul>
<b>Functional escalation</b>	(Service operation) Transferring an incident, problem or change to a technical team with a higher level of expertise to assist in an escalation.
<b>Governance</b>	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.
<b>Guideline</b>	A document describing Best Practice, that recommends what should be done. Compliance to a guideline is not normally enforced. See <i>standard</i> .
<b>Help desk</b>	(Service operation) A point of contact for users to log incidents. A help desk is usually more technically focussed than a service desk, and does not provide a single point of contact for all interaction. The term help desk is often used as a synonym for service desk.
<b>Hierarchic escalation</b>	(Service operation) Informing or involving more senior levels of management to assist in an escalation.
<b>Hot standby</b>	Synonym for <i>fast recovery</i> or <i>immediate recovery</i> .
<b>Identity</b>	(Service operation) A unique name that is used to identify a user, person or role. The identity is used to grant rights to that user, person, or role. Example identities might be the username SmithJ or the Role Change Manager.
<b>Impact</b>	(Service operation) (Service transition) 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.
<b>Incident</b>	(Service operation) 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.
<b>Incident management</b>	(Service operation) 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.
<b>Incident record</b>	(Service operation) A record containing the details of an incident. Each incident record documents the lifecycle of a single incident.
<b>Information Technology (IT)</b>	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.
<b>Infrastructure service</b>	An IT service that is not directly used by the business, but is required by the IT service provider, so they can provide other IT services. For example, directory services, naming services, or communication services.
<b>Insourcing</b>	Synonym for <i>internal sourcing</i> .
<b>Interactive Voice Response (IVR)</b>	(Service operation) A form of automatic call distribution that accepts user input, such as key presses and spoken commands, to identify the correct destination for incoming calls.

Term	Description
<b>Internal customer</b>	A customer who works for the same business as the IT service provider. See <i>internal service provider, external customer</i> .
<b>Internal metric</b>	A metric that is used within the IT service provider to monitor the efficiency, effectiveness or cost effectiveness of the IT service provider's internal processes. Internal metrics are not normally reported to the customer of the IT service. See <i>external metric</i> .
<b>International Organisation for Standardisation (ISO)</b>	The International Organisation 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 <a href="http://www.iso.org/">http://www.iso.org/</a> .
<b>International Standards Organisation</b>	See <i>International Organisation for Standardisation (ISO)</i>
<b>Ishikawa diagram</b>	(Service operation) (Continual service improvement) 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.
<b>ISO 9000</b>	A generic term that refers to a number of international standards and guidelines for quality management systems. See <a href="http://www.iso.org/">http://www.iso.org/</a> for more information. See <i>ISO</i> .
<b>ISO 9001</b>	An international standard for quality management systems. See <i>ISO 9000, standard</i> .
<b>ISO/IEC 20000</b>	ISO specification and code of practice for IT service management. ISO/IEC 20000 is aligned with ITIL best practice.
<b>IT infrastructure</b>	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.
<b>IT operations</b>	(Service operation) 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.
<b>IT operations control</b>	(Service operation) The function responsible for monitoring and control of the IT services and IT infrastructure. See <i>operations bridge</i> .
<b>IT operations management</b>	(Service operation) 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.
<b>IT service</b>	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.
<b>IT service Management (ITSM)</b>	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 <i>service management</i> .
<b>IT Service Management Forum (itsmf)</b>	The IT Service Management Forum is an independent organisation dedicated to promoting a professional approach to IT service management. The itsmf is a not for profit membership organisation 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 <a href="http://www.itsmf.com/">http://www.itsmf.com/</a> for more information.

Term	Description
<b>IT Steering Group (ISG)</b>	A formal group that is responsible for ensuring that business and IT service provider strategies and plans are closely aligned. An IT Steering Group includes senior representatives from the business and the IT service provider.
<b>ITIL</b>	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 <a href="http://www.itil.co.uk/">http://www.itil.co.uk/</a> for more information.
<b>Job description</b>	A document which defines the roles, responsibilities, skills and knowledge required by a particular person. One job description can include multiple roles. For example, the roles of Configuration Manager and Change Manager may be carried out by one person.
<b>Job scheduling</b>	(Service operation) Planning and managing the execution of software tasks that are required as part of an IT service. Job scheduling is carried out by IT operations management, and is often automated using software tools that run batch or online tasks at specific times of the day, week, month or year.
<b>Kepner and Tregoe analysis</b>	(Service operation) (Continual service improvement) 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.
<b>Known error</b>	(Service operation) 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.
<b>Known Error Database (KEDB)</b>	(Service operation) 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.
<b>Known error record</b>	(Service operation) 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.
<b>Lifecycle</b>	<p>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:</p> <ul style="list-style-type: none"> <li>■ The lifecycle of an application includes requirements, design, build, deploy, operate, optimise.</li> <li>■ The expanded incident lifecycle includes detect, respond, diagnose, repair, recover, restore.</li> <li>■ The lifecycle of a server may include: ordered, received, in test, live, disposed etc.</li> </ul>
<b>Major incident</b>	(Service operation) The highest category of impact for an incident. A major incident results in significant disruption to the business.
<b>Management information</b>	Information that is used to support decision making by managers. Management information is often generated automatically by tools supporting the various IT service management processes. Management information often includes the values of KPIs, such as percentage of changes leading to incidents or first time fix rate.
<b>Management of Risk (MoR)</b>	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 organisation's business objectives. See <a href="http://www.m-o-r.org/">http://www.m-o-r.org/</a> for more details.
<b>Management system</b>	The framework of policy, processes and functions that ensures an organisation can achieve its objectives.

<b>Term</b>	<b>Description</b>
<b>Manual workaround</b>	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.
<b>Maturity level</b>	A named level in a maturity model, such as the Carnegie Mellon Capability Maturity Model Integration.
<b>Mean Time To Repair (MTTR)</b>	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.
<b>Mean Time to Restore service (MTRS)</b>	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 <i>maintainability, Mean Time to Repair</i> .
<b>Mission statement</b>	The mission statement of an organisation is a short but complete description of the overall purpose and intentions of that organisation. It states what is to be achieved, but not how this should be done.
<b>Model</b>	A representation of a system, process, IT service, configuration item etc., that is used to help understand or predict future behaviour.
<b>Monitor control loop</b>	(Service operation) Monitoring the output of a task, process, IT service or configuration item; comparing this output to a predefined norm; and taking appropriate action based on this comparison.
<b>Monitoring</b>	(Service operation) Repeated observation of a configuration item, IT service or process to detect events and to ensure that the current status is known.
<b>Objective</b>	The defined purpose or aim of a process, an activity or an organisation as a whole. Objectives are usually expressed as measurable targets. The term objective is also informally used to mean a requirement. See <i>outcome</i> .
<b>Office of Government Commerce (OGC)</b>	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.
<b>Office of Public Sector Information (OPSI)</b>	OPSI license the Crown Copyright material used in the ITIL publications. They are a UK Government department, who provide online access to UK legislation, license the re-use of Crown copyright material, manage the Information Fair Trader Scheme, maintain the Government's Information Asset Register and provide advice and guidance on official publishing and Crown copyright.
<b>Operate</b>	To perform as expected. A process or configuration item is said to operate if it is delivering the required outputs. Operate also means to perform one or more operations. For example, to operate a computer is to do the day to day operations needed for it to perform as expected.
<b>Operation</b>	(Service operation) Day to day management of an IT service, system, or other configuration item. Operation is also used to mean any predefined activity or transaction. For example, loading a magnetic tape, accepting money at a point of sale or reading data from a disk drive.
<b>Operational</b>	The lowest of three levels of planning and delivery (strategic, tactical, operational). Operational activities include the day to day or short term planning or delivery of a business process or IT service management process. The term operational is also a synonym for <i>live</i> .
<b>Operational cost</b>	Cost resulting from running the IT services. Often repeating payments. For example, staff costs, hardware maintenance and electricity (also known as current expenditure or revenue expenditure). See <i>capital expenditure</i> .



Term	Description
<b>Operational Expenditure (OPEX)</b>	Synonym for <i>operational cost</i> .
<b>Operations bridge</b>	(Service operation) A physical location where IT services and IT infrastructure are monitored and managed.
<b>Operations control</b>	Synonym for <i>IT operations control</i> .
<b>Operations management</b>	Synonym for <i>IT operations management</i> .
<b>Optimise</b>	Review, plan and request changes, in order to obtain the maximum efficiency and effectiveness from a process, configuration item, application etc.
<b>Organisation</b>	A company, legal entity or other institution. Examples of organisations that are not companies include international standards organisation or itSMF. The term organisation is sometimes used to refer to any entity which has people, resources and budgets. For example, a project or business unit.
<b>Outcome</b>	The result of carrying out an activity; following a process; delivering an IT service etc. The term outcome is used to refer to intended results, as well as to actual results. See <i>objective</i> .
<b>Pain value analysis</b>	(Service operation) 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).
<b>Pareto principle</b>	(Service operation) 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.
<b>Partnership</b>	A relationship between two organisations, 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 <i>value network</i> .
<b>Passive monitoring</b>	(Service operation) Monitoring of a configuration item, an IT service or a process that relies on an alert or notification to discover the current status. See <i>active monitoring</i> .
<b>Performance</b>	A measure of what is achieved or delivered by a system, person, team, process, or IT service.
<b>Plan</b>	A detailed proposal which describes the activities and resources needed to achieve an objective. For example, a plan to implement a new IT service or process. ISO/IEC 20000 requires a plan for the management of each IT service management process.
<b>Planning</b>	An activity responsible for creating one or more plans. For example, capacity planning.
<b>PMBOK</b>	A project management standard maintained and published by the Project Management Institute. PMBOK stands for Project Management Body of Knowledge. See <a href="http://www.pmi.org/">http://www.pmi.org/</a> for more information. See <i>PRINCE2</i> .
<b>Policy</b>	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.
<b>Post Implementation Review (PIR)</b>	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.
<b>Practice</b>	A way of working, or a way in which work must be done. Practices can include activities, processes, functions, standards and guidelines. See <i>best practice</i> .

Term	Description
<b>Prerequisite for Success (PFS)</b>	An activity that needs to be completed, or a condition that needs to be met, to enable successful implementation of a plan or process. A PFS is often an output from one process that is a required input to another process.
<b>PRINCE2</b>	The standard UK government methodology for project management. See <a href="http://www.ogc.gov.uk/prince2/">http://www.ogc.gov.uk/prince2/</a> for more information. See <i>PMBOK</i> .
<b>Priority</b>	(Service Transition) (Service operation) 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.
<b>Proactive monitoring</b>	(Service operation) Monitoring that looks for patterns of events to predict possible future failures. See <i>reactive monitoring</i> .
<b>Proactive problem management</b>	(Service operation) 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.
<b>Problem</b>	(Service operation) 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.
<b>Problem management</b>	(Service operation) 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.
<b>Problem record</b>	(Service operation) A record containing the details of a problem. Each problem record documents the lifecycle of a single problem.
<b>Procedure</b>	A document containing steps that specify how to achieve an activity. Procedures are defined as part of processes. See <i>work instruction</i> .
<b>Process</b>	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.
<b>Process control</b>	The activity of planning and regulating a process, with the objective of performing the process in an effective, efficient, and consistent manner.
<b>Process Manager</b>	A role responsible for operational management of a process. The Process Manager's responsibilities include, planning and coordination 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 organisations.
<b>Process owner</b>	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 organisations.
<b>Production environment</b>	Synonym for <i>live environment</i> .
<b>Pro-forma</b>	A template or example document containing example data that will be replaced with the real values when these are available.
<b>Programme</b>	A number of projects and activities that are planned and managed together to achieve an overall set of related objectives and other outcomes.

<b>Term</b>	<b>Description</b>
<b>Project</b>	A temporary organisation, 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.
<b>Projects IN Controlled Environments (PRINCE2)</b>	See <i>PRINCE2</i> .
<b>Quality</b>	The ability of a product, service, or process to provide the intended value. For example, a hardware component can be considered to be of high quality if it performs as expected and delivers the required reliability. Process quality also requires an ability to monitor effectiveness and efficiency, and to improve them if necessary. See <i>quality management system</i> .
<b>Reactive monitoring</b>	(Service operation) Monitoring that takes action in response to an event. For example, submitting a batch job when the previous job completes, or logging an incident when an error occurs. See <i>proactive monitoring</i> .
<b>Record</b>	A document containing the results or other output from a process or activity. Records are evidence of the fact that an activity took place and may be paper or electronic. For example, an audit report, an incident record, or the minutes of a meeting.
<b>Recovery</b>	(Service design) (Service operation) Returning a configuration item or an IT service to a working state. Recovery of an IT service often includes recovering data to a known consistent state. After recovery, further steps may be needed before the IT service can be made available to the users (restoration).
<b>Recovery Point Objective (RPO)</b>	(Service operation) The maximum amount of data that may be lost when service is restored after an interruption. Recovery Point Objective is expressed as a length of time before the failure. For example, a Recovery Point Objective of one day may be supported by daily backups, and up to 24 hours of data may be lost. Recovery Point Objectives for each IT service should be negotiated, agreed and documented, and used as requirements for service design and IT service continuity plans.
<b>Recovery Time Objective (RTO)</b>	(Service operation) The maximum time allowed for recovery of an IT service following an interruption. The service level to be provided may be less than normal service level targets. Recovery Time Objectives for each IT service should be negotiated, agreed and documented. See <i>business impact analysis</i> .
<b>Redundancy</b>	Synonym for <i>fault tolerance</i> . The term redundant also has a generic meaning of obsolete, or no longer needed.
<b>Relationship</b>	A connection or interaction between two people or things. In business relationship management, it is the interaction between the IT service provider and the business. In configuration management, it is a link between two configuration items that identifies a dependency or connection between them. For example, applications may be linked to the servers they run on, IT services have many links to all the CIs that contribute to them.
<b>Relationship processes</b>	The ISO/IEC 20000 process group that includes business relationship management and supplier management.
<b>Release process</b>	The name used by ISO/IEC 20000 for the process group that includes release management. This group does not include any other processes. Release process is also used as a synonym for release management process.
<b>Repair</b>	(Service operation) The replacement or correction of a failed configuration item.
<b>Request fulfilment</b>	(Service operation) The process responsible for managing the lifecycle of all service requests.

Term	Description
<b>Resolution</b>	(Service operation) Action taken to repair the root cause of an incident or problem, or to implement a workaround. In ISO/IEC 20000, resolution processes is the process group that includes incident and problem management.
<b>Resolution processes</b>	The ISO/IEC 20000 process group that includes incident management and problem management.
<b>Response time</b>	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.
<b>Responsiveness</b>	A measurement of the time taken to respond to something. This could be response time of a transaction, or the speed with which an IT service provider responds to an incident or request for change etc.
<b>Restoration of service</b>	See <i>restore</i> .
<b>Restore</b>	(Service operation) 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.
<b>Review</b>	An evaluation of a change, problem, process, project etc. Reviews are typically carried out at predefined points in the lifecycle, and especially after closure. The purpose of a review is to ensure that all deliverables have been provided, and to identify opportunities for improvement. See <i>post implementation review</i> .
Rights	(Service operation) Entitlements, or permissions, granted to a user or role. For example, the right to modify particular data, or to authorize a change.
<b>Risk</b>	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.
<b>Risk assessment</b>	The initial steps of risk management. Analysing 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.
<b>Risk management</b>	The process responsible for identifying, assessing and controlling risks. See <i>risk assessment</i> .
<b>Role</b>	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.
<b>Root cause</b>	(Service operation) The underlying or original cause of an incident or Problem.
<b>Root Cause Analysis (RCA)</b>	(Service operation) An activity that identifies the root cause of an incident or problem. RCA typically concentrates on IT infrastructure failures. See <i>service failure analysis</i> .
<b>Running costs</b>	Synonym for operational costs.
<b>Scalability</b>	The ability of an IT service, process, configuration item etc., to perform its agreed function when the workload or scope changes.
<b>Scope</b>	The boundary, or extent, to which a process, procedure, certification, contract etc. applies. For example, the scope of change management may include all live IT services and related configuration items, the scope of an ISO/IEC 20000 certificate may include all IT services delivered out of a named data centre.
<b>Second line support</b>	(Service operation) The second 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.

Term	Description
<b>Server</b>	(Service operation) A computer that is connected to a network and provides software functions that are used by other computers.
<b>Service</b>	A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.
<b>Service continuity management</b>	Synonym for IT service continuity management.
<b>Service culture</b>	A customer oriented culture. The major objectives of a service culture are customer satisfaction and helping the customer to achieve their business objectives.
<b>Service desk</b>	(Service operation) 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.
<b>Service level</b>	Measured and reported achievement against one or more service level targets. The term service level is sometimes used informally to mean service level target.
<b>Service maintenance objective</b>	(Service operation) The expected time that a configuration item will be unavailable due to planned maintenance activity.
<b>Service management</b>	Service management is a set of specialized organizational capabilities for providing value to customers in the form of services.
<b>Service management lifecycle</b>	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.
<b>Service Manager</b>	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.
<b>Service operation</b>	(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 <i>operation</i> .
<b>Service request</b>	(Service operation) 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 <i>request fulfilment</i> .
<b>Shift</b>	(Service operation) A group or team of people who carry out a specific role for a fixed period of time. For example, there could be four shifts of IT operations control personnel to support an IT service that is used 24 hours a day.
<b>Single point of contact</b>	(Service operation) Providing a single consistent way to communicate with an organisation or business unit. For example, a single point of contact for an IT service provider is usually called a service desk.
<b>Specification</b>	A formal definition of requirements. A specification may be used to define technical or operational requirements, and may be internal or external. Many public standards consist of a code of practice and a specification. The specification defines the standard against which an organisation can be audited.
<b>Stakeholder</b>	All people who have an interest in an organisation, 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 <i>RACI</i> .

Term	Description
<b>Standard</b>	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 organisation, such as ISO or BSI. See <i>guideline</i> .
<b>Standard Operating Procedures (SOP)</b>	(Service operation) Procedures used by IT operations management.
<b>Status</b>	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.
<b>Storage management</b>	(Service operation) The process responsible for managing the storage and maintenance of data throughout its lifecycle.
<b>Super user</b>	(Service operation) A user who helps other users, and assists in communication with the service desk or other parts of the IT service provider. Super users typically provide support for minor incidents and training.
<b>Support group</b>	(Service operation) A group of people with technical skills. Support groups provide the technical support needed by all of the IT service management processes. See <i>technical management</i> .
<b>Support hours</b>	(Service design) (Service operation) The times or hours when support is available to the users. Typically this is the hours when the Service desk is available. Support hours should be defined in a Service Level Agreement, and may be different from service hours. For example, service hours may be 24 hours a day, but the support hours may be 0700 to 1900.
<b>System</b>	A number of related things that work together to achieve an overall objective. For example: <ul style="list-style-type: none"> <li>■ A computer system, including hardware, software and applications.</li> <li>■ A management system, including multiple processes that are planned and managed together. For example, a quality management system.</li> <li>■ A database management system or operating system that includes many software modules that are designed to perform a set of related functions.</li> </ul>
<b>System management</b>	The part of IT service management that focuses on the management of IT infrastructure rather than process.
<b>Tactical</b>	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.
<b>Technical management</b>	(Service operation) 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.
<b>Third line support</b>	(Service operation) 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.
<b>Threat</b>	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.
<b>Threshold</b>	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 four hours, more than five soft disk errors in an hour, or more than ten failed changes in a month.

Term	Description
<b>Urgency</b>	(Service operation) 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.
<b>User</b>	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.
<b>Value for money</b>	An informal measure of cost effectiveness. Value for money is often based on a comparison with the cost of alternatives. See <i>cost benefit analysis</i> .
<b>Vision</b>	A description of what the organisation intends to become in the future. A vision is created by senior management and is used to help influence culture and strategic planning.
<b>Work in Progress (WIP)</b>	A status that means activities have started but are not yet complete. It is commonly used as a status for incidents, problems, changes etc.
<b>Work instruction</b>	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.
<b>Workaround</b>	(Service operation) 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.
<b>Workload</b>	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 analysing and managing the capacity, performance and utilisation of configuration items and IT services. The term workload is sometimes used as a synonym for throughput.