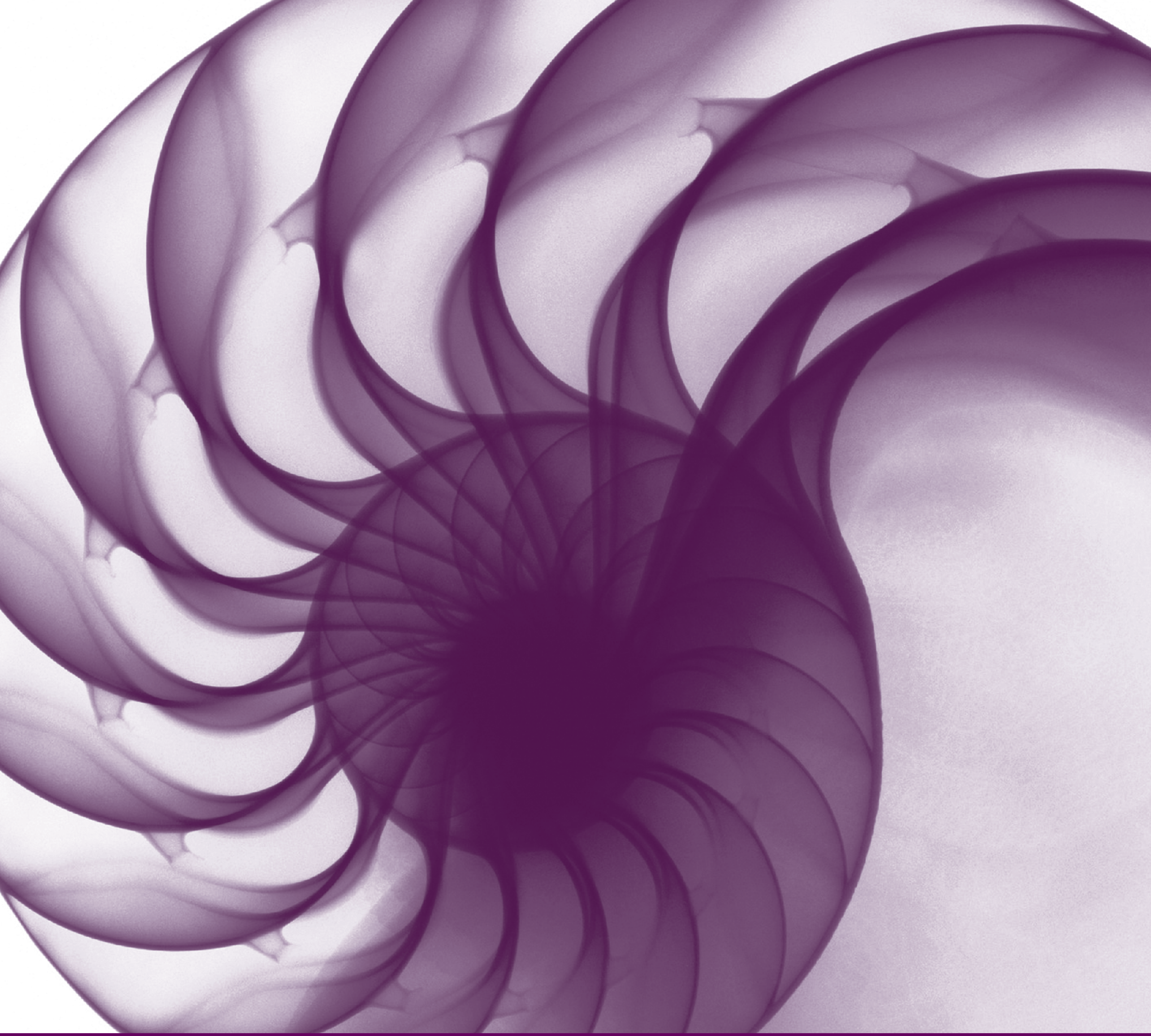


A

Appendix A: The service design package

Appendix A: The service design package

A 'service design package' (SDP) should be produced during the design stage, for each new service, major change to a service or removal of a service or changes to the 'service design package' itself. This pack is then passed from service design to service transition and details all aspects of the service and its requirements through all of the subsequent stages of its lifecycle. The contents of the SDP are shown in Table A.1.

Table A.1 Contents of the service design package

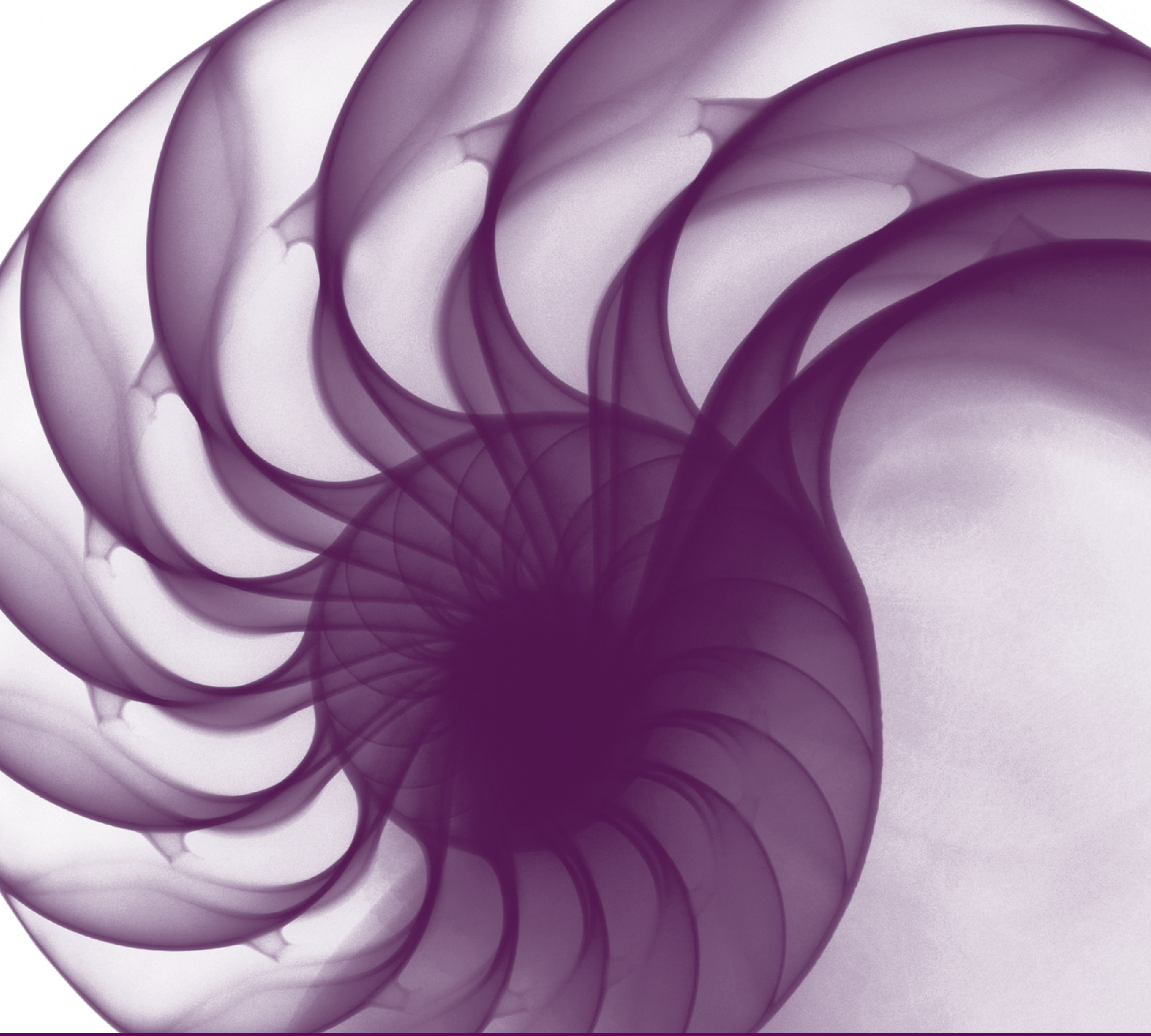
	Sub-category	Description of what is in the SDP
Requirements	Business requirements	The initial agreed and documented business requirements
	Service applicability	This defines how and where the service would be used. This could reference business, customer and user requirements for internal services
	Service contacts	The business contacts, customer contacts and other stakeholders in the service
Service design	Service functional requirements	The changed functionality (utility) of the new or changed service, including its planned outcomes and deliverables, in a formally agreed statement of requirements (SoR)
	Service level requirements	The service level requirements (SLR), representing the desired warranty of the service for a new or changed service. Once specific service level targets have been agreed and validated, the revised or new service level agreement (SLA), including service and quality targets
	Service and operational management requirements	Management requirements to manage the new or changed service and its components, including all supporting services and agreements, control, operation, monitoring, measuring and reporting
	Service design and topology	The design, transition and subsequent implementation and operation of the service solution and its supporting components, including: ■ The service definition, service model, packaging and service options ■ All service components and infrastructure (including hardware, software, networks, environments, data, applications, technology, tools, documentation), including version numbers and relationships, preferably within the configuration management system (CMS) ■ All user, business, service, component, transition, support and operational documentation ■ Processes, procedures, measurements, metrics and reports ■ Supporting products, services, agreements and suppliers
Organizational readiness assessment	Organizational readiness assessment	'Organizational readiness assessment' report and plan, including: business benefit, financial assessment, technical assessment, resource assessment and organizational assessment, together with details of all new skills, competences, capabilities required of the service provider organization, its suppliers, supporting services and contracts

Table continues

Table A.1 continued

	Sub-category	Description of what is in the SDP
Service lifecycle plan	Service programme	An overall programme or plan covering all stages of the lifecycle of the service, including the timescales and phasing, for the transition, operation and subsequent improvement of the new service including: ■ Management, coordination and integration with any other projects, or new or changed activities, services or processes ■ Management of risks and issues ■ Scope, objectives and components of the service ■ Skills, competences, roles and responsibilities ■ Processes required ■ Interfaces and dependencies with other services ■ Management of teams, resources, tools, technology, budgets, facilities required ■ Management of suppliers and contracts ■ Progress reports, reviews and revision of the programme and plans ■ Communication plans and training plans ■ Timescales, deliverables, targets and quality targets for each stage
	Service transition plan	Overall transition strategy, objectives, policy, risk assessment and plans including: ■ Build policy, plans and requirements, including service and component build plans, specifications, control and environments, technology, tools, processes, methods and mechanisms, including all platforms ■ Testing policy, plans and requirements, including test environments, technology, tools, processes, methods and mechanisms ■ Testing must include: ● Functional testing ● Component testing, including all suppliers, contracts and externally provided supporting products and services ● User acceptance and usability testing ● System compatibility and integration testing ● Service and component performance and capacity testing ● Resilience and continuity testing ● Failure, alarm and event categorization, processing and testing ● Service and component, security and integrity testing ● Logistics, release and distribution testing ● Management testing, including control, monitoring, measuring and reporting, together with backup, recovery and all batch scheduling and processing

	Sub-category	Description of what is in the SDP
	Service transition plan *continued*	■ Deployment policy, release policy, plans and requirements, including logistics, deployment, staging, deployment environments, cultural change, organizational change, technology, tools, processes, approach, methods and mechanisms, including all platforms, knowledge, skill and competence transfer and development, supplier and contract transition, data migration and conversion
	Service operational acceptance plan	Overall operational strategy, objectives, policy, risk assessment and plans including: ■ Interface and dependency management and planning ■ Events, reports, service issues, including all changes, releases, resolved incidents, problems and known errors, included within the service; and any errors, issues or non-conformances within the new service ■ Final service acceptance
	Service acceptance criteria	Development and use of service acceptance criteria for progression through each stage of the service lifecycle, including: ■ All environments ■ Guarantee and pilot criteria and periods



Appendix B: Service acceptance criteria

B

Appendix B: Service acceptance criteria

The service acceptance criteria (SAC) comprise a set of criteria used to ensure that a service meets its expected functionality and quality and that the service provider is ready to deliver the new service once it has been deployed. Table B.1 gives examples of such criteria.

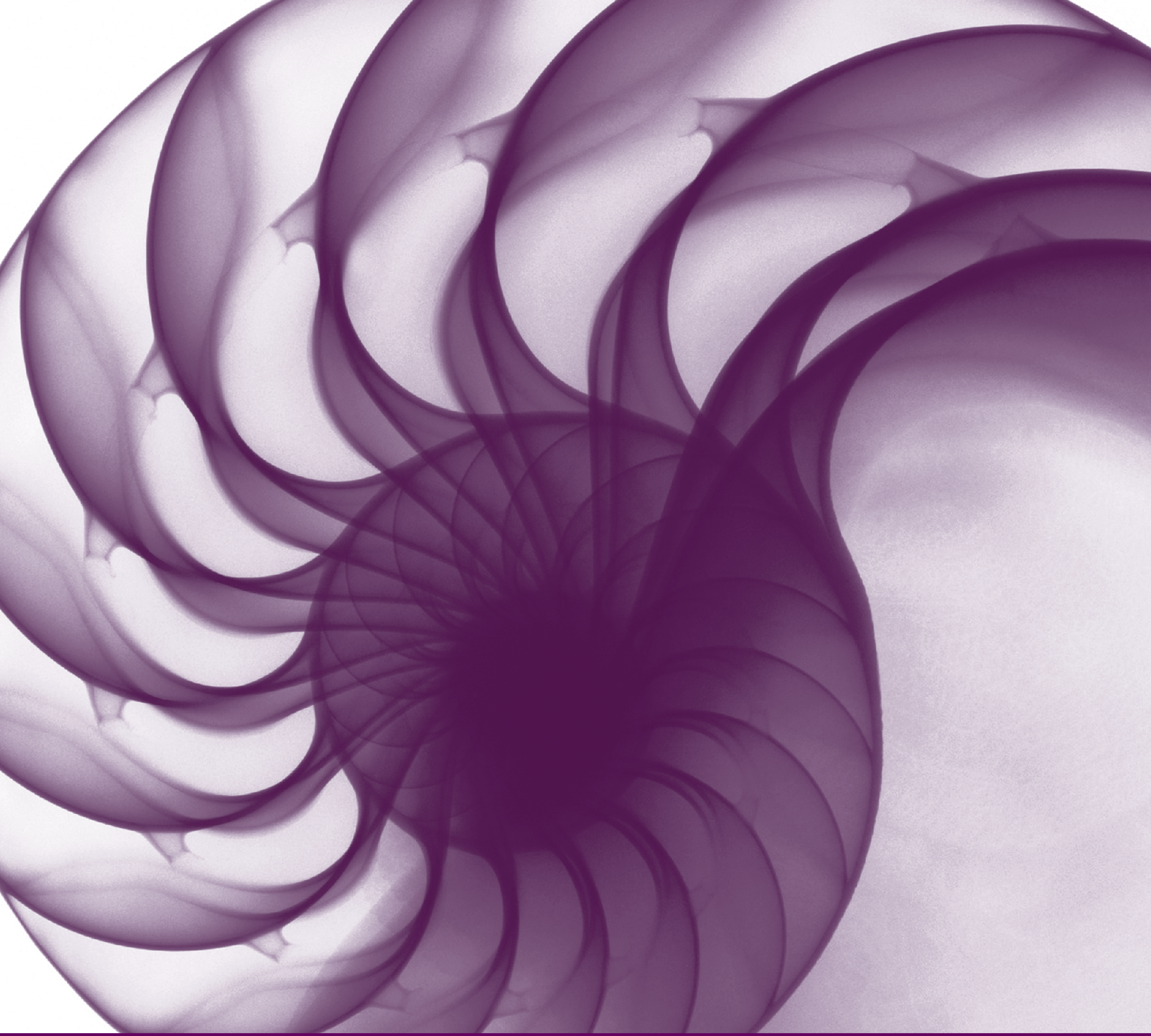
Table B.1 Examples of service acceptance criteria

Criteria	Responsibility
Have the 'go-live' date and the guarantee period been agreed with all concerned parties, together with final acceptance criteria?	Change, service level
Have the deployment project and schedule been documented, agreed and made public to all affected personnel?	Change, incident
Has the service level agreement (SLA)/requirements (SLR) been reviewed, revised and agreed with all concerned parties?	Service level
Has the service been entered/updated in the service catalogue/service portfolio within the configuration management system (CMS) and appropriate relationships established for all supporting components?	Service level, configuration
Have all customers and other stakeholders been identified and recorded in the CMS?	Service level, business relationship
Have all operational risks associated with running the new service been assessed and mitigation actions completed where appropriate?	Business continuity, availability
Have contingency and fail-over measures been successfully tested and added to the overall resilience test schedule?	Business continuity, availability
Can all SLA/SLR targets be monitored, measured, reported and reviewed, including availability and performance?	Service level, availability
Have all users been identified/approved and their appropriate accounts created for them?	Account management
Can all workload characteristics, performance and capacity targets be measured and incorporated into capacity plans?	Capacity
Have all operational processes, schedules and procedures been agreed, tested, documented and accepted (e.g. site documentation, backups, housekeeping, archiving, retention)?	Operations, business continuity
Have all batch jobs and printing requirements been agreed, tested, documented and accepted?	Operations
Have all test plans been completed successfully?	Test manager
Have all security checks and tests been completed successfully?	Security compliance
Are appropriate monitoring and measurement tools and procedures in place to monitor the new service, together with an out-of-hours support rota?	Systems management
Have all ongoing operational workloads and costs been identified and approved?	Operations, IT finance
Are all service and component operational costs understood and incorporated into financial processes and the cost model?	IT finance
Have incident and problem categories and processes been reviewed and revised for the new service, together with any known errors and deficiencies?	Incident, problem reporting

Table continues

Table B.1 ***continued***

Criteria	Responsibility
Have all new suppliers been identified and their associated contracts drawn up accordingly?	Contract and supplier management
Have all support arrangements been reviewed and revised – SLAs, SLRs, operational level agreements (OLAs) – and contracts agreed, with documentation accepted by all teams (including suppliers, support teams, supplier management, development teams and application support)?	Project manager
Has appropriate technical support documentation been provided and accepted by incident, problem and all IT support teams?	Incident, problem
Have all requests for change and release records been authorized and updated?	Change
Have all service, SLA, SLR, OLA and contract details, together with all applications and infrastructure component details, been entered on the CMS?	Project management, support teams configuration
Have appropriate software licences been purchased or reallocated licences used?	Configuration
Have all new hardware components been recorded in the CMS?	Configuration
Have all new software components been lodged in the definitive media library (DML) with details recorded in the CMS?	Configuration
Have all maintenance and upgrade plans been agreed, together with release policies, frequencies and mechanisms?	Release and deployment
Have all users been trained, and has user documentation been accepted and supplied to all users?	Project manager
Are all relationships, interfaces and dependencies with all other internal and external systems and services documented, agreed and supported?	Project manager
Have appropriate business managers signed off acceptance of the new service?	Project manager



Appendix C: Process documentation template

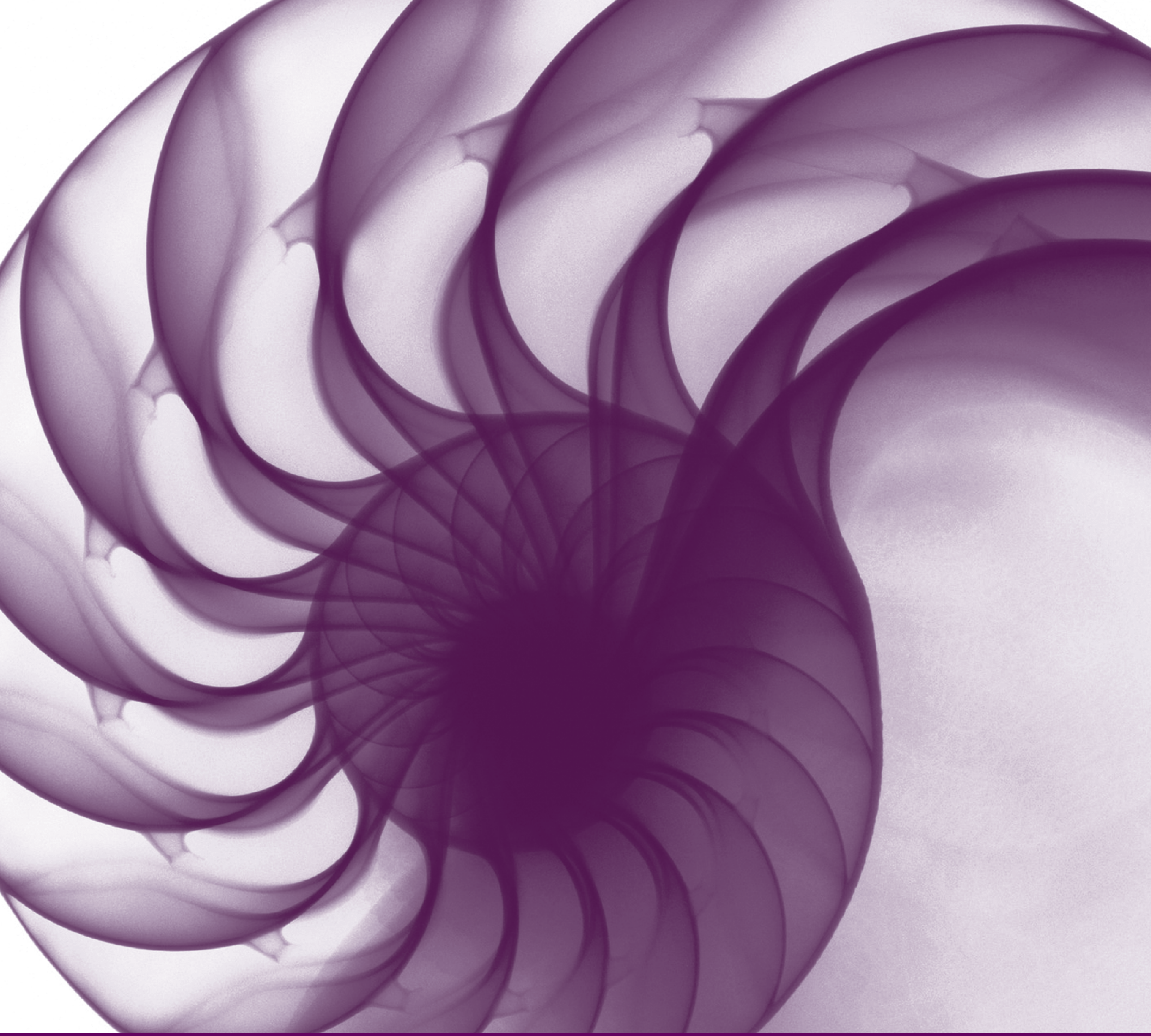
C

Appendix C: Process documentation template

C.1 PROCESS FRAMEWORK

When designing a new or revised process for any of the service management processes, it is recommended that a process specification or framework be produced. The specification should be kept at a fairly high level, but it needs to detail the scope and interfaces of the process. More detailed procedures and work instructions will also be needed to ensure consistency of the process and its application. The typical contents of a process framework or specification are:

- Process name, description and administration (documentation administration: version, change control, author etc.)
- Vision and mission statements
- Objectives
- Scope and terms of reference
- Process overview:
  - Description and overview
  - Inputs
  - Procedures
  - Activities
  - Outputs
  - Triggers
  - Tools and other deliverables
  - Communication and training
- Roles and responsibilities:
  - Operational responsibilities
  - Process owner
  - Process members
  - Process users
  - Other roles
- Associated documentation and references
- Interfaces and dependencies to:
  - Other service management processes
  - Other IT processes
  - Business processes
- Process measurements and metrics:
  - Critical success factors
  - Key performance indicators
  - Process reviews, assessments and audits
- Deliverables and reports produced by the process:
  - Frequency
  - Content
  - Distribution
- Glossary, abbreviations and references.



Appendix D: Design and planning documents and their contents

D

Appendix D: Design and planning documents and their contents

This appendix contains suggested details of the types of design documents, plans and standards documents that should be produced and maintained by IT, and also outlines the minimum contents of IT architectures and plans. However, it should be stressed again that all these documents should be frequently and regularly reviewed and revised and should be actively used within everyday IT processes and procedures.

They must also be maintained in alignment with all similar documents in use within the business and the overall organization.

D.1 DESIGN AND ARCHITECTURAL DOCUMENTS AND STANDARDS

The design documents and standards developed and maintained by IT should include:

- Design and planning standards, policies, processes and procedures
- Application architectures, design methods and standards
- Business requirements, business impact assessment and prioritization and business case methods and standards
- Functional requirements standards
- Statements of requirements (SoR) and invitations to tender (ITT) standards and methods for their evaluation
- IT technology architectures, design standards and policies, covering all areas of technology, including mainframe, server, desktop, laptop, hand-held and mobile devices, telephony systems, storage, backup, network and network addressing
- Operating systems, systems software, utilities and firmware architectures, design policies and standards
- Data, information and database architectures, design policies and standards, including information flows, knowledge management, information security and access, data management, data storage, data warehousing, data analysis and data mining
- Management systems, platforms, tools and agents and their architectures and design polices and standards, including functionality, domains, interfaces, management protocols, event and alarm handling and categorization, automation and escalation
- Cabling architectures, designs and standards
- Development standards, methods and policies
- Testing methods, polices and standards
- Handover, acceptance and sign-off standards and methods
- Partner, supplier and contract standards and policies
- Communications policies and standards
- Document and document library standards and policies
- Internet and intranet architectures, design standards and policies, including e-commerce and e-business
- Email and groupware architectures, design standards and policies
- Environmental requirements, design policies and standards
- IT security design policies and standards, including firewalling, virus checking, service and system access levels, methods and policies, remote access, user account and password management
- Procurement standards and policies
- Programme standards and policies, project methods and project planning and review policies and standards
- Quality standards and policies
- User interfaces and standards.

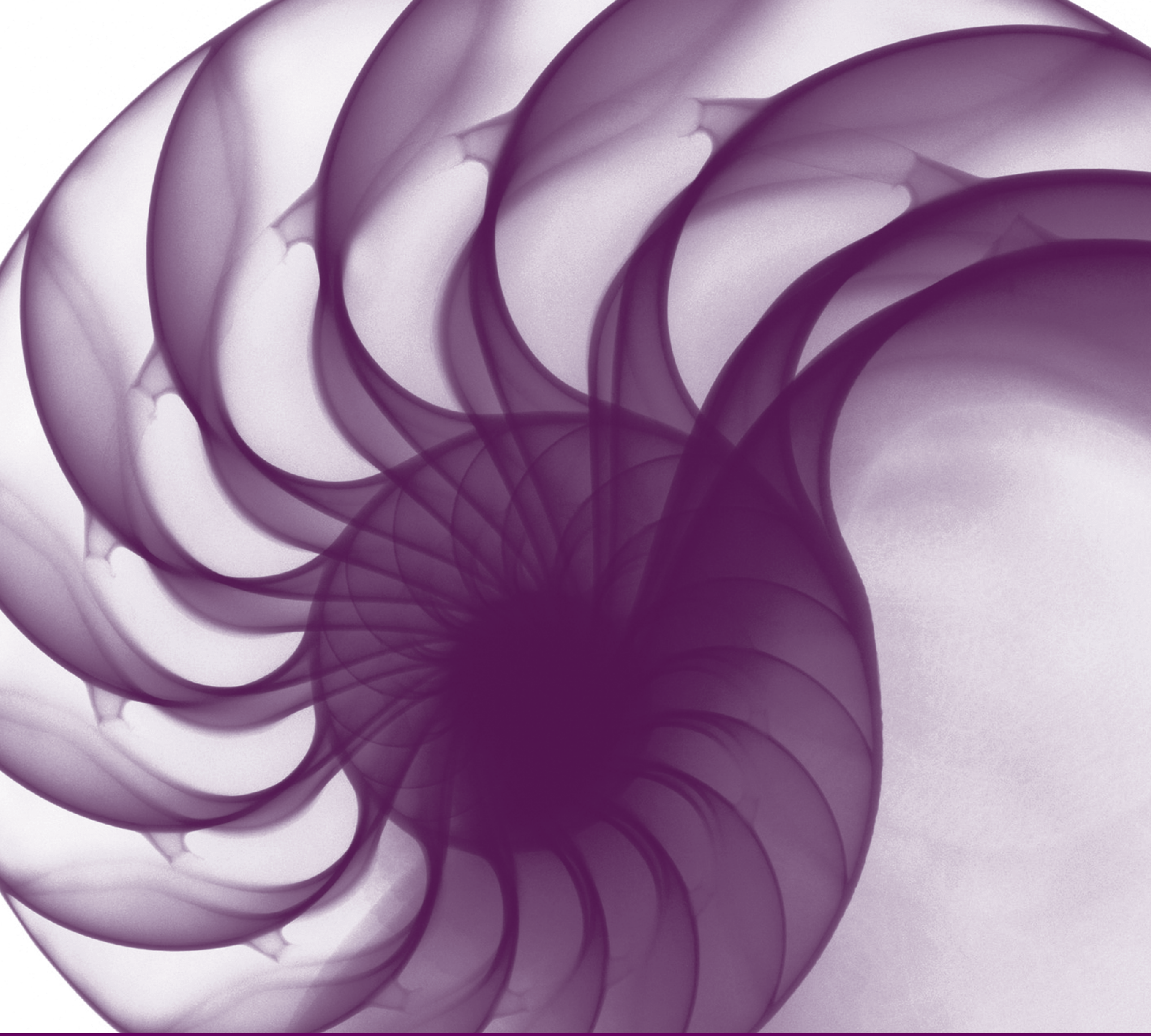
D.2 IT PLANS

IT should produce and maintain a number of plans in order to coordinate and manage the overall development and quality of IT services. These should include:

- **IT business plans** The business plans for the development of IT services

- **Strategic plans** Providing plans for the achievement of the long-term vision, mission and objectives of IT
- **Tactical plans** Providing plans for the achievement of the short- and medium-term vision, mission and objectives of ICT
- **Functional plans** Providing plans for the achievement of the vision, mission and objectives of key IT functions
- **Operational plans** Providing plans for the development and improvement of operational processes, procedures and methods
- **Project plans and programmes**:
  - IT and business programmes
  - IT projects
- **Processes plans and programmes**:
  - Objectives and targets
  - Process improvement
  - Roles and responsibilities
- **Transition plans**:
  - Build plans and schedules
  - Testing and release schedules
  - Development and test environments
  - Transition schedules
- **Service management plans**:
  - Service quality plan(s)
  - Service improvement plans and programmes
  - Financial plans and budgets
  - IT service continuity and recovery plans and business continuity plans
  - Capacity plan
  - Availability plan
  - Service support plans
  - Release plans and schedules
  - Service asset and configuration management plans
  - Change management plans and the change schedule
  - Service desk, incident management and problem management plans
  - Supplier and contract plans.

All IT plans should be developed, maintained and reviewed in line within the business and the overall organization. This should be achieved using the impact assessment process of a suitable change management system. Organizations should take the legal requirements for systems into consideration and also look into international and national standards and regulation and the need for corporate governance.



Appendix E: Environmental architectures and standards

E

Appendix E: Environmental architectures and standards

This appendix contains details of environmental architectures and standards. Every organization should produce an environmental policy for equipment location, with minimum agreed standards for particular concentrations of equipment. Additionally, minimum standards should be agreed for the protection of buildings containing equipment and equipment room shells.

Tables E.1–E.6 cover the major aspects that need to be considered, with example characteristics.

Note: This section is concerned with items that require attention in design. It is not intended to cover all the related concerns of the facilities management function, which is covered in Appendix E of *ITIL Service Operation*. However, a review of this related area may yield additional ideas for design.

Table E.1 Building/site

Access	Secure perimeters, secure entrances, audit trail
Building and site protection	Security fencing, video cameras, movement and intruder detectors, window and door alarms, lightning protectors, good working environment (standard)
Entry	Multiple controlled points of entry
External environment	Safeguards to minimize external risks such as floods, electrical storms or hurricanes
Services	Where possible and justifiable, alternative routes and suppliers for all essential services, including network services

Table E.2 Major equipment room

Access	Secure controlled entry, combination lock, swipe card, video camera (if business critical and unattended)
Location	First floor wherever possible, with no water, gas, chemical or fire hazards within the vicinity, above, below or adjacent
Temperature	Strict control, 22°C (± 3°C). Provide for up to 550 W/m^2. 6°C variation throughout the room and a maximum of 6°C per hour
Visibility	No signage, no external windows
Shell	External shell: waterproof, airtight, soundproofed, fire-resistant (0.5 hours to 4 hours depending on criticality)
Equipment delivery	Adequate provision should be made for the delivery and positioning of large delicate equipment
Internal floor	Sealed
Separate plant room	Uninterruptible power supply (UPS). Electrical supply and switching, air-handling units, dual units and rooms if business critical
Fire extinguishers	Sufficient electrical fire extinguishers with adequate signage and procedures
External	Generator for major data centres and business-critical systems

Table continues

Table E.3 Major data centres

Access	Secure controlled entry, combination lock, swipe card, video camera (if business critical and unattended)
Temperature	Strict control, 22°C (± 3°C). Provide for up to 550 W/m^2. 6°C variation throughout the room and a maximum of 6°C per hour
Humidity control	Strict control: 50% (± 10%)
Air quality	Positive pressure, filtered intake, low gaseous pollution (e.g. sulphur dioxide ≤ 0.14 ppm), dust levels for particles > 1 micron, less than 5 × 106 particles/m^3. Auto shut-down on smoke or fire detection
Power	Power distribution unit (PDU), with three-phase supply to non-switched boxes, one per piece of equipment, with appropriate rated circuit-breakers for each supply. Alternatively, approved power distribution strips can be used. Balanced three-phase loadings. UPS (online or line interactive with simple network management protocol [SNMP] management) to ensure voltage supplied is within ± 5% of rating with minimal impulse, sags, surges and over/under voltage conditions
False floors	Antistatic, liftable floor tiles 600 × 600 mm on pedestals, with alternate pedestals screwed to the solid floor. Minimum of 600 mm clearance to solid floor. Floor loadings of up to 5 kN/m^2 with a recommended minimum of 3 m between false floor and ceiling
Internal walls	From false floor to ceiling, fire-resistant, but with air flow above and below floor level
Fire detection/ prevention	HSSD or VESDA multi-level alarm with auto FM200 (or alternative halon replacement) release on 'double-knock' detection
Environmental detectors	For smoke, temperature, power, humidity, water and intruder with automated alarm capability. Local alarm panels with repeater panels and also remote alarm capability
Lighting	Normal levels of ceiling lighting with emergency lighting on power failure
Power safety	Clean earth should be provided on the PDU and for all equipment. Clearly marked remote power-off buttons on each exit. Dirty power outlets, clearly marked, should also be supplied
Fire extinguishers	Sufficient electrical fire extinguishers with adequate signage and procedures
Vibration	Vibrations should be minimal within the complete area
Electromagnetic interference	Minimal interference should be present (1.5 V/m ambient field strength)
Installations	All equipment should be provided and installed by qualified suppliers and installers to appropriate electrical and health and safety standards
Network connections	The equipment space should be flood-wired with adequate capacity for reasonable growth. All cables should be positioned and secured to appropriate cable trays
Disaster recovery	Fully tested recovery plans should be developed for all major data centres including the use of stand-by sites and equipment

Table E.4 Regional data centres and major equipment centres

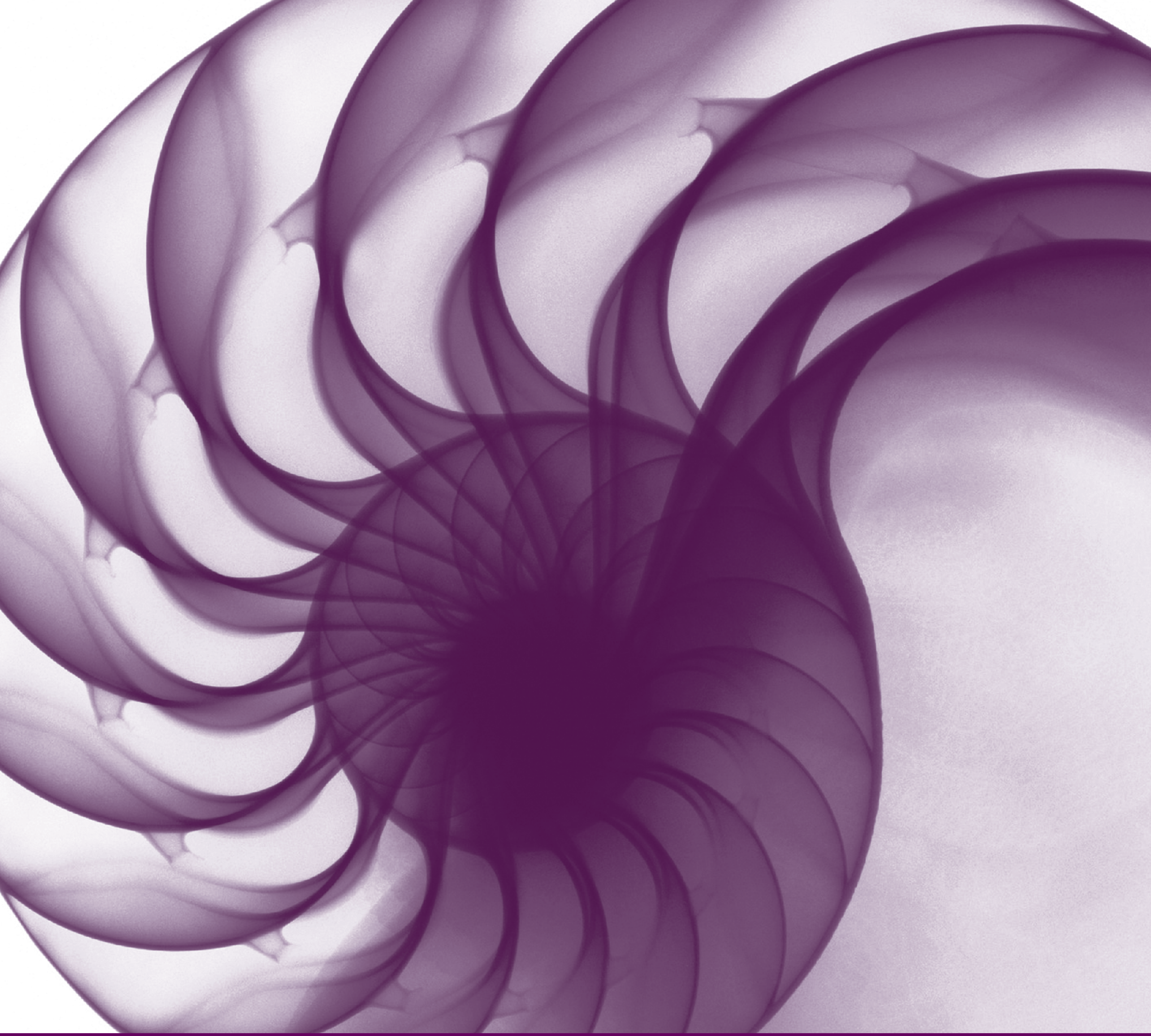
Access	Secure controlled entry, combination lock, swipe card, video camera (if business critical and unattended)
Temperature	Temperature control, 22°C (± 5°C), preferable
Humidity control	Strict control: 50% (± 10%) preferable
Air quality	Positive pressure, filtered intake, low gaseous pollution (e.g. sulphur dioxide ≤ 0.14 ppm), dust levels for particles > 1 micron, less than 5 × 106 particles/m^3. Auto shut-down on smoke or fire detection
Power	PDU with three-phase supply to non-switched boxes, one per piece of equipment, with appropriate rated circuit-breakers for each supply. Alternatively, approved power distribution strips can be used. Balanced three-phase loadings. Room UPS to ensure voltage supplied is within ± 5% of rating with minimal impulse, sags, surges and over/under voltage conditions
False floors	Antistatic, liftable floor tiles 600 × 600 mm on pedestals, with alternate pedestals screwed to the solid floor. Minimum of 600 mm clearance to solid floor. Floor loadings of up to 5 kN/m^2 with a recommended minimum of 3 m between false floor and ceiling
Internal walls	From false floor to ceiling, fire-resistant, but with air flow above and below floor level
Fire detection/ prevention	Generally fire detection but not suppression, although HSSD or VESDA multi-level alarm with auto FM200 (or alternative halon replacement) release on 'double-knock' detection may be included if business-critical systems are contained
Environmental detectors	For smoke, temperature, power, humidity, water and intruder with automated alarm capability
Lighting	Normal levels of ceiling lighting with emergency lighting on power failure
Power safety	Clean earth should be provided on the PDU and for all equipment. Clearly marked remote power-off buttons on each exit. Dirty power outlets, clearly marked, should also be supplied
Fire extinguishers	Sufficient electrical fire extinguishers with adequate signage and procedures
Vibration	Vibrations should be minimal within the complete area
Electromagnetic interference	Minimal interference should be present (1.5 V/m ambient field strength)
Installations	All equipment should be provided and installed by qualified suppliers and installers to appropriate electrical and health and safety standards
Network connections	The equipment space should be flood-wired with adequate capacity for reasonable growth. All cables should be positioned and secured to appropriate cable trays
Disaster recovery	Fully tested recovery plans should be developed for all regional data centres, including the use of stand-by sites and equipment where appropriate

Table E.5 Server or network equipment rooms

Access	Secure controlled entry, by combination lock, swipe card or lock and key. In some cases equipment may be contained in open offices in locked racks or cabinets
Temperature	Normal office environment, but if in closed/locked rooms adequate ventilation should be provided
Humidity control	Normal office environment
Air quality	Normal office environment
Power	Clean power supply with a UPS-supplied power to the complete rack
False floors	Recommended minimum of 3 m between floor and ceiling with all cables secured in multi-compartment trunking
Internal walls	Wherever possible all walls should be fire-resistant
Fire detection/prevention	Normal office smoke/fire detection systems, unless major concentrations of equipment
Environmental detectors	For smoke, power, intruder with audible alarm capability
Lighting	Normal levels of ceiling lighting with emergency lighting on power failure
Power safety	Clean earth should be provided for all equipment, with clearly marked power-off buttons
Fire extinguishers	Sufficient electrical fire extinguishers, with adequate signage and procedures
Vibration	Vibrations should be minimal within the complete area
Electromagnetic interference	Minimal interference should be present (1.5 V/m ambient field strength)
Installations	All equipment should be provided and installed by qualified suppliers and installers to appropriate electrical and health and safety standards
Network connections	The equipment space should be flood-wired with adequate capacity for reasonable growth. All cables should be positioned and secured to appropriate cable trays
Disaster recovery	Fully tested recovery plans should be developed where appropriate

Table E.6 Office environments

Access	All offices should have the appropriate secure access depending on the business, the information and the equipment contained within them
Lighting, temperature, humidity and air quality	A normal clean, comfortable and tidy office environment, conforming to the organization's health, safety and environmental requirements
Power	Clean power supply for all computer equipment, with UPS facilities if appropriate
False floors	Preferred if possible, but all cables should be contained within appropriate trunking
Fire detection/ prevention and extinguishers	Normal office smoke/fire detection systems and intruder alerting systems, unless there are major concentrations of equipment. Sufficient fire extinguishers of the appropriate type, with adequate signage and procedures
Network connections	The office space should preferably be flood-wired with adequate capacity for reasonable growth. All cables should be positioned and secured to appropriate cable trays. All network equipment should be secured in secure cupboards or cabinets
Disaster recovery	Fully tested recovery plans should be developed where appropriate



Appendix F: Sample service level agreement and operational level agreement

F

Appendix F: Sample service level agreement and operational level agreement

This appendix contains examples of a service level agreement (SLA) and an operational level agreement (OLA) and their contents. It is not recommended that every SLA or OLA should necessarily contain all of the sections listed within the following sample documents. It is suggested that these areas are considered when preparing document templates, but that they are only incorporated into the actual documents themselves where they are appropriate and relevant. So the following outlines should only be considered as guidelines or checklists.

F.1 SAMPLE SERVICE LEVEL AGREEMENT

This agreement is made between .... and ....

The agreement covers the provision and support of the ABC services which .... (brief service description).

This agreement remains valid for 12 months from (date) until (date). The agreement will be reviewed annually. Minor changes may be recorded on the form at the end of the agreement, provided they are mutually endorsed by the two parties and managed through the change management process.

Signatories:

Name .... Position .... Date ....

Name .... Position .... Date ....

Service description

The ABC service consists of .... (a fuller description to include key business functions, deliverables and all relevant information to describe the service and its scale, impact and priority for the business).

Scope of the agreement

What is covered within the agreement and what is excluded?

Service hours

A description of the hours that the customers can expect the service to be available (e.g. 7 × 24 × 365, 08:00 to 18:00, Monday to Friday).

Special conditions for exceptions (e.g. weekends, public holidays) and procedures for requesting service extensions (whom to contact – normally the service desk – and what notice periods are required).

This could include a service calendar or reference to a service calendar.

Details of any pre-agreed maintenance or housekeeping slots, if these impact on service hours, together with details of how any other potential outages must be negotiated and agreed – by whom and notice periods etc.

Procedures for requesting permanent changes to service hours.

Functionality (if appropriate)

Details of the minimal functionality to be provided and the number of errors of particular types that can be tolerated before the SLA is breached. Should include severity levels and the reporting period.

Service availability

The target availability levels that the IT service provider will seek to deliver within the agreed service hours. Availability targets within agreed service hours, normally expressed as percentages (e.g. 99.5%), measurement periods, method and calculations must be stipulated. This figure may be expressed for the overall service, supporting services and critical components or all three. However, it is difficult to relate such simplistic percentage availability figures to service quality, or to customer business activities. It is therefore often better to try to measure service unavailability in terms of the customer's inability to conduct its business activities. For example, 'sales are immediately affected by a failure of IT to provide an adequate Point of Sale (PoS) support service'. This strong link between the IT service and the customer's business processes is a sign of maturity in both the service level management and the availability management processes.

Agreed details of how and at what point this will be measured and reported, and over what agreed period, should also be documented.

Reliability

The maximum number of service breaks that can be tolerated within an agreed period (may be defined either as number of breaks (for example, four per annum) or as a mean time between failures (MTBFs) or mean time between service incidents (MTBSIs)).

Definition of what constitutes a 'break' and how these will be monitored and recorded.

Service performance

Details of the expected responsiveness of the IT service (such as target workstation response times for average, or maximum workstation response times, sometimes expressed as a percentile, e.g. 95% within two seconds), details of expected service throughput on which targets are based, and any thresholds that would invalidate the targets).

This should include indication of likely traffic volumes, throughput activity, constraints and dependencies (e.g. the number of transactions to be processed, number of concurrent users, and amount of data to be transmitted over the network). This is important so that performance issues that have been caused by excessive throughput outside the terms of the agreement may be identified.

Batch turnaround times

If appropriate, details of any batch turnaround times, completion times and key deliverables, including times for delivery of input and the time and place for delivery of output where appropriate.

Service continuity

Brief mention of and/or reference out to the organization's service continuity plans, together with details of how the SLA might be affected or reference to a separate continuity SLA, containing details of any diminished or amended service targets should a disaster situation occur. Details of any specific responsibilities on both sides (e.g. data backup, off-site storage). Also details of the invocation of plans and coverage of any security issues, particularly any customer responsibilities (e.g. coordination of business activities, business documentation, backup of freestanding PCs, password changes).

Security

Brief mention of and/or reference out to the organization's security policy (covering issues such as password controls, security violations, unauthorized software, viruses etc.). Details of any specific responsibilities on both sides (e.g. virus protection, firewalls).

Customer support

Details of how to contact the service desk, the hours it will be available, the hours support is available and what to do outside these hours to obtain assistance (e.g. on-call support, third-party assistance etc.) must be documented. The SLA may also include reference to internet/intranet self help and/or incident logging. Metrics and measurements should be included such as telephone call answer targets (number of rings, missed calls etc.)

Targets for incident response times (how long will it be before someone starts to assist the customer – may include travelling time etc.) should be provided. A definition is needed of 'response' (Is it a telephone call back to the customer or a site visit?) as appropriate.

Arrangements for requesting support extensions, including required notice periods (e.g. request must be made to the service desk by 12 noon for an evening extension, by 12 noon on Thursday for a weekend extension) should be specified. Note that:

- Both incident response and resolution times will be based on whatever incident impact/priority codes are used – details of the classification of incidents should also be included here.
- In some cases, it may be appropriate to reference out to third-party contacts and contracts and OLAs – but not as a way of diverting responsibility.

Contact points and escalation

Details of the contacts within each of the parties involved in the agreement and the escalation processes and contact points. This should also include the definition of a complaint and procedure for managing complaints.

Change management

Brief mention of and/or reference out to the organization's change management procedures that must be followed – just to reinforce compliance. Also targets for approving, handling and implementing requests for change, usually based on the category or urgency/priority of the change, should be included, as well as details of any known changes that will impact on the agreement, if any.

Printing

Details of any special conditions relating to printing or printers (e.g. print distribution details, notification of large centralized print runs, or handling of any special high-value stationery).

Responsibilities

Details of the responsibilities of the various parties involved within the service and their agreed responsibilities, including the service provider, the customer and the users.

Charging (if applicable)

Details of any charging formulas used, charging periods, or reference out to charging policy documents, together with invoicing procedures and payment conditions etc. must be included. This should also include details of any financial penalties or bonuses that will be paid if service targets do not meet expectations. What will the penalties/bonuses be and how will they be calculated, agreed and collected/paid (more appropriate for third-party situations)? If the SLA covers an outsourcing relationship, charges should be detailed in an appendix as they are often covered by commercial in-confidence provisions.

It should be noted that penalty clauses can create their own difficulties. They can prove a barrier to partnerships if unfairly invoked on a technicality and can also make service provider staff unwilling to admit to mistakes for fear of penalties being imposed. This can, unless used properly, be a barrier to developing effective relationships and problem solving.

Service reporting and reviewing

The content, frequency, timing and distribution of service reports, and the frequency of associated service review meetings. Also details of how and when SLAs and the associated service targets will be reviewed and possibly revised, including who will be involved and in what capacity.

Glossary

Explanation of any unavoidable abbreviations or terminology used, to assist customer understanding.

Amendment sheet

To include a record of any agreed amendments, with details of amendments, dates and signatories. It should also contain details of a complete change history of the document and its revisions.

It should be noted that the SLA contents given above are examples only. They should not be regarded as exhaustive or mandatory, but they provide a good starting point.

F.2 SAMPLE OPERATIONAL LEVEL AGREEMENT

This agreement is made between .... and ....

The agreement covers the provision of the support service providing .... (brief service description).

This agreement remains valid for 12 months from (date) until (date).

The agreement will be reviewed annually. Minor changes may be recorded on the form at the end of the agreement, provided they are mutually endorsed by the two parties and managed through the change management process.

Signatories:

Name .... Position .... Date ....

Name .... Position .... Date ....

Details of previous amendments

Support service description

Comprehensive explanation and details of the support service being provided.

Scope of the agreement

What is covered within the agreement and what is excluded.

Service hours

A description of the hours for which the support service is provided.

Service targets

The targets for the provision of the support service and the reporting and reviewing processes and frequency.

Contact points and escalation

Details of the contacts within each of the parties involved within the agreement, and the escalation processes and contact points.

Service desk and incident response times and responsibilities

The responsibilities and targets agreed for the progress and resolution of incidents and for support by the service desk.

Problem response times and responsibilities

The responsibilities and targets agreed for the progress and resolution of problems.

Change management

The responsibilities and targets agreed for the progress and implementation of changes.

Release and deployment management

The responsibilities and targets agreed for the progress and implementation of releases.

Service asset and configuration management

The responsibilities for the ownership, provision and maintenance of accurate service asset and configuration management information.

Information security management

The responsibilities and targets agreed for the support of the security policy(s) and the information security management process.

Availability management

Responsibility for ensuring that all components within their support domain are managed and supported to meet and continue to meet all of the service and component availability targets.

IT service continuity management

Responsibility for ensuring that all components within their support domain have up-to-date and tested recovery plans that support agreed and documented business requirements. This should include assistance with the technical assessment of risk and its subsequent management and mitigation.

Capacity management

Responsibility for supporting the needs of the capacity management process within the agreed scope of their technical domain.

Service level management

Assistance with the definition and agreement of appropriate targets within SLAs, service level requirements and OLAs, concerning components within the scope of their technical domain.

Supplier management

Assistance with the management of contracts and suppliers, again principally within the scope of their technical domain.

Provision of information

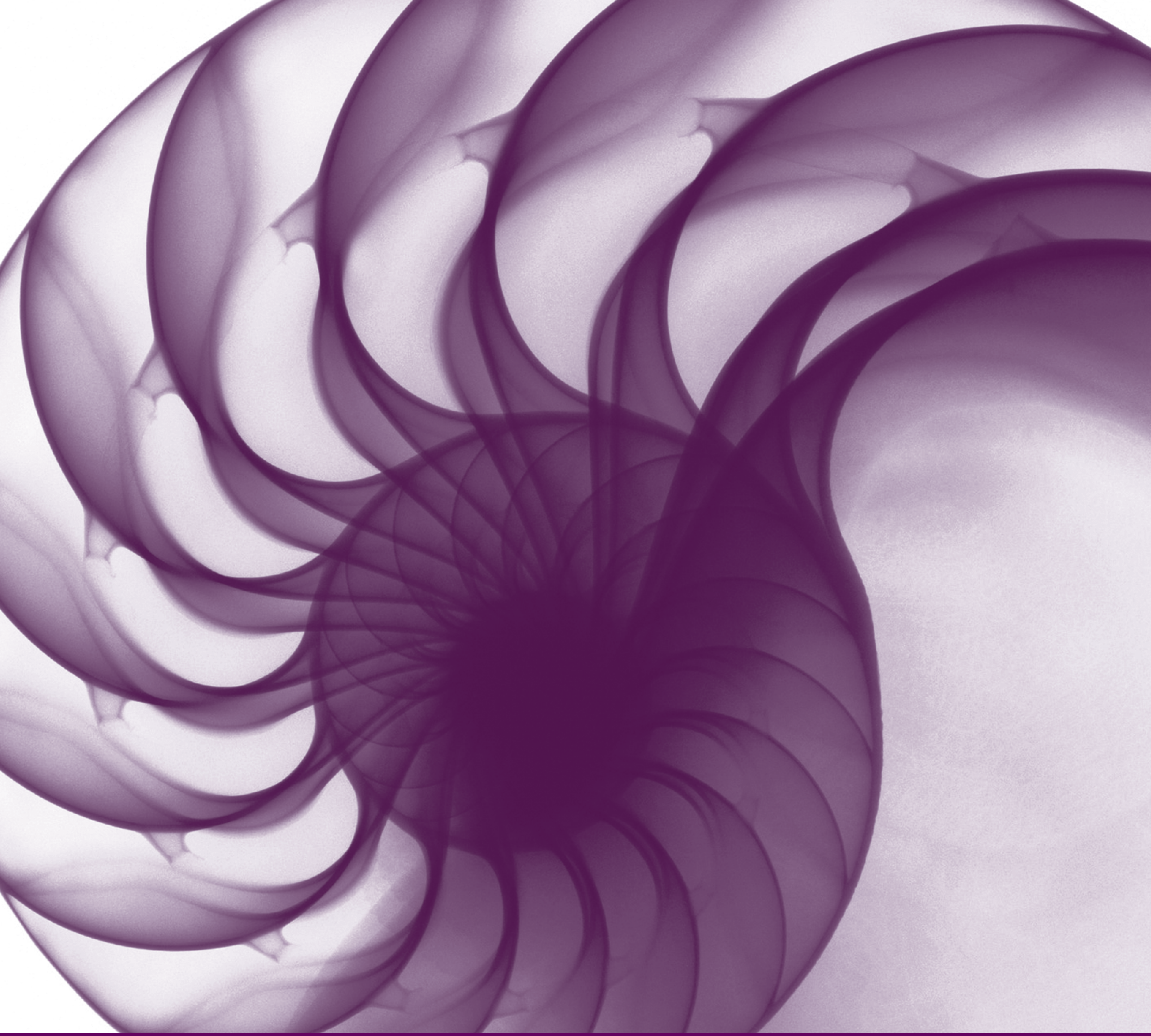
The provision and maintenance of accurate information, including financial data for all components within the agreed scope of their technical domain.

Glossary

Explanation of any unavoidable abbreviations or terminology used, to assist understanding of terms contained within the agreement.

Amendment sheet

To include a record of any agreed amendments, with details of amendments, dates and signatories. It should also contain details of a complete change history of the document and its revisions.



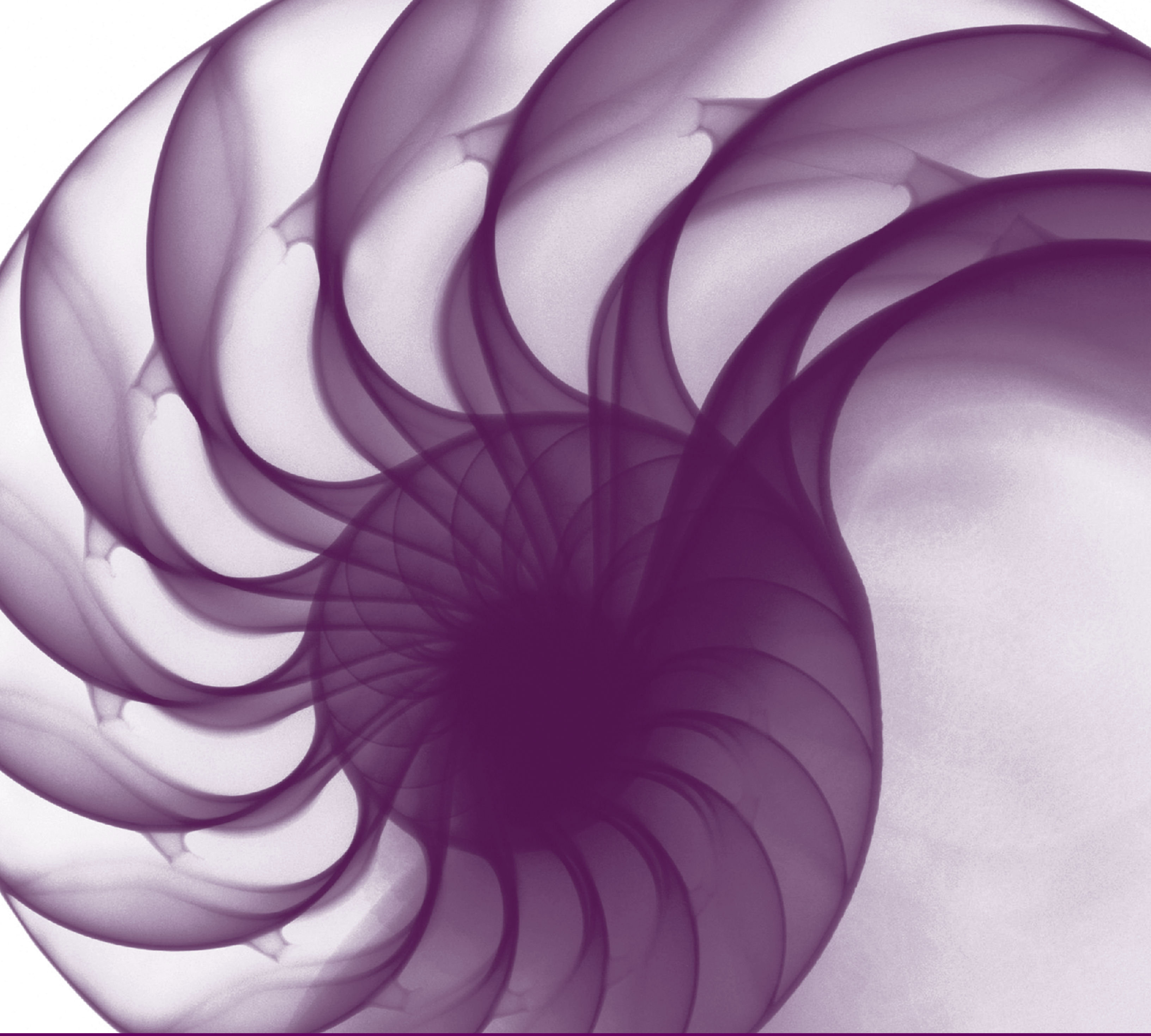
Appendix G: Service catalogue example

Appendix G: Service catalogue example

The service catalogue (Table G.1) is a key document containing valuable information on the complete set of services offered. It should preferably be stored as a set of 'service' configuration items within a configuration management system, maintained under change management. As it is such a valuable set of information, it should be available to anyone within the organization. Every new service should immediately be entered into the service catalogue once its initial definition of requirements has been documented and agreed. So as well as the information below, the service catalogue should record the status of every service, through the stages of its defined lifecycle.

Table G.1 Service catalogue example

Service name	Service description	Service type	Supporting services	Business owner(s)	Business unit(s)	Service owner(s)	Business impact	Business priority	Service level agreement	Service hours	Business contacts	Escalation contacts	Service reports	Service reviews	Security rating
Service 1															
Service 2															
Service 3															
Service 4															



Appendix H: The service management process maturity framework

H

Appendix H: The service management process maturity framework

The process maturity framework (PMF) can be used either as a framework to assess the maturity of each of the service management processes individually, or to measure the maturity of the service management process as a whole. This is an approach that has been widely used in the IT industry for a number of years, with many proprietary models being used by a number of organizations. This particular PMF has been developed to bring a common, best-practice approach to the review and assessment of service management process maturity. This framework, which is shown in Figure 8.3, can be used by organizations to internally review their own service management processes as well as by third-party organizations brought in as external reviewers, assessors or auditors.

The use of the PMF in the assessment of service management processes relies on an appreciation of the IT organization growth model. The maturity of the service management processes is heavily dependent on the stage of growth of the IT organization as a whole. It is difficult, if not impossible, to develop the maturity of the service management processes beyond the maturity and capability of the overall IT organization. The maturity of the IT organization is not just dependent on the maturity of the service management processes. Each level requires a change of a combination of elements in order to be fully effective. Therefore a review of processes will require an assessment to be completed against the five areas of:

- Vision and steering
- Process
- People
- Technology
- Culture.

These are the five areas described within the PMF for assessing process maturity. The major characteristics of each level of the PMF are as follows.

H.1 INITIAL (LEVEL 1)

The process has been recognized but there is little or no process management activity and it is allocated no importance, resources or focus within the organization. This level can also be described as 'ad hoc' or occasionally even 'chaotic'. See Table H.1.

Table H.1 PMF level 1: initial

Vision and steering	Minimal funds and resources with little activity
	Results temporary, not retained
	Sporadic reports and reviews
Process	Loosely defined processes and procedures, used reactively when problems occur
	Totally reactive processes
	Irregular, unplanned activities
People	Loosely defined roles or responsibilities
Technology	Manual processes or a few specific, discrete tools (pockets/islands)
Culture	Tool and technology-based and driven with a strong activity focus

H.2 REPEATABLE (LEVEL 2)

The process has been recognized and is allocated little importance, resource or focus within the operation. Generally activities related to the process are uncoordinated, irregular, without direction and are directed towards process effectiveness. See Table H.2.

Table H.2 PMF Level 2: repeatable

Vision and steering	No clear objectives or formal targets
	Funds and resources available
	Irregular, unplanned activities, reporting and reviews
Process	Defined processes and procedures
	Largely reactive process
	Irregular, unplanned activities
People	Self-contained roles and responsibilities
Technology	Many discrete tools, but a lack of control
	Data stored in separate locations
Culture	Product- and service-based and driven

H.3 DEFINED (LEVEL 3)

The process has been recognized and is documented but there is no formal agreement, acceptance or recognition of its role within the IT operation as a whole. However, the process has a process owner, formal objectives and targets with allocated resources, and is focused on the efficiency as well as the effectiveness of the process. Reports and results are stored for future reference. See Table H.3.

Table H.3 PMF Level 3: defined

Vision and steering	Documented and agreed formal objectives and targets
	Formally published, monitored and reviewed plans
	Well-funded and appropriately resourced
	Regular, planned reporting and reviews
Process	Clearly defined and well-publicized processes and procedures
	Regular, planned activities
	Good documentation
	Occasionally proactive process
People	Clearly defined and agreed roles and responsibilities
	Formal objectives and targets
	Formalized process training plans
Technology	Continuous data collection with alarm and threshold monitoring
	Consolidated data retained and used for formal planning, forecasting and trending
Culture	Service- and customer-oriented with a formalized approach

H.4 MANAGED (LEVEL 4)

The process has now been fully recognized and accepted throughout IT. It is service-focused and has objectives and targets that are based on business objectives and goals. The process is fully defined, managed and has become proactive, with documented, established interfaces and dependencies with other IT process. See Table H.4.

Table H.4 PMF level 4: managed

Vision and steering	Clear direction with business goals, objectives and formal targets, measured progress
	Effective management reports actively used
	Integrated process plans linked to business and IT plans
	Regular improvements, planned and reviewed
Process	Well-defined processes, procedures and standards, included in all IT staff job descriptions
	Clearly defined process interfaces and dependencies
	Integrated service management and systems development processes
	Mainly proactive process
People	Inter- and intra-process team working
	Responsibilities clearly defined in all IT job descriptions
Technology	Continuous monitoring measurement, reporting and threshold alerting to a centralized set of integrated toolsets, databases and processes
Culture	Business-focused with an understanding of the wider issues

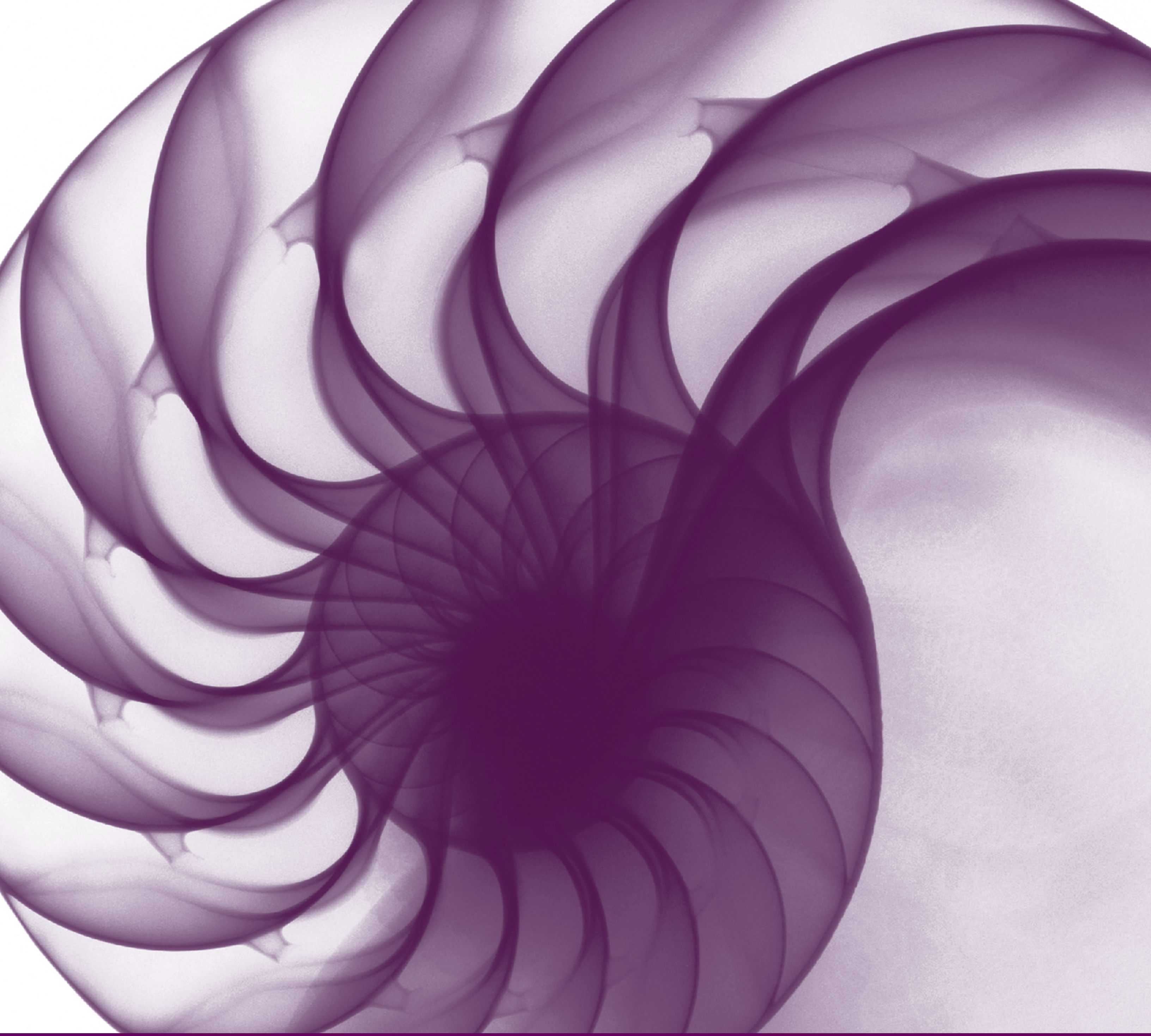
H.5 OPTIMIZING (LEVEL 5)

The process has now been fully recognized and has strategic objectives and goals aligned with overall strategic business and IT goals. These have now become 'institutionalized' as part of the everyday activity for everyone involved with the process. A self-contained continual process of improvement is established as part of the process, which is now developing a pre-emptive capability. See Table H.5.

Table H.5 PMF level 5: optimizing

Vision and steering	Integrated strategic plans inextricably linked with overall business plans, goals and objectives
	Continuous monitoring, measurement, reporting alerting and reviews linked to a continual process of improvement
	Regular reviews and/or audits for effectiveness, efficiency and compliance
Process	Well-defined processes and procedures part of corporate culture
	Proactive and pre-emptive process
People	Business aligned objectives and formal targets actively monitored as part of the everyday activity
	Roles and responsibilities part of an overall corporate culture
Technology	Well-documented overall tool architecture with complete integration in all areas of people, processes and technology
Culture	A continual improvement attitude, together with a strategic business focus. An understanding of the value of IT to the business and its role within the business value chain

This maturity framework is aligned with the Software Engineering Institute Capability Maturity Model® Integration (SEI CMMI) and its various maturity models including the evolving CMMI-SVC, which focuses on the delivery of services.

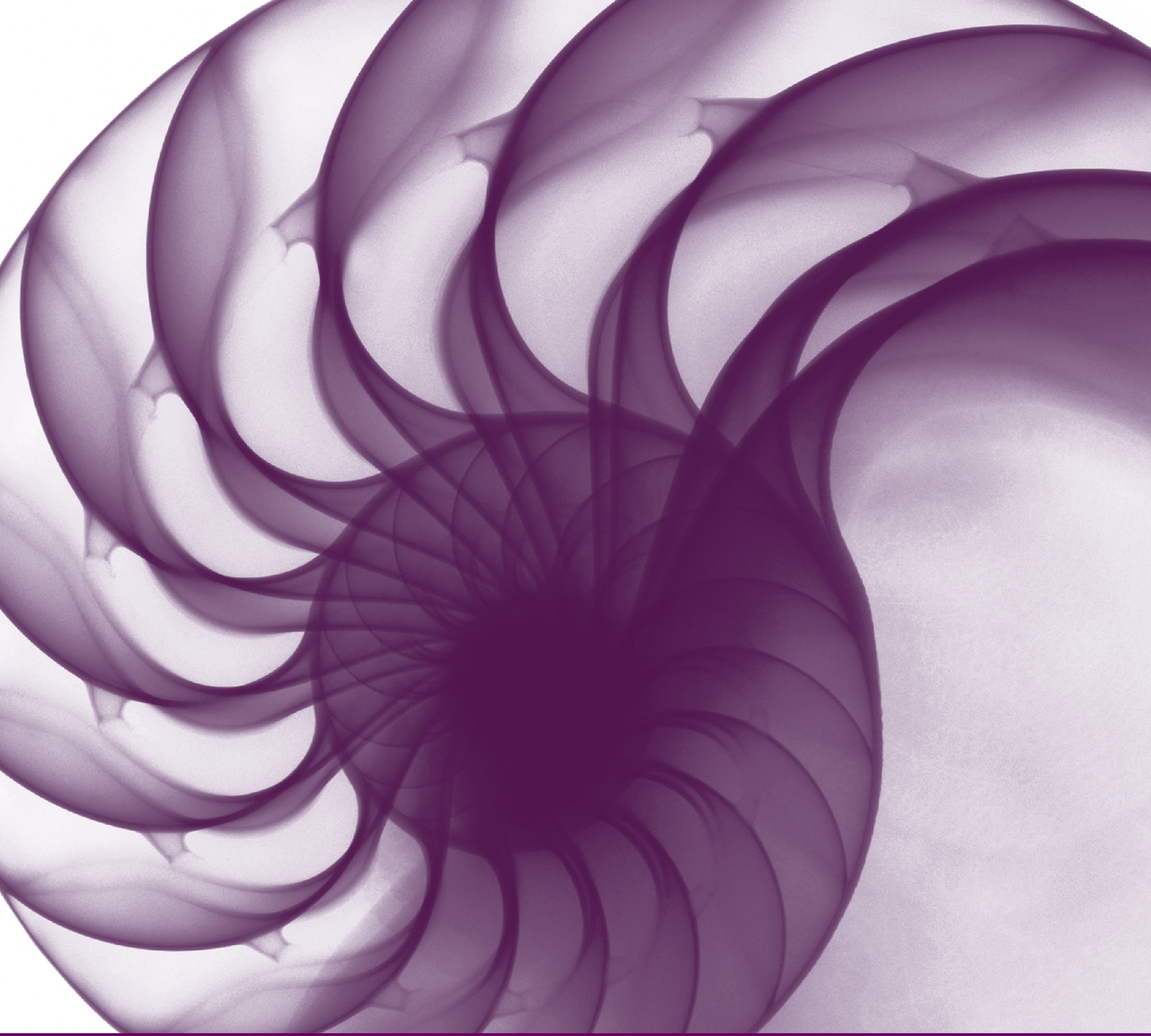


Appendix I: Example of the contents of a statement of requirements and/or invitation to tender

Appendix I: Example of the contents of a statement of requirements and/or invitation to tender

The following is an example of a minimum set of contents that should be included in an invitation to tender (ITT) or statement of requirements (SoR):

- A description of the services, products and/or components required
- All relevant technical specifications, details and requirements
- A service level requirement (SLR) where applicable
- Availability, reliability, maintainability and serviceability requirements
- Details of ownership of hardware, software, buildings, facilities etc.
- Details of performance criteria to be met by the equipment and the supplier(s)
- Details of all standards to be complied with (internal, external, national and international)
- Legal and regulatory requirements (industry, national, EU and international)
- Details of quality criteria
- Contractual timescales, details and requirements, terms and conditions
- All commercial considerations: costs, charges, bonus and penalty payments, and schedules
- Interfaces and contacts required
- Project management methods to be used
- Reporting, monitoring and reviewing procedures and criteria to be used during and after the implementation
- Supplier requirements and conditions
- Sub-contractor requirements
- Details of any relevant terms and conditions
- Description of the supplier response requirements:
    - Format
    - Criteria
    - Conditions
    - Timescales
    - Variances and omissions
    - Customer responsibilities and requirements
- Details of planned and possible growth
- Procedures for handling changes



Appendix J: Typical contents of a capacity plan

J

Appendix J: Typical contents of a capacity plan

The typical contents of a capacity plan are as follows.

J.1 INTRODUCTION

This section briefly explains the background to this issue of the capacity plan, how it was produced and what it contains. For example:

- The current services, technology and resources
- The organization's current levels of capacity
- Problems being experienced or envisaged due to over- or under-capacity
- The degree to which service levels are being achieved
- What has changed since the last issue of the plan.

J.2 MANAGEMENT SUMMARY

Much of the capacity plan, by necessity, contains technical detail that is not of interest to all readers of the plan. The management summary should highlight the main issues, options, recommendations and costs. It may be necessary to produce a separate executive summary document that contains the main points from each of the sections of the main plan.

J.3 BUSINESS SCENARIOS

It is necessary to put the plan into the context of the current and envisaged business environment. For example, a British airline planned to move a large number of staff into its headquarters building. A ratio of 1.7 people per desktop terminal was forecast. Capacity management was alerted and was able to calculate the extra network traffic that would result.

It is important to mention explicitly all known business forecasts so that readers can determine what is within and what is outside the scope of the plan. It should include the anticipated growth in existing services, the potential new services and existing services scheduled for closure.

J.4 SCOPE AND TERMS OF REFERENCE OF THE PLAN

Ideally, the capacity plan should encompass all IT resources. This section should explicitly name those elements of the IT infrastructure that are included and those that are excluded, if any.

J.5 METHODS USED

The capacity plan uses information gathered by the sub-processes. This sub-section, therefore, should contain details of how and when this information was obtained – for example, business forecasts obtained from business plans, workload forecasts obtained from customers, service level forecasts obtained by the use of modelling tools.

J.6 ASSUMPTIONS MADE

It is important that any assumptions made, particularly those concerning the business drivers for IT capacity, are highlighted early on in the plan. If they are the cornerstones on which more detailed calculations are built, then it is vital that all concerned understand this.

J.7 SERVICE SUMMARY

The service summary section should include:

- **Current and recent service provision** For each service that is delivered, provide a service profile. This should include throughput rates and the resulting resource utilization, for example, of memory, storage space, transfer rates, processor usage and network usage. Short-, medium- and long-term trends should be presented here.
- **Service forecasts** The business plans should provide capacity management with details of the new services planned and the growth or contraction in the use of existing services. This sub-section should report on new services and the demise of legacy systems.

J.8 RESOURCE SUMMARY

The resource summary section should include:

- **Current and recent resource usage** This sub-section concentrates on the resulting resource usage by the services. It reports, again, on the short-, medium- and long-term trends in component usage, broken down by hardware platform. Information on component and other resource usage has been gathered and analysed by the sub-processes of service capacity management and component capacity management and so should be readily available.
- **Resource forecasts** This sub-section forecasts the likely resource usage resulting from the service forecasts. Each business scenario mentioned above should be addressed here. For example, a carpet wholesale business in the north of England could accurately predict what the peak and average processor usage would be before it decided to take over a rival business. It was proved that an upgrade would not be required. This was fed into the cost model, leading to a successful takeover.

J.9 OPTIONS FOR SERVICE IMPROVEMENT

Building on the results of the previous section, this section outlines the possible options for improving the effectiveness and efficiency of service delivery. It could contain options for merging different services on a single processor, upgrading the network to take advantage of technological advances, tuning the use of resource or service performance, rewriting legacy systems, purchasing new hardware or software etc.

J.10 COSTS FORECAST

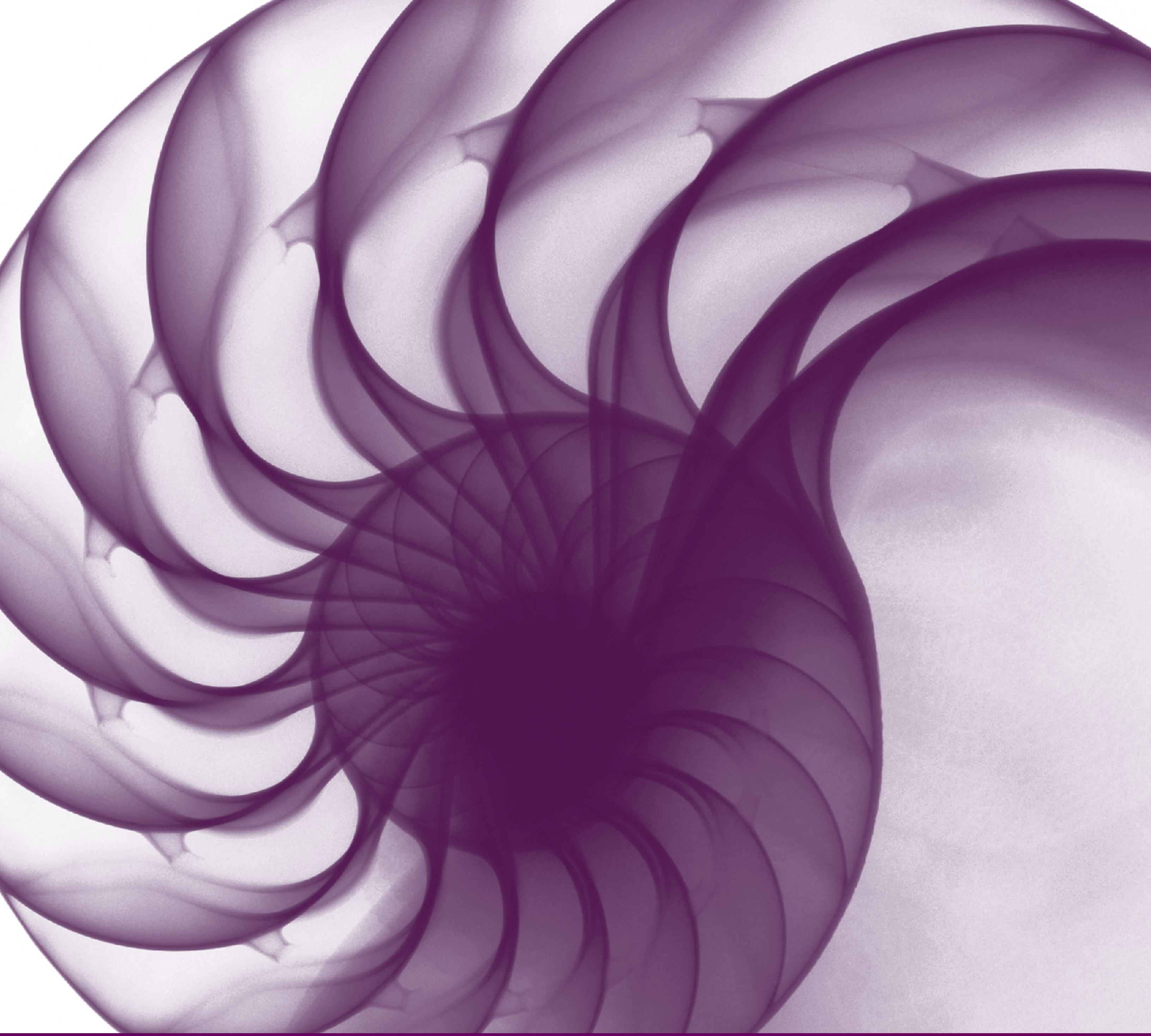
The costs associated with these options should be documented here. In addition, the current and forecasted cost of providing IT services should be included. In practice, capacity management obtains much of this information from the financial management for IT services process and the IT financial plan.

J.11 RECOMMENDATIONS

The final section of the plan should contain a summary of the recommendations made in the previous plan and their status – for example, rejected, planned, implemented – and any variances from the plan. Any new recommendations should be made here, i.e. which of the options mentioned in the plan is preferred, and the implications if the plan and its recommendations are not implemented should also be included.

The recommendations should be quantified in terms of the:

- Business benefits to be expected
- Potential impact of carrying out the recommendations
- Risks involved
- Resources required
- Costs, both setup and ongoing.



Appendix K: Typical contents of a recovery plan

K

Appendix K: Typical contents of a recovery plan

The typical contents of an IT service continuity management recovery plan are as follows.

K.1 GENERIC RECOVERY PLAN

K.1.1 Document control

This document must be maintained to ensure that the systems, infrastructure and facilities included, appropriately support business recovery requirements.

K.1.1.1 Document distribution

Copy	Issued to	Date	Position
1.			
2.			
3.			
4.			

K.1.1.2 Document revision

This document will be reviewed every X months.

Current revision .... Date ....

Next revision .... Date ....

Revision date	Version no	Summary of changes

K.1.1.3 Document approval

This document must be approved by the following personnel:

Name	Title	Signature

K.1.1.4 Scope

The following describes what is in scope of this document and what is out of scope:

In scope of document:
Out of scope of document:

K.2 SUPPORTING INFORMATION

K.2.1 Introduction

This document details the instructions and procedures that are required to be followed to recover or continue the operation of systems, infrastructure, services or facilities to maintain service continuity to the level defined or agreed with the business.

K.2.2 Recovery strategy

The systems, infrastructure, services or facilities will be recovered to alternative systems, infrastructure, services or facilities.

It will take approximately X hours to recover the systems, infrastructure, services or facilities. The system will be recovered to the last known point of stability/data integrity, which is [point in day/timing].

The required recovery time for this system, infrastructure, service or facility is: ....

The recovery time and procedures for this system, infrastructure, service or facility was last tested on:

....

K.2.3 Invocation

The following personnel are authorized to invoke this plan:

1 ....

2 ....

K.2.4 Interfaces and dependencies on other plans

Details of the inter-relationships and references with all other continuity and recovery plans and how the interfaces are activated. Includes recovery prioritization between systems.

K.2.5 General guidance

All requests for information from the media or other sources should be referred to the company procedure.

When notifying personnel of a potential or actual disaster, follow the defined operational escalation procedures, and in particular:

- Be calm and avoid lengthy conversation
- Advise them of the need to refer information requests to escalation point
- Advise them of expectations and actions (avoid giving them details of the incident unless absolutely necessary)
- If the call is answered by somebody else:
  - Ask if the contact is available elsewhere
  - If they cannot be contacted, leave a message to contact you on a given number
  - Do not provide details of the incident
  - Always document call time details, responses and actions.

All activities and contact/escalation should be clearly and accurately recorded. To facilitate this, actions should be in a checklist format and there should be space to record the date and time the activity was started and completed, and who carried out the activity.

K.2.6 Dependencies

System, infrastructure, service, facility or interface dependencies should be documented (in priority order) so that related recovery plans or procedures that will need to be invoked in conjunction with this recovery plan can be identified and actioned. The person responsible for invocation should ensure recovery activities are coordinated with these other plans. Documented dependencies should include services/infrastructure dependent upon this system, and services/infrastructure that this system depends upon.

System	Document reference	Contact

K.2.7 Contact lists

Lists of all contact names, organizations and contact details and mechanisms:

Name	Organization/role	Title	Contact details

K.2.8 Recovery team

The following staff/functions are responsible for actioning these procedures or ensuring the procedures are actioned, and for recording any issues or problems encountered. Contact will be made via the normal escalation procedures.

Name	Title	Contact details

K.2.9 Recovery team checklist

To facilitate the execution of key activities in a timely manner, a checklist similar to the following should be used.

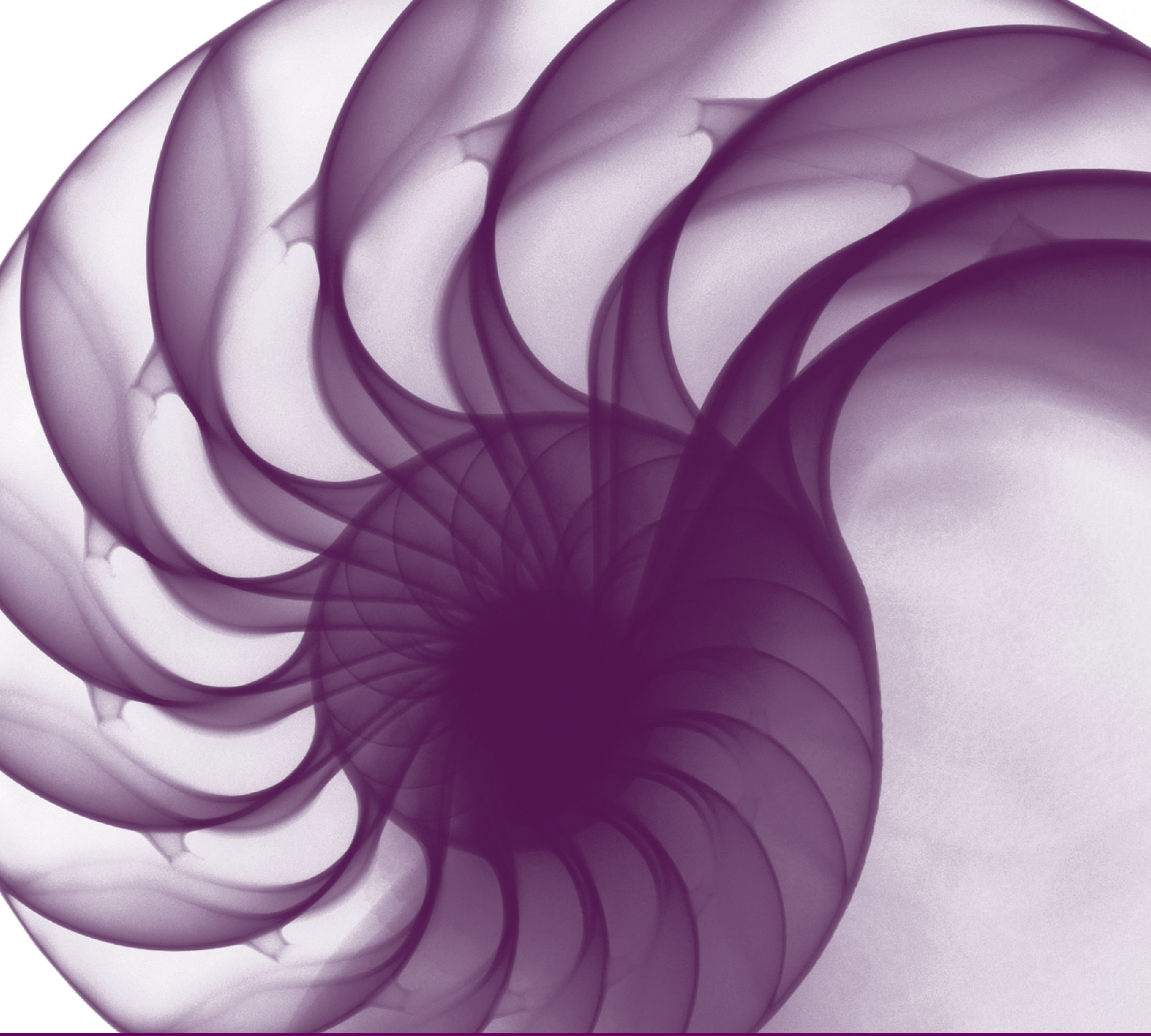
Task	Target completion	Actual completion
Confirm invocation		
Initiate call tree and escalation procedures		
Instigate and interface with any other recovery plans necessary (e.g. business continuity plan, crisis management, emergency response plan)		
Arrange for backup media and documentation to be shipped to recovery site(s)		
Establish recovery teams		
Initiate recovery actions		
Confirm progress reporting		
Inform recovery team of reporting requirements		
Confirm liaison requirements with all recovery teams		
Advise customers and management of estimated recovery completion		

K.3 RECOVERY PROCEDURE

Enter recovery instructions/procedures or references to all recovery procedures here.

Content/format should be in line with company standards for procedures. If there are none, guidance should be issued by the manager or team leader for the area responsible for the system, infrastructure, services or facility. The only guideline is that the instructions should be capable of being executed by an experienced professional without undue reliance on local knowledge.

Where necessary, references should be made to supporting documentation (and its location), diagrams and other information sources. This should include the document reference number (if it exists). It is the responsibility of the plan author to ensure that this information is maintained with this plan. If there is only a limited amount of supporting information, it may be easier for this to be included within the plan, providing this plan remains easy to read/follow and does not become too cumbersome.



Appendix L: Procurement documents

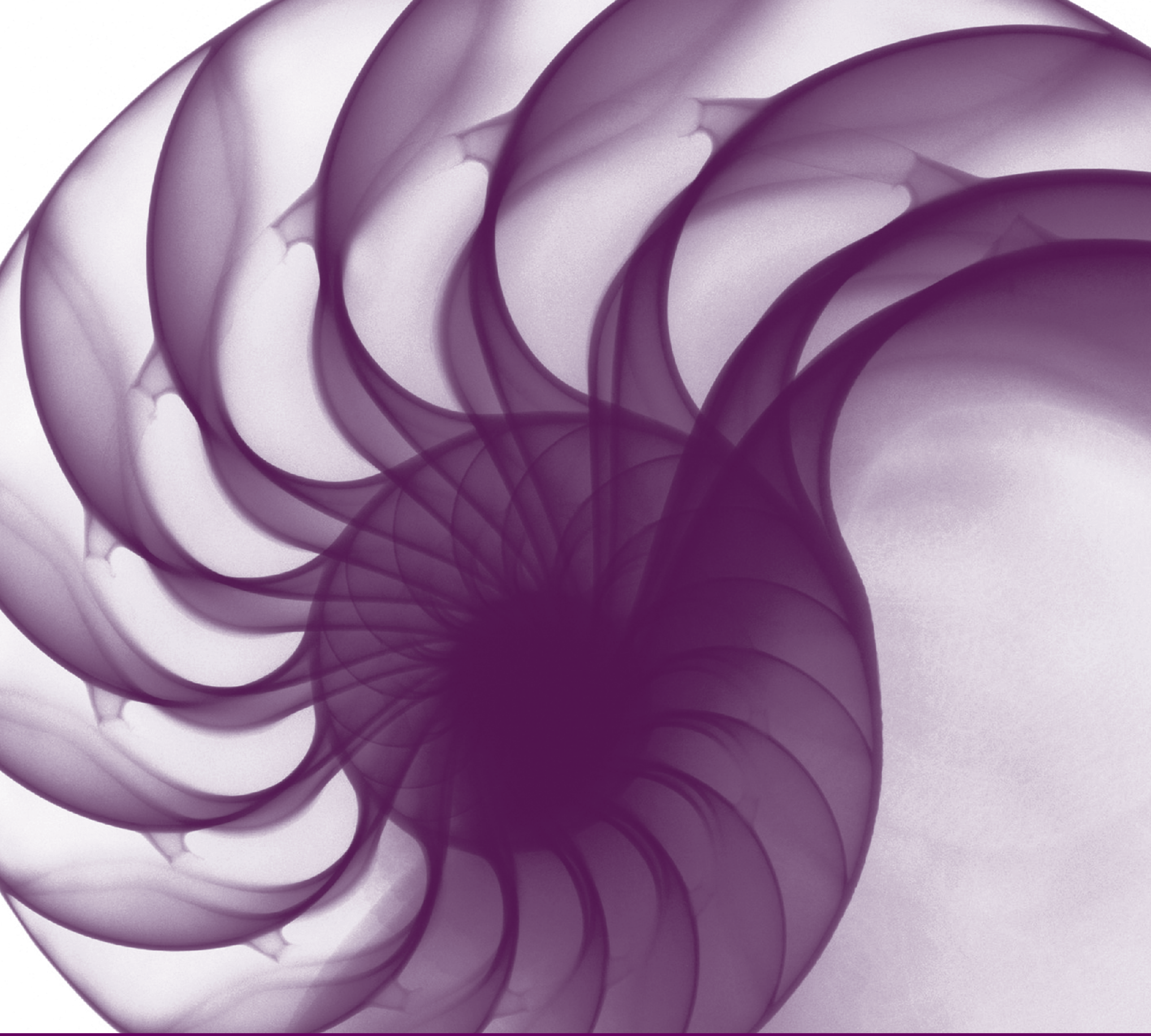
L

Appendix L: Procurement documents

Table L.1 lists the documents that are frequently utilized in the process of procuring services from an external supplier.

Table L.1 Procurement documents

Abbreviation	Document	Description
SoR	Statement of requirements	A document detailing all of the requirements for a product purchase, or a new or changed IT service
ToR	Terms of reference	A document specifying the requirements, scope, deliverables, resources and schedule for a project or activity
RFI	Request for information	A document sent to a broad base of potential suppliers soliciting responses for the purpose of gathering information supporting broad understanding. An RFI is frequently a preliminary for preparing for an RFP or RFQ, and can assist the requesting organization in developing a strategy and/or narrowing the field of potential suppliers
RFP	Request for proposal	A document inviting potential suppliers to submit a proposal on a specific commodity or service. An RFP describes the need of the requesting organization and specifies when and how responses are to be submitted and considered. Comparison of RFP responses can allow the requesting organization to evaluate different potential approaches to addressing their business need and further narrow the field of potential suppliers
RFQ	Request for quotation	A document sent to potential suppliers containing in exacting detail a list or description of all relevant parameters of an intended purchase and soliciting a competitive price. In contrast to an RFP, an RFQ provides information on the exact requirements of the requesting organization, allowing comparison of pricing across multiple suppliers
ITT	Invitation to tender	A document inviting short-listed suppliers to 'tender their services' through a formal, written document that is evaluated against specific criteria



Appendix M: Risk assessment and management

M

Appendix M: Risk assessment and management

This appendix contains basic information about several broadly known and used approaches to the assessment and management of risk. It is not intended to be a comprehensive study of the subject, but rather to provide an awareness of some of the methods in use.

M.1 DEFINITION OF RISK AND RISK MANAGEMENT

Risk may be defined as uncertainty of outcome, whether a positive opportunity or negative threat. It is the fact that there is uncertainty that creates the need for attention and formal management of risk. After all, if an organization were absolutely certain that a negative threat would materialize, there would be little difficulty in determining an appropriate course of action. Likewise, if an organization could be guaranteed that the positive opportunity would be realized, then its path would be clear. Managing risks requires the identification and control of the exposure to those risks which may have an impact on the achievement of an organization's business objectives.

Every organization manages its risk, but not always in a way that is visible, repeatable and consistently applied to support decision-making. The purpose of formal risk management is to enable better decision-making based on a sound understanding of risks and their likely impact on the achievement of objectives. An organization can gain this understanding by ensuring that it makes cost-effective use of a risk framework that has a series of well-defined steps. Decision-making should include determining any appropriate actions to take to manage the risks to a level deemed to be acceptable by the organization.

A number of different methodologies, standards and frameworks have been developed for risk management. Some focus more on generic techniques widely applicable to different levels and needs, while others are specifically concerned with risk management relating to important assets used by the organization in the pursuit of its objectives. Each organization should determine the approach to risk management that is best suited to its needs and circumstances, and it is possible that the approach adopted will leverage the ideas reflected in more than one of the recognized standards and/or frameworks.

In this appendix the following approaches to managing risks are briefly explained:

- Management of Risk (M_o_R)
- ISO 31000
- ISO/IEC 27001
- Risk IT.

M.2 MANAGEMENT OF RISK (M_o_R)

Management of Risk (M_o_R) is intended to help organizations put in place an effective framework for risk management. This will help them take informed decisions about the risks that affect their strategic, programme, project and operational objectives.

M_o_R provides a route map of risk management, bringing together principles, an approach, a process with a set of interrelated steps and pointers to more detailed sources of advice on risk management techniques and specialisms. It also provides advice on how these principles, approach and process should be embedded, reviewed and applied differently depending on the nature of the objectives at risk.

The M_o_R framework is illustrated in Figure M.1.

The M_o_R framework is based on four core concepts:

- **M_o_R principles** Principles are essential for the development and maintenance of good risk management practice. They are informed by corporate governance principles and the international standard for risk management, ISO 31000: 2009. They are high-level and universally applicable statements that provide guidance to organizations as they design an appropriate approach to risk management as part of their internal controls.

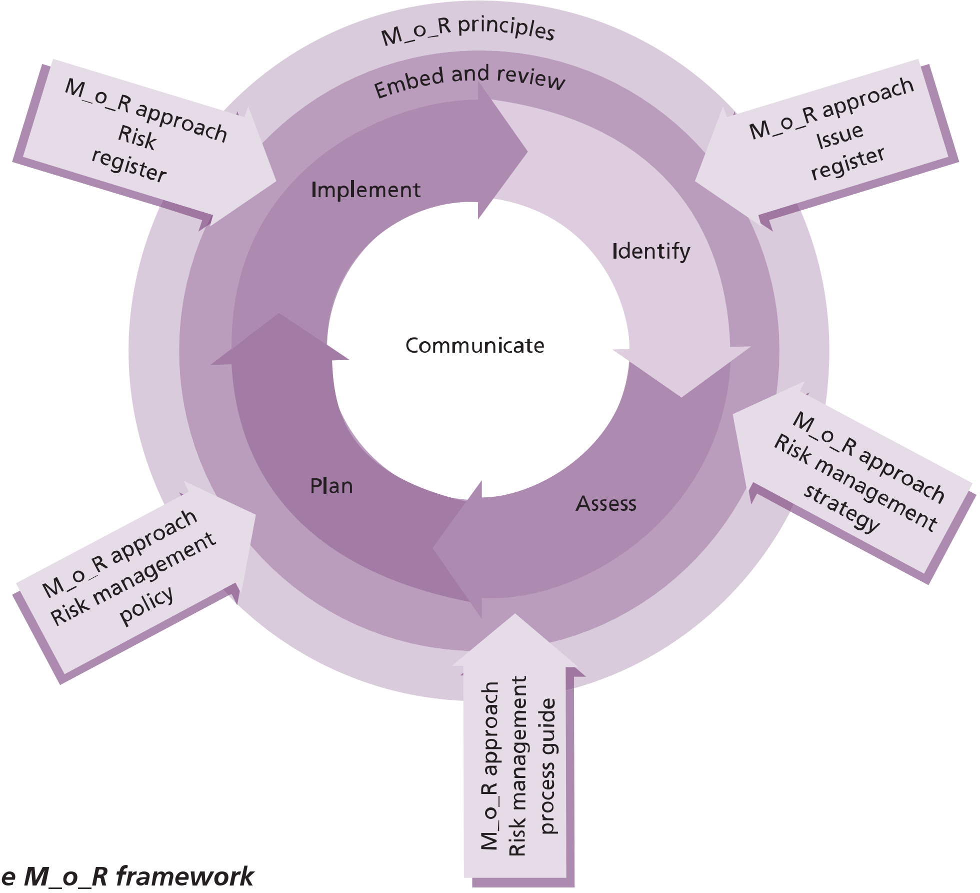

M_o_R principles
Embed and review
Implement
Identify
Communicate
Plan
Assess
M_o_R approach Risk register
M_o_R approach Issue register
M_o_R approach Risk management strategy
M_o_R approach Risk management policy
M_o_R approach Risk management process guide

Figure M.1 The M_o_R framework

- **M_o_R approach** Principles need to be adapted and adopted to suit each individual organization. An organization's approach to the principles needs to be agreed and defined within a risk management policy, process guide and strategies.
- **M_o_R process** The process is divided into four main steps: identify, assess, plan and implement. Each step describes the inputs, outputs, tasks and techniques involved to ensure that the overall process is effective.
- **Embedding and reviewing M_o_R** Having put in place an approach and process that satisfy the principles, an organization should ensure that they are consistently applied across the organization and that their application undergoes continual improvement in order for them to be effective.

There are several common techniques which support risk management, including a summary risk profile. A summary risk profile is a graphical representation of information normally found in an existing risk register, and helps to increase the visibility of risks. For more information on summary risk profiles and other M_o_R techniques, see *Management of Risk: Guidance for Practitioners* (OGC, 2010).

M.3 ISO 31000

ISO 31000 was published in November 2009 and is the first set of international guidelines for risk management, intended to be applicable and adaptable for 'any public, private or community enterprise, association, group or individual.' ISO 31000 is a process-oriented rather than a control-oriented approach to risk management, and provides guidance on a broader, more conceptual basis, rather than specifying all aspects of an organization's risk assessment and management approach. For example, ISO 31000 does not define how an organization will create risk data or measure risk, nor does it ensure that an organization will include a review of all risk areas relevant to the achievement of their objectives. ISO 31000 was published as a standard without certification.

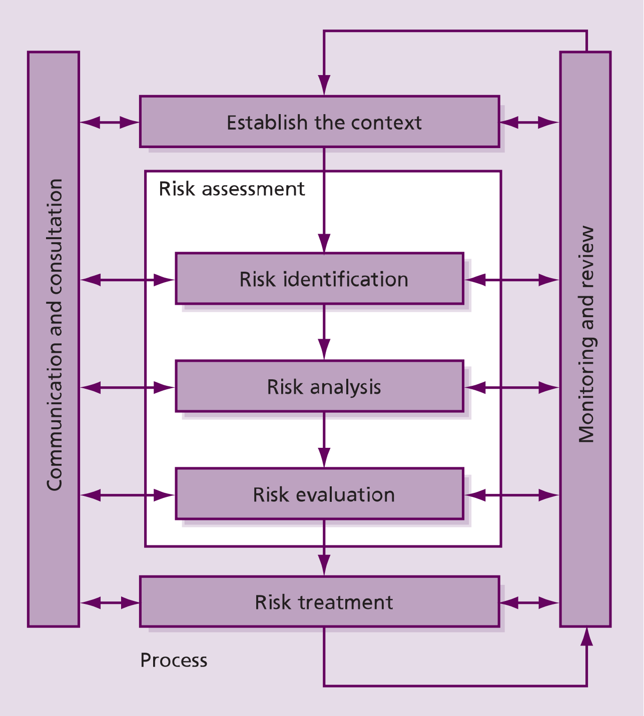


Figure M.2 ISO 31000 risk management process flow

ISO 31000 defines risk as 'the effect of uncertainty on objectives'. Risk management should be performed within a framework that provides the foundations and provisions which will embed the management of risk throughout all levels of the organization. ISO 31000 identifies the necessary components of such a framework as:

- Mandate and commitment
- Design of framework for managing risk
- Understanding the organization and its context
- Establishing risk management policy
- Accountability
- Integration into organizational processes
- Resources
- Establishing internal communication and reporting mechanisms
- Establishing external communication and reporting mechanisms
- Implementing risk management
- Monitoring and review of the framework
- Continual improvement of the framework.

Within this context the risk management process is seen at a high level in Figure M.2.

Once the framework has been established and the context understood, risk assessment is undertaken. This consists of three steps: risk identification, risk analysis and risk evaluation. The risk identification step is intended to create a comprehensive list of risks based on those events that might create, enhance, prevent, degrade, accelerate or delay the achievement of the organization's objectives. Risk analysis involves developing a full understanding of the risks as an input to risk evaluation and the decisions regarding the plan for treating the risks. Risk evaluation is to make decisions about which risks require treatment and the relative priorities amongst them.

Risk treatment involves the modification of risks using one or more approaches. These approaches are not necessarily mutually exclusive and may include:

- Avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk
- Taking or increasing the risk in order to pursue an opportunity
- Removing the risk source
- Changing the likelihood
- Changing the consequences
- Sharing the risk with another party or parties (including contracts and risk financing)
- Retaining the risk by informed decision.

The approach described in ISO 31000 provides broad scope for each organization to adopt the high-level principles and adapt them to their specific needs and circumstances.

M.4 ISO/IEC 27001

ISO/IEC 27001 was published in October 2005 and is an information security management system (ISMS) standard which formally specifies a management system that is intended to bring information security under explicit management control. While ISO/IEC 27001 is a security standard, not a risk management standard, it mandates specific requirements for security, including requirements relating to risk management. The risk management methods described in this context may be applied to general risk management activities as well.

ISO/IEC 27001 requires that management:

- Systematically examines the organization's information security risks, taking account of the threats, vulnerabilities and impacts

- Designs and implements a coherent and comprehensive suite of information security controls and/or other forms of risk treatment (such as risk avoidance or risk transfer) to address those risks that are deemed unacceptable
- Adopts an overarching management process to ensure that the information security controls continue to meet the organization's information security needs on an ongoing basis.

The key risk management-related steps described in ISO/IEC 27001 include:

- Define the risk assessment approach of the organization
- Identify a risk assessment methodology that is suited to the ISMS, and the identified business information security, legal and regulatory requirements
- Develop criteria for accepting risks and identify acceptable levels of risk
- Identify the risks
- Identify the assets within the scope of the ISMS, and the owners of these assets
- Identify the threats to these assets
- Identify the vulnerabilities that might be exploited by the threats
- Identify the impact that losses of confidentiality, integrity and availability may have on these assets
- Analyse and evaluate the risks
- Assess the business impacts on the organization that might result from security failures, taking into account the consequences of a loss of confidentiality, integrity or availability of the assets
- Assess the realistic likelihood of security failures occurring in the light of prevailing threats and vulnerabilities, and impacts associated with these assets, and the controls currently implemented
- Estimate the levels of risk
- Determine whether the risks are acceptable or require treatment using the previously established criteria for accepting risks
- Identify and evaluate options for the treatment of risks. Possible actions may include:
    - Applying appropriate controls
    - Knowingly and objectively accepting risks, providing they clearly satisfy the organization's policies and the criteria for accepting risks
    - Avoiding risks
    - Transferring the associated business risks to other parties, e.g. insurers, suppliers
- Select control objectives and controls for the treatment of risks
- Obtain management approval of the proposed residual risks
- Obtain management authorization to implement and operate the ISMS.

During the implementation and operation of the ISMS, a plan for risk treatment is formulated (identifying the appropriate management action, resources, responsibilities and priorities for managing information security risks) and implemented. ISO/IEC 27001 also calls for the ongoing monitoring and reviewing of the risks and risk treatment and the formal maintenance of the ISMS to ensure that the organization's goals are met.

This approach is focused specifically on the assets involved in organizational information security, but the general principles can be applied to overall service provision.

M.5 RISK IT

Risk IT is part of the IT governance product portfolio of ISACA that provides a framework for effective governance and management of IT risk, based on a set of guiding principles. Risk IT is about IT risk, including business risk related to the use of IT. The publications in which Risk IT is documented include *The Risk IT Framework* (ISACA, 2009) and *The Risk IT Practitioner Guide* (ISACA, 2009) (available from www.isaca.org).

The key principles in Risk IT are that effective enterprise governance and management of IT risk:

- Always connect to the business objectives
- Align the management of IT-related business risk with overall enterprise risk management
- Balance the costs and benefits of managing IT risk
- Promote fair and open communication of IT risk

- Establish the right tone from the top while defining and enforcing personal accountability for operating within acceptable and well-defined tolerance levels
- Are continuous processes and part of daily activities.

The framework provides for three domains, each containing three processes, as shown in Figure M.3. *The Risk IT Framework* describes the key activities of each process, the responsibilities for the process, information flows between the processes and the performance management of each process.

Risk governance ensures that IT risk management practices are embedded in the enterprise, enabling it to secure optimal risk-adjusted return. Risk evaluation ensures that IT-related risks and opportunities are identified, analysed and presented in business terms. Risk response ensures that IT-related risk issues, opportunities and events are addressed in a cost-effective manner and in line with business priorities.

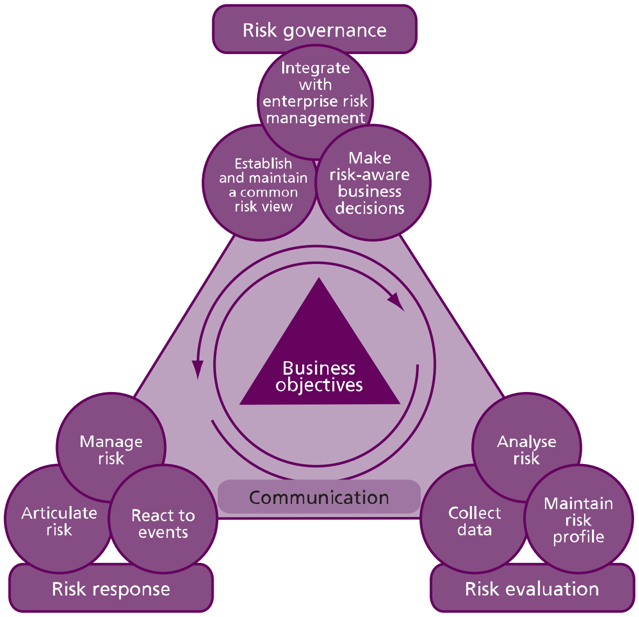
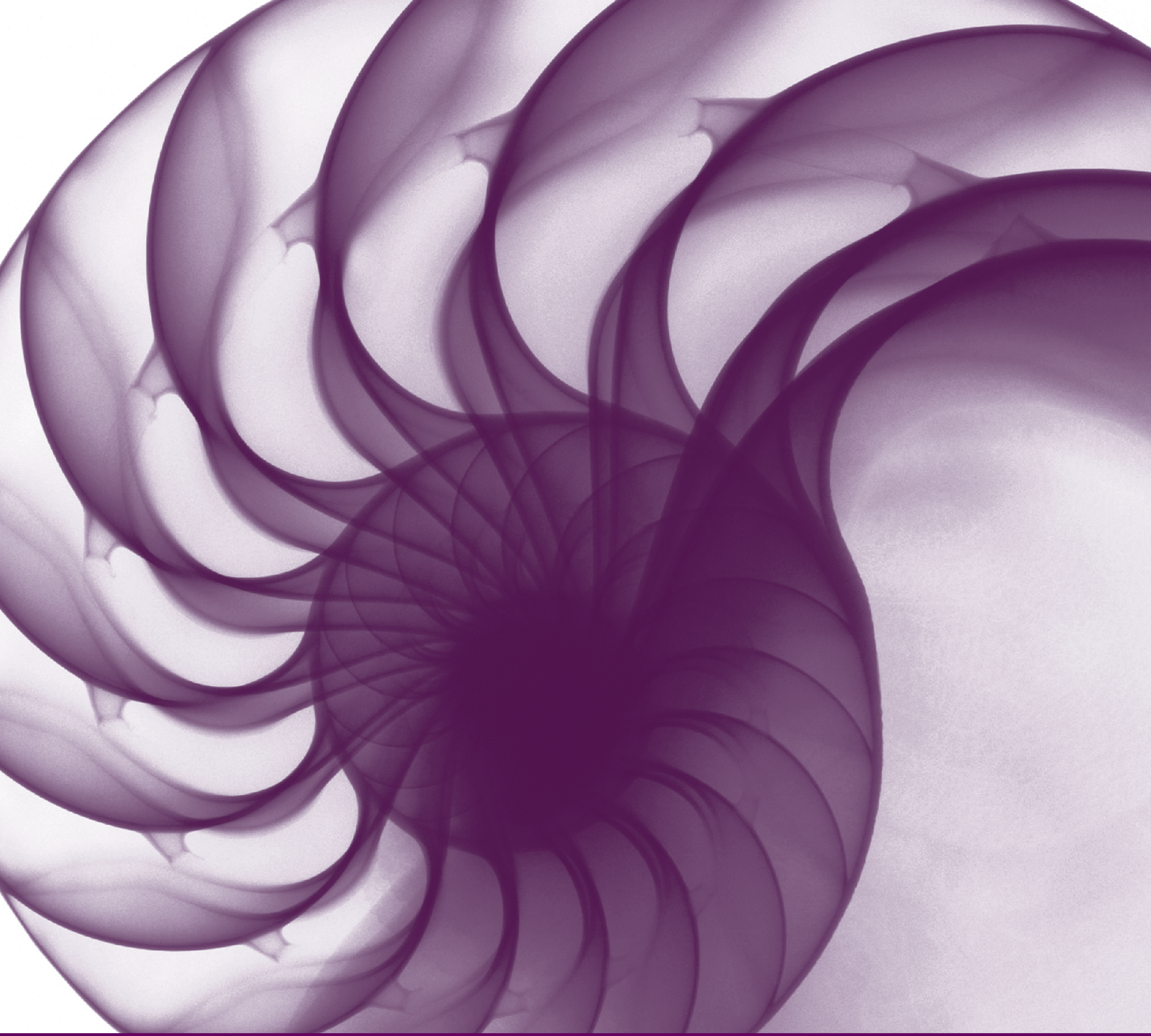


Figure M.3 ISACA Risk IT process framework



Appendix N: Related guidance

Appendix N: Related guidance

This is a common appendix across the ITIL core publications. It includes frameworks, best practices, standards, models and quality systems that complement and have synergy with the ITIL service lifecycle.

Section 2.1.7 describes the role of best practices in the public domain and references some of the publications in this appendix. Each core publication references this appendix where relevant.

Related guidance may also be referenced within a single ITIL core publication where the topic is specific to that publication.

N.1 ITIL GUIDANCE AND WEB SERVICES

ITIL is part of the Best Management Practice (BMP) portfolio of best-practice guidance (see section 1.3). BMP products present flexible, practical and effective guidance, drawn from a range of the most successful global business experiences. Distilled to its essential elements, the guidance can then be applied to every type of business and organization.

The BMP website (www.best-management-practice.com) includes news, reviews, case studies and white papers on ITIL and all other BMP best-practice guidance.

The ITIL official website (www.itil-officialsite.com) contains reliable, up-to-date information on ITIL – including information on accreditation and the ITIL software scheme for the endorsement of ITIL-based tools.

Details of the core publications are as follows:

- Cabinet Office (2011). *ITIL Service Strategy*. TSO, London.
- Cabinet Office (2011). *ITIL Service Design*. TSO, London.
- Cabinet Office (2011). *ITIL Service Transition*. TSO, London.
- Cabinet Office (2011). *ITIL Service Operation*. TSO, London.
- Cabinet Office (2011). *ITIL Continual Service Improvement*. TSO, London.

The full ITIL glossary, in English and other languages, can be accessed through the ITIL official site at:

www.itil-officialsite.com/InternationalActivities/ITILGlossaries.aspx

The range of translated glossaries is always growing, so check this website for the most up-to-date list.

Details of derived and complementary publications can be found in the publications library of the Best Management Practice website at:

www.best-management-practice.com/Publications-Library/IT-Service-Management-ITIL/

N.2 QUALITY MANAGEMENT SYSTEM

Quality management focuses on product/service quality as well as the quality assurance and control of processes to achieve consistent quality. Total Quality Management (TQM) is a methodology for managing continual improvement by using a quality management system. TQM establishes a culture involving all people in the organization in a process of continual monitoring and improvement.

ISO 9000:2005 describes the fundamentals of quality management systems that are applicable to all organizations which need to demonstrate their ability to consistently provide products that meet customer and applicable statutory and regulatory requirements. ISO 9001:2008 specifies generic requirements for a quality management system.

Many process-based quality management systems use the methodology known as 'Plan-Do-Check-Act' (PDCA), often referred to as the Deming Cycle, or Shewhart Cycle, that can be applied to all processes. PDCA can be summarized as:

- **Plan** Establish the objectives and processes necessary to deliver results in accordance with customer requirements and the organization's policies.
- **Do** Implement the processes.
- **Check** Monitor and measure processes and product against policies, objectives and requirements for the product and report the results.

- **Act** Take actions to continually improve process performance.

There are distinct advantages of tying an organization's ITSM processes, and service operation processes in particular, to its quality management system. If an organization has a formal quality management system that complies with ISO 9001, then this can be used to assess progress regularly and drive forward agreed service improvement initiatives through regular reviews and reporting.

Visit www.iso.org for information on ISO standards.

See www.deming.org for more information on the W. Edwards Deming Institute and the Deming Cycle for process improvement.

N.3 RISK MANAGEMENT

A number of different methodologies, standards and frameworks have been developed for the assessment and management of risk. Some focus more on generic techniques widely applicable to different levels and needs, while others are specifically concerned with risk management relating to important assets used by the organization in the pursuit of its objectives. Each organization should determine the approach to risk management that is best suited to its needs and circumstances. It is possible that the approach adopted will leverage the ideas reflected in more than one of the recognized standards and/or frameworks.

Appendix M gives more information on risk management. See also:

- Office of Government Commerce (2010). *Management of Risk*: *Guidance for Practitioners*. TSO, London.
- ISO 31000:2009 Risk management – principles and guidelines.
- ISO/IEC 27001: 2005 Information technology – security techniques – information security management systems – requirements.
- ISACA (2009). *The Risk IT Framework* (based on COBIT, see section N.5).

N.4 GOVERNANCE OF IT

Corporate governance refers to the rules, policies, processes (and in some cases, laws) by which businesses are operated, regulated and controlled. These are often defined by the board or shareholders, or the constitution of the organization; but they can also be defined by legislation, regulation or consumer groups.

ISO 9004 (Managing for the sustained success of an organization – a quality management approach) provides guidance on governance for the board and executive of an organization.

The standard for corporate governance of IT is ISO/IEC 38500. The purpose of this standard is to promote effective, efficient and acceptable use of IT in all organizations by:

- Assuring stakeholders (including consumers, shareholders and employees) that, if the standard is followed, they can have confidence in the organization's corporate governance of IT
- Informing and guiding directors in governing the use of IT in their organization
- Providing a basis for objective evaluation of the corporate governance of IT.

Typical examples of regulations that impact IT include: financial, safety, data protection, privacy, software asset management, environment management and carbon emission targets.

Further details are available at www.iso.org

ITIL Service Strategy references the concepts of ISO/IEC 38500 and how the concepts can be applied.

N.5 COBIT

The Control OBjectives for Information and related Technology (COBIT) is a governance and control framework for IT management created by ISACA and the IT Governance Institute (ITGI).

COBIT is based on the analysis and harmonization of existing IT standards and good practices and conforms to generally accepted governance principles. It covers five key governance focus areas: strategic alignment, value delivery, resource management, risk management and performance management. COBIT is primarily aimed at internal and external stakeholders within an enterprise who wish to generate value from IT investments;

those who provide IT services; and those who have a control/risk responsibility.

COBIT and ITIL are not 'competitive', nor are they mutually exclusive – on the contrary, they can be used in conjunction as part of an organization's overall governance and management framework. COBIT is positioned at a high level, is driven by business requirements, covers the full range of IT activities, and concentrates on *what* should be achieved rather than *how* to achieve effective governance, management and control. ITIL provides an organization with best-practice guidance on *how* to manage and improve its processes to deliver high-quality, cost-effective IT services. The following COBIT guidance supports strategy management and continual service improvement (CSI):

- COBIT maturity models can be used to benchmark and drive improvement.
- Goals and metrics can be aligned to the business goals for IT and used to create an IT management dashboard.
- The COBIT 'monitor and evaluate' (ME) process domain defines the processes needed to assess current IT performance, IT controls and regulatory compliance.

Further details are available at www.isaca.org and www.itgi.org

N.6 ISO/IEC 20000 SERVICE MANAGEMENT SERIES

ISO/IEC 20000 is an internationally recognized standard for ITSM covering service providers who manage and deliver IT-enabled services to internal or external customers. ISO/IEC 20000-1 is aligned with other ISO management systems standards such as ISO 9001 and ISO/IEC 27001.

One of the most common routes for an organization to achieve the requirements of ISO/IEC 20000 is by adopting ITIL best practices. ISO/IEC 20000-1 is based on a service management system (SMS). The SMS is defined as a management system to direct and control the service management activities of the service provider. ISO/IEC 20000 includes:

- ISO/IEC 20000-1:2005 – Information technology – Service management – Part 1: Specification
- ISO/IEC 20000-1:2011 – Information technology – Service management – Part 1: Requirements for a service management system (the most recent edition of the ISO/IEC 20000 standard)
- ISO/IEC 20000-2:2005 – Information technology – Service management – Part 2: Code of practice (being updated to include guidance on the application of service management systems and to support ISO/IEC 20000-1:2011)
- ISO/IEC 20000-3:2005 – Information technology – Service management – Part 3: Scope and applicability
- ISO/IEC TR 20000-4 – Information technology – Service management – Part 4: Process reference model
- ISO/IEC TR 20000-5:2010 – Information technology – Service management – Part 5: Exemplar implementation plan for ISO/IEC 20000-1.

A closely related publication that is under development is ISO/IEC TR 15504-8 – Process assessment model for IT service management.

Further details can be found at www.iso.org or www.isoiec20000certification.com

Organizations using ISO/IEC 20000-1: 2005 for certification audits will transfer to the new edition, ISO/IEC 20000-1: 2011.

ITIL guidance supports organizations that are implementing service management practices to achieve the requirements of ISO/IEC 20000-1: 2005 and the new edition ISO/IEC 20000-1: 2011.

Other references include:

- Dugmore, J. and Lacy, S. (2011). *Introduction to ISO/IEC 20000 Series: IT Service Management*. British Standards Institution, London.
- Dugmore, J. and Lacy, S. (2011). *BIP 0005: A Manager's Guide to Service Management* (6th edition). British Standards Institution, London.

N.7 ENVIRONMENTAL MANAGEMENT AND GREEN/SUSTAINABLE IT

The transition to a low-carbon economy is a global challenge. Many governments have set targets to reduce carbon emissions or achieve carbon neutrality. IT is an enabler for environmental and cultural change that will help governments to achieve their targets – for example, through enabling tele- and video-conferencing, and remote and home working. However, IT is also a major user of energy and natural resources. Green IT refers to environmentally sustainable computing where the use and disposal of computers and printers are carried out in sustainable ways that do not have a negative impact on the environment.

Appendix E includes further information on environmental architectures and standards. Appendix E in *ITIL Service Operation* also provides useful considerations for facilities management, including environmental aspects.

The ISO 14001 series of standards for an environment management system is designed to assure internal and external stakeholders that the organization is an environmentally responsible organization. It enables an organization of any size or type to:

- Identify and control the environmental impact of its activities, products or services
- Improve its environmental performance continually
- Implement a systematic approach to setting and achieving environmental objectives and targets, and then demonstrating that they have been achieved.

Further details are available at www.iso.org

N.8 ISO STANDARDS AND PUBLICATIONS FOR IT

ISO 9241 is a series of standards and guidance on the ergonomics of human system interaction that cover people working with computers. It covers aspects that impact the utility of a service (whether it is fit for purpose) such as:

- ISO 9241-11:1999 Guidance on usability
- ISO 9241-210:2010 Human-centred design for interactive systems
- ISO 9241-151:2008 Guidance on world wide web user interfaces.

ISO/IEC JTC1 is Joint Technical Committee 1 of ISO and the International Electrotechnical Commission (IEC). It deals with information technology standards and other publications.

SC27 is a subcommittee under ISO/IEC JTC1 that develops ISO/IEC 27000, the information security management system (ISMS) family of standards. For further details, Appendix M includes information on ISO/IEC 27001. SC7 is a subcommittee under ISO/IEC JTC1 that covers the standardization of processes, supporting tools and supporting technologies for the engineering of systems, services and software. SC7 publications include:

- ISO/IEC 20000 Information technology – service management (see section N.6)
- ISO/IEC 19770-1 Information technology – software asset management processes. ISO/IEC 19770-2:2009 establishes specifications for tagging software to optimize its identification and management
- ISO/IEC 15288 Systems and software engineering – systems life cycle processes. The processes can be used as a basis for establishing business environments – e.g. methods, procedures, techniques, tools and trained personnel
- ISO/IEC 12207 Systems and software engineering – software life cycle processes
- ISO/IEC 15504 Process assessment series. Also known as SPICE (software process improvement and capability determination), it aims to ensure consistency and repeatability of the assessment ratings with evidence to substantiate the ratings. The series includes exemplar process assessment models (PAM), related to one or more conformant or compliant process reference model (PRM). ISO/IEC 15504-8 is an exemplar process assessment model for IT service management that is under development
- ISO/IEC 25000 series – provides guidance for the use of standards named Software product Quality Requirements and Evaluation (SQuaRE)
- ISO/IEC 42010 Systems and software engineering — recommended practice for architectural description of software-intensive systems.

SC7 is working on the harmonization of standards in the service management, software and IT systems domains. Further details are available at www.iso.org

N.9 ITIL AND THE OSI FRAMEWORK

At around the time that ITIL V1 was being written, the International Standards Organization launched an initiative that resulted in the Open Systems Interconnection (OSI) framework. Since this initiative covered many of the same areas as ITIL V1, it is not surprising that there was considerable overlap.

However, it is also not surprising that they classified their processes differently, used different terminology, or used the same terminology in different ways. To confuse matters even more, it is common for different groups in an organization to use terminology from both ITIL and the OSI framework.

The OSI framework made significant contributions to the definition and execution of ITSM programmes and projects around the world. It has also caused a great deal of debate between teams that do not realize the origins of the terminology that they are using. For example, some organizations have two change management departments – one following the ITIL change management process and the other using the OSI installation, moves, additions and changes (IMAC) model. Each department is convinced that it is completely different from the other, and that it is performing a different role. Closer examination will reveal that there are several areas of commonality.

In service operation, the management of known errors may be mapped to fault management. There is also a section related to operational capacity management, which can be related to the OSI concept of performance management.

Information on the set of ISO standards for the OSI framework is available at: www.iso.org

N.10 PROGRAMME AND PROJECT MANAGEMENT

Large, complex deliveries are often broken down into manageable, interrelated projects. For those managing this overall delivery, the principles of programme management are key to delivering on time and within budget. Best management practice in this area is found in *Managing Successful Programmes* (MSP).

Guidance on effective *portfolio, programme and project management is brought together in Portfolio, Programme and Project Offices (P3O), which* is aimed at helping organizations to establish and maintain appropriate business support structures with proven roles and responsibilities.

Structured project management methods, such as PRINCE2 (PRojects IN Controlled Environments) or the Project Management Body of Knowledge (PMBOK) developed by the Project Management Institute (PMI), can be used when improving IT services. Not all improvements will require a structured project approach, but many will, due to the sheer scope and scale of the improvement. Project management is discussed in more detail in *ITIL Service Transition*.

Visit www.msp-officialsite.com for more information on MSP.

Visit www.p3o-officialsite.com for more information on P3O.

Visit www.prince-officialsite.com for more information on PRINCE2.

Visit www.pmi.org for more information on PMI and PMBOK.

See also the following publications:

- Cleland, David I. and Ireland, Lewis R. (2006). *Project Management: Strategic Design and Implementation* (5th edition). McGraw-Hill Professional.
- Haugan, Gregory T. (2006). *Project Management Fundamentals*. Management Concepts.
- Office of Government Commerce (2009). *Managing Successful Projects with PRINCE2*. TSO, London.
- Cabinet Office (2011). *Managing Successful Programmes*. TSO, London.
- Office of Government Commerce (2008). *Portfolio, Programme and Project Offices*. TSO, London.
- The Project Management Institute (2008). *A Guide to the Project Management Body of Knowledge* (PMBOK Guide) (4th edition). Project Management Institute.

N.11 ORGANIZATIONAL CHANGE

There is a wide range of publications that cover organizational change including the related guidance for programme and project management referred to in the previous section.

Chapter 5 in *ITIL Service Transition* covers aspects of organizational change elements that are an essential part of, or a strong contributor towards, service transition. *ITIL Service Transition* and *ITIL Continual Service Improvement* refer to Kotter's 'eight steps for organizational change'.

Visit www.johnkotter.com for more information. See also the following publications:

- Kotter, John P. (1996). *Leading Change*. Harvard Business School Press.
- Kotter, John P. (1999) *What Leaders Really Do*. Harvard Business School Press.
- Kotter, J. P. (2000). Leading change: why transformation efforts fail. *Harvard Business Review* January–February.
- Kotter, John P. and Cohen, Dan S. (2002) *The Heart of Change: Real-Life Stories of How People Change their Organizations*. Harvard Business School Press.
- Kotter, J. P. and Schlesinger, L. C. (1979). Choosing strategies for change. *Harvard Business Review* Vol. 57, No. 2, p.106.
- Kotter, John P., Rathgeber, Holger, Mueller, Peter and Johnson, Spenser (2006). *Our Iceberg Is Melting: Changing and Succeeding Under Any Conditions*. St. Martin's Press.

N.12 SKILLS FRAMEWORK FOR THE INFORMATION AGE

The Skills Framework for the Information Age (SFIA) enables employers of IT professionals to carry out a range of human resource activities against a common framework including a skills audit, planning future skill requirements, development programmes, standardization of job titles and functions, and resource allocation.

SFIA provides a standardized view of the wide range of professional skills needed by people working in IT. SFIA is constructed as a simple two-dimensional matrix consisting of areas of work on one axis and levels of responsibility on the other. It uses a common language and a sensible, logical structure that can be adapted to the training and development needs of a very wide range of businesses.

Visit www.sfia.org.uk for further details.

N.13 CARNEGIE MELLON: CMMI AND ESCM FRAMEWORK

The Capability Maturity Model Integration (CMMI) is a process improvement approach developed by the Software Engineering Institute (SEI) of Carnegie Mellon University. CMMI provides organizations with the essential elements of effective processes. It can be used to guide process improvement across a project, a division or an entire organization. CMMI helps integrate traditionally separate organizational functions, sets process improvement goals and priorities, provides guidance for quality processes, and suggests a point of reference for appraising current processes. There are several CMMI models covering different domains of application.

The eSourcing Capability Model for Service Providers (eSCM-SP) is a framework developed by ITSqc at Carnegie Mellon to improve the relationship between IT service providers and their customers.

Organizations can be assessed against CMMI models using SCAMPI (Standard CMMI Appraisal Method for Process Improvement).

For more information, see www.sei.cmu.edu/cmmi/

N.14 BALANCED SCORECARD

A new approach to strategic management was developed in the early 1990s by Drs Robert Kaplan (Harvard Business School) and David Norton. They named this system the 'balanced scorecard'. Recognizing some of the weaknesses and vagueness of previous management approaches, the balanced scorecard approach provides a clear prescription as to what companies should measure in order to 'balance' the financial perspective. The balanced scorecard suggests that the organization be viewed from four perspectives, and it is valuable to develop metrics, collect data and analyse the organization relative to each of these perspectives:

- The learning and growth perspective
- The business process perspective
- The customer perspective
- The financial perspective.

Some organizations may choose to use the balanced scorecard method as a way of assessing and reporting their IT quality performance in general and their service operation performance in particular.

Further details are available through the balanced scorecard user community at www.scorecardsupport.com

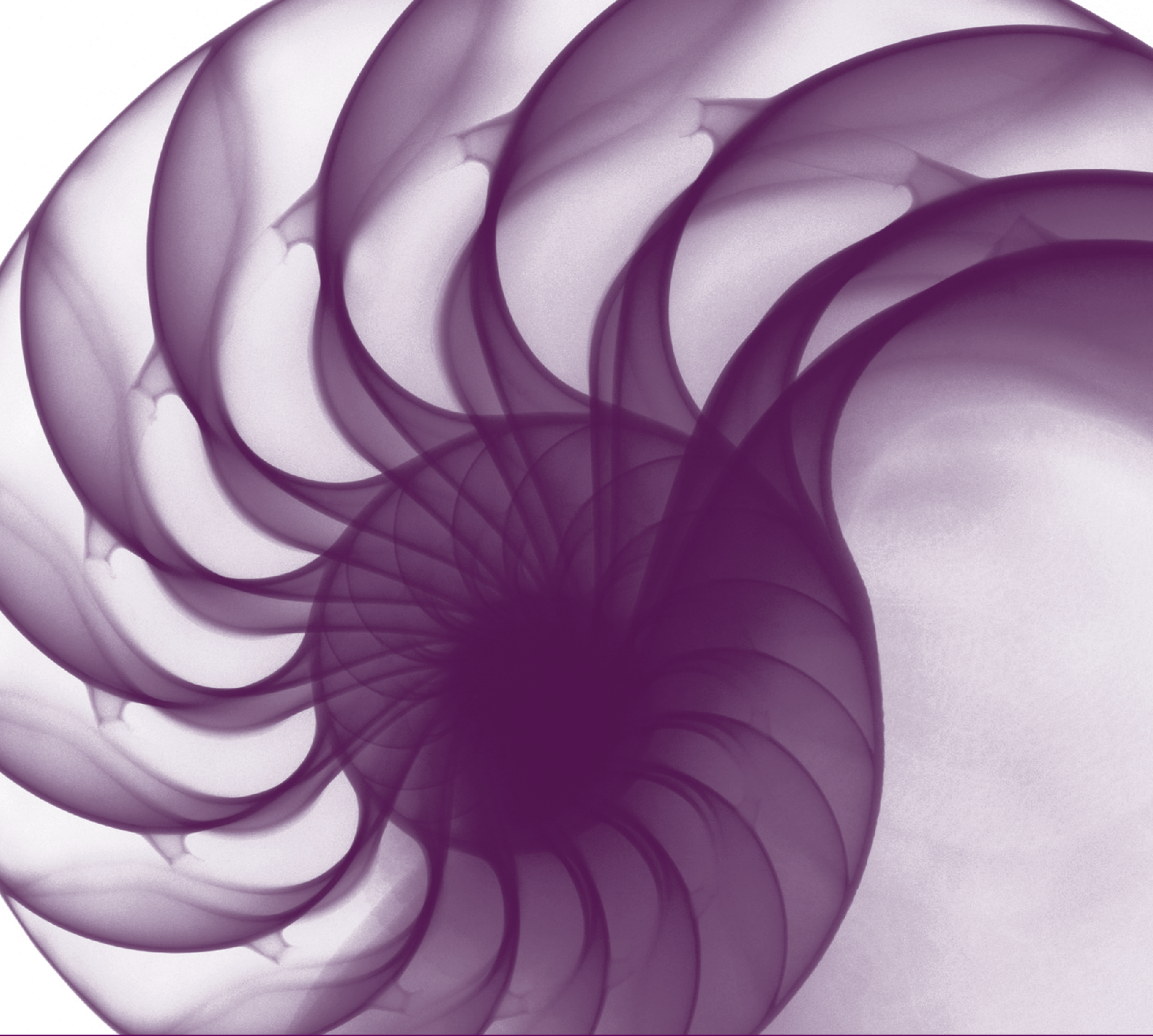
N.15 SIX SIGMA

Six Sigma is a data-driven process improvement approach that supports continual improvement. It is business-output-driven in relation to customer specification. The objective is to implement a measurement-oriented strategy focused on process improvement and defects reduction. A Six Sigma defect is defined as anything outside customer specifications.

Six Sigma focuses on dramatically reducing process variation using statistical process control (SPC) measures. The fundamental objective is to reduce errors to fewer than 3.4 defects per million executions (regardless of the process). Service providers must determine whether it is reasonable to expect delivery at a Six Sigma level given the wide variation in IT deliverables, roles and tasks within IT operational environments.

There are two primary sub-methodologies within Six Sigma: DMAIC (Define, Measure, Analyse, Improve, Control) and DMADV (Define, Measure, Analyse, Design, Verify). DMAIC is an improvement method for existing processes for which performance does not meet expectations, or for which incremental improvements are desired. DMADV focuses on the creation of new processes. For more information, see:

- George, Michael L. (2003). *Lean Six Sigma for Service: How to Use Lean Speed and Six Sigma Quality to Improve Services and Transactions*. McGraw-Hill.
- Pande, Pete and Holpp, Larry (2001) *What Is Six Sigma?* McGraw-Hill.
- Pande, Peter S., Neuman, Robert P. and Cavanagh, Roland R. (2000). *The Six Sigma Way: How GE, Motorola, and Other Top Companies are Honing their Performance*. McGraw-Hill.



Appendix O: Examples of inputs and outputs across the service lifecycle

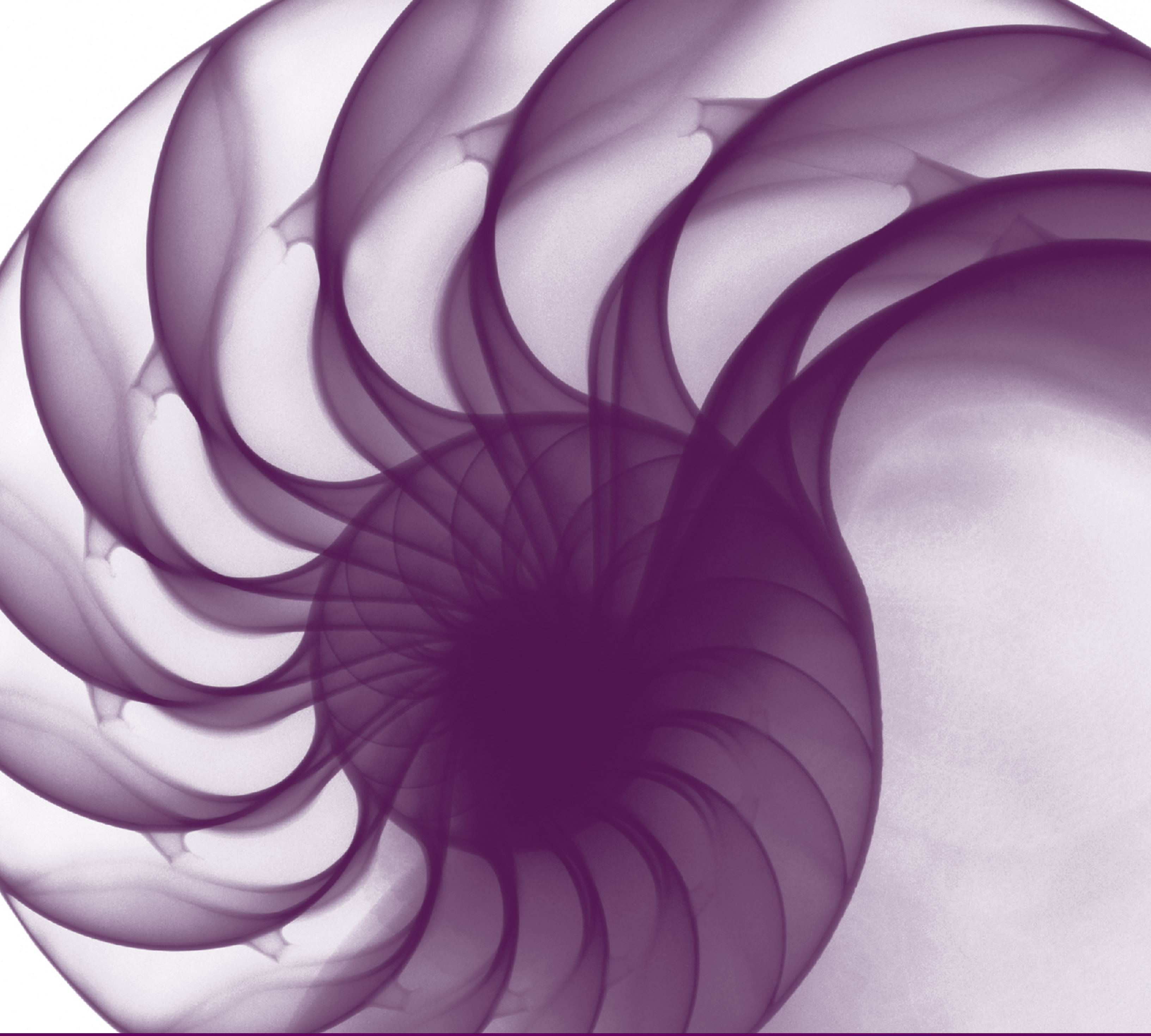
O

Appendix O: Examples of inputs and outputs across the service lifecycle

This appendix identifies some of the major inputs and outputs between each stage of the service lifecycle. This is not an exhaustive list and is designed to help understand how the different lifecycle stages interact. See Table 3.7 for more detail on the inputs and outputs of the service design stage.

Lifecycle stage	Examples of inputs from other service lifecycle stages	Examples of outputs to other service lifecycle stages
Service strategy	Information and feedback for business cases and service portfolio Requirements for strategies and plans Inputs and feedback on strategies and policies Financial reports, service reports, dashboards, and outputs of service review meetings Response to change proposals Service portfolio updates including the service catalogue Change schedule Knowledge and information in the service knowledge management system (SKMS)	Vision and mission Strategies, strategic plans and policies Financial information and budgets Service portfolio Change proposals Service charters including service packages, service models, and details of utility and warranty Patterns of business activity and demand forecasts Updated knowledge and information in the SKMS Achievements against metrics, KPIs and CSFs Feedback to other lifecycle stages Improvement opportunities logged in the CSI register
Service design	Vision and mission Strategies, strategic plans and policies Financial information and budgets Service portfolio Service charters including service packages, service models, and details of utility and warranty Feedback on all aspects of service design and service design packages Requests for change (RFCs) for designing changes and improvements Input to design requirements from other lifecycle stages Service reports, dashboards, and outputs of service review meetings Knowledge and information in the SKMS	Service portfolio updates including the service catalogue Service design packages, including: ■ Details of utility and warranty ■ Acceptance criteria ■ Updated service models ■ Designs and interface specifications ■ Transition plans ■ Operation plans and procedures Information security policies Designs for new or changed services, management information systems and tools, technology architectures, processes, measurement methods and metrics SLAs, OLAs and underpinning contracts RFCs to transition or deploy new or changed services Financial reports Updated knowledge and information in the SKMS Achievements against metrics, KPIs and CSFs Feedback to other lifecycle stages Improvement opportunities logged in the CSI register

Lifecycle stage	Examples of inputs from other service lifecycle stages	Examples of outputs to other service lifecycle stages
Service transition	Vision and mission Strategies, strategic plans and policies Financial information and budgets Service portfolio Change proposals, including utility and warranty requirements and expected timescales RFCs for implementing changes and improvements Service design packages, including: ■ Details of utility and warranty ■ Acceptance criteria ■ Service models ■ Designs and interface specifications ■ Transition plans ■ Operation plans and procedures Input to change evaluation and change advisory board (CAB) meetings Knowledge and information in the SKMS	New or changed services, management information systems and tools, technology architectures, processes, measurement methods and metrics Responses to change proposals and RFCs Change schedule Known errors Standard changes for use in request fulfilment Knowledge and information in the SKMS (including the configuration management system) Financial reports Updated knowledge and information in the SKMS Achievements against metrics, KPIs and CSFs Feedback to other lifecycle stages Improvement opportunities logged in the CSI register
Service operation	Vision and mission Strategies, strategic plans and policies Financial information and budgets Service portfolio Service reports, dashboards, and outputs of service review meetings Service design packages, including: ■ Details of utility and warranty ■ Operations plans and procedures ■ Recovery procedures Service level agreements (SLAs), operational level agreements (OLAs) and underpinning contracts Known errors Standard changes for use in request fulfilment Information security policies Change schedule Patterns of business activity and demand forecasts Knowledge and information in the SKMS	Achievement of agreed service levels to deliver value to the business Operational requirements Operational performance data and service records RFCs to resolve operational issues Financial reports Updated knowledge and information in the SKMS Achievements against metrics, KPIs and CSFs Feedback to other lifecycle stages Improvement opportunities logged in the CSI register
Continual service improvement	Vision and mission Strategies, strategic plans and policies Financial information and budgets Service portfolio Achievements against metrics, key performance indicators (KPIs) and critical success factors (CSFs) from each lifecycle stage Operational performance data and service records Improvement opportunities logged in the CSI register Knowledge and information in the SKMS	RFCs for implementing improvements across all lifecycle stages Business cases for significant improvements Updated CSI register Service improvement plans Results of customer and user satisfaction surveys Service reports, dashboards, and outputs of service review meetings Financial reports Updated knowledge and information in the SKMS Achievements against metrics, KPIs and CSFs Feedback to other lifecycle stages



Abbreviations and glossary

Abbreviations

ACD	automatic call distribution
AM	availability management
AMIS	availability management information system
ASP	application service provider
AST	agreed service time
BCM	business continuity management
BCP	business continuity plan
BIA	business impact analysis
BMP	Best Management Practice
BRM	business relationship manager
BSI	British Standards Institution
CAB	change advisory board
CAPEX	capital expenditure
CCM	component capacity management
CFIA	component failure impact analysis
CI	configuration item
CMDB	configuration management database
CMIS	capacity management information system
CMM	capability maturity model
CMMI	Capability Maturity Model Integration
CMS	configuration management system
COBIT	Control OBjectives for Information and related Technology
COTS	commercial off the shelf
CSF	critical success factor
CSI	continual service improvement
CTI	computer telephony integration
DIKW	Data-to-Information-to-Knowledge-to-Wisdom
DML	definitive media library
ECAB	emergency change advisory board
ELS	early life support
eSCM-CL	eSourcing Capability Model for Client Organizations
eSCM-SP	eSourcing Capability Model for Service Providers
FTA	fault tree analysis
IRR	internal rate of return
ISG	IT steering group
ISM	information security management
ISMS	information security management system
ISO	International Organization for Standardization
ISP	internet service provider
IT	information technology
ITSCM	IT service continuity management
ITSM	IT service management
itSMF	IT Service Management Forum
IVR	interactive voice response
KEDB	known error database
KPI	key performance indicator
LOS	line of service
MIS	management information system
M_o_R	Management of Risk
MTBF	mean time between failures
MTBSI	mean time between service incidents
MTRS	mean time to restore service
MTTR	mean time to repair
NPV	net present value
OLA	operational level agreement
OPEX	operational expenditure
PBA	pattern of business activity
PDCA	Plan-Do-Check-Act
PFS	prerequisite for success
PIR	post-implementation review
PMBOK	Project Management Body of Knowledge
PMI	Project Management Institute
PMO	project management office
PRINCE2	PRojects IN Controlled Environments
PSO	projected service outage
QA	quality assurance
QMS	quality management system

RACI	responsible, accountable, consulted and informed
RCA	root cause analysis
RFC	request for change
ROA	return on assets
ROI	return on investment
RPO	recovery point objective
RTO	recovery time objective
SAC	service acceptance criteria
SACM	service asset and configuration management
SAM	software asset management
SCM	service capacity management
SCMIS	supplier and contract management information system
SDP	service design package
SFA	service failure analysis
SIP	service improvement plan
SKMS	service knowledge management system
SLA	service level agreement
SLM	service level management
SLP	service level package
SLR	service level requirement
SMART	specific, measurable, achievable, relevant and time-bound
SMIS	security management information system
SMO	service maintenance objective
SoC	separation of concerns
SOP	standard operating procedure
SOR	statement of requirements
SOX	Sarbanes-Oxley (US law)
SPI	service provider interface
SPM	service portfolio management
SPOF	single point of failure
TCO	total cost of ownership
TCU	total cost of utilization
TO	technical observation
TOR	terms of reference
TQM	total quality management
UC	underpinning contract
UP	user profile
VBF	vital business function
VOI	value on investment
WIP	work in progress

Glossary

The core ITIL publications (*ITIL Service Strategy*, *ITIL Service Design*, *ITIL Service Operation*, *ITIL Service Transition*, *ITIL Continual Service Improvement*) referred to in parentheses at the beginning of a definition indicate where a reader can find more information. Terms without such a reference may either be used generically across all five core publications, or simply may not be explained in any greater detail elsewhere in the ITIL series. In other words, readers are only directed to other sources where they can expect to expand on their knowledge or to see a greater context.

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 change evaluation or testing and is often required before proceeding to the next stage of a project or process. *See also* service acceptance criteria.

access management

(*ITIL 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 them. Access management implements the policies of information security management and is sometimes referred to as rights management or identity management.

accounting

(*ITIL Service Strategy*) The process responsible for identifying the 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.

active monitoring

(*ITIL Service Operation*) Monitoring of a configuration item or an IT service that uses automated regular checks to discover the current status. *See also* passive monitoring.

activity

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.

agreed service time (AST)

(*ITIL Service Design*) A synonym for service hours, commonly used in formal calculations of availability. *See also* downtime.

agreement

A document that describes a formal understanding between two or more parties. An agreement is not legally binding, unless it forms part of a contract. *See also* operational level agreement; service level agreement.

alert

(*ITIL Service Operation*) A notification 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.

analytical modelling

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) (*ITIL Service Strategy*) A technique that uses mathematical models to predict the behaviour of IT services or other configuration items. Analytical models are commonly used in capacity management and availability management. *See also* modelling; simulation modelling.

application

Software that provides functions which 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 also* application management; application portfolio.

application management

(*ITIL Service Operation*) The function responsible for managing applications throughout their lifecycle.

application portfolio

(*ITIL Service Design*) A database or structured document used to manage applications throughout their lifecycle. The application portfolio contains key attributes of all applications. The application portfolio is sometimes implemented as part of the service portfolio, or as part of the configuration management system.

application service provider (ASP)

(*ITIL Service Design*) 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

(*ITIL Service Design*) 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.

architecture

(*ITIL Service Design*) 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 that guide the design and evolution of the system.

assembly

(*ITIL Service Transition*) A configuration item that is made up of a number of other CIs. For example, a server CI may contain CIs for CPUs, disks, memory etc.; an IT service CI may contain many hardware, software and other CIs. *See also* build; component CI.

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 also* audit.

asset

(*ITIL Service Strategy*) Any resource or capability. The 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 or financial capital. *See also* customer asset; service asset; strategic asset.

asset management

(*ITIL Service Transition*) A generic activity or process responsible for tracking and reporting the value and ownership of assets throughout their lifecycle. *See also* service asset and configuration management; fixed asset management; software asset management.

attribute

(*ITIL Service Transition*) A piece of information about a configuration item. Examples are name, location, version number and cost. Attributes of CIs are recorded in a configuration management database (CMDB) and maintained as part of a configuration management system (CMS). *See also* relationship; configuration management system.

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 also* assessment; certification.

authority matrix

See RACI.

availability

(*ITIL Service Design*) Ability of an IT service or other configuration item 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 of an IT service using measurements of the business output.

availability management (AM)

(*ITIL Service Design*) The process responsible for ensuring that IT services meet the current and future availability needs of the business in a cost-effective and timely manner. Availability management defines, analyses, plans, measures and improves all aspects of the availability of IT services, and ensures that all IT infrastructures, processes, tools, roles etc. are appropriate for the agreed service level targets for availability. *See also* availability management information system.

availability management information system (AMIS)

(*ITIL Service Design*) A set of tools, data and information that is used to support availability management. *See also* service knowledge management system.

availability plan

(*ITIL Service Design*) A plan to ensure that existing and future availability requirements for IT services can be provided cost-effectively.

back-out

(*ITIL Service Transition*) An activity that restores a service or other configuration item to a previous baseline. Back-out is used as a form of remediation when a change or release is not successful.

backup

(*ITIL Service Design*) (*ITIL Service Operation*) Copying data to protect against loss of integrity or availability of the original.

balanced scorecard

(*ITIL Continual Service Improvement*) A management tool developed by Drs Robert Kaplan (Harvard Business School) and David Norton. A balanced scorecard enables a strategy to be broken down into key performance indicators. Performance against the KPIs is used to demonstrate how well the strategy is being achieved. A balanced scorecard has four major areas, each of which has a small number of KPIs. The same four areas are considered at different levels of detail throughout the organization.

baseline

(*ITIL Continual Service Improvement*) (*ITIL Service Transition*) A snapshot that is used as a reference point. Many snapshots may be taken and recorded over time but only some will be used as baselines. 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 baseline can be used as part of a back-out plan to enable the IT infrastructure to be restored to a known configuration if a change or release fails.

See also benchmark.

benchmark

(*ITIL Continual Service Improvement*) (*ITIL Service Transition*) A baseline that is used to compare related data sets as part of a benchmarking exercise. For example, a recent snapshot of a process can be compared to a previous baseline of that process, or a current baseline can be compared to industry data or best practice. *See also* benchmarking; baseline.

benchmarking

(*ITIL Continual Service Improvement*) The process responsible for comparing a benchmark with related data sets such as a more recent snapshot, industry data or best practice. The term is also used to mean creating a series of benchmarks over time, and comparing the results to measure progress or improvement. This process is not described in detail within the core ITIL publications.

Best Management Practice (BMP)

The Best Management Practice portfolio is owned by the Cabinet Office, part of HM Government. Formerly owned by CCTA and then OGC, the BMP functions moved to the Cabinet Office in June 2010. The BMP portfolio includes guidance on IT service management and project, programme, risk, portfolio and value management. There is also a management maturity model as well as related glossaries of terms.

best practice

Proven activities or processes that have been successfully used by multiple organizations. ITIL is an example of best practice.

billing

(*ITIL Service Strategy*) Part of the charging process. Billing is the activity responsible for producing an invoice or a bill and recovering the money from customers. *See also* pricing.

brainstorming

(*ITIL Service Design*) (*ITIL Service Operation*) A technique that helps a team to generate ideas. Ideas are not reviewed during the brainstorming session, but at a later stage. Brainstorming is often used by problem management to identify possible causes.

British Standards Institution (BSI)

The UK national standards body, responsible for creating and maintaining British standards. See www.bsi-global.com for more information. *See also* International Organization for Standardization.

budget

A list of all the money an organization or business unit plans to receive, and plans to pay out, over a specified period of time. *See also* budgeting; planning.

budgeting

The activity of predicting and controlling the spending of money. Budgeting consists of a periodic negotiation cycle to set future budgets (usually annual) and the day-to-day monitoring and adjusting of current budgets.

build

(*ITIL Service Transition*) The activity of assembling a number of configuration items to create part of an IT service. The term is also used to refer to a release that is authorized for distribution – for example, server build or laptop build. *See also* configuration baseline.

business

(*ITIL Service Strategy*) An overall corporate entity or organization formed of a number of business units. In the context of ITSM, the term includes public sector and not-for-profit organizations, as well as companies. An IT service provider provides IT services to a customer within a business. The IT service provider may be part of the same business as its customer (internal service provider), or part of another business (external service provider).

business capacity management

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) In the context of ITSM, business capacity management is the sub-process of capacity management responsible for understanding future business requirements for use in the capacity plan. *See also* service capacity management; component capacity management.

business case

(*ITIL Service Strategy*) Justification for a significant item of expenditure. The business case includes information about costs, benefits, options, issues, risks and possible problems. *See also* cost benefit analysis.

business continuity management (BCM)

(*ITIL Service Design*) The business process responsible for managing risks that could seriously affect the business. Business continuity management safeguards the interests of key stakeholders, reputation, brand and value-creating activities. The process involves reducing risks to an acceptable level and planning for the recovery of business processes should a disruption to the business occur. Business continuity management sets the objectives, scope and requirements for IT service continuity management.

business continuity plan (BCP)

(*ITIL Service Design*) A plan defining the steps required to restore business processes following a disruption. The plan also identifies the triggers for invocation, people to be involved, communications etc. IT service continuity plans form a significant part of business continuity plans.

business customer

(*ITIL Service Strategy*) A recipient of a product or a service from the business. For example, if the business is a car manufacturer, then the business customer is someone who buys a car.

business impact analysis (BIA)

(*ITIL Service Strategy*) Business impact analysis 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. Business impact analysis 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 objective

(*ITIL Service Strategy*) The objective of a business process, or of the business as a whole. Business objectives support the business vision, provide guidance for the IT strategy, and are often supported by IT services.

business operations

(*ITIL Service Strategy*) The day-to-day execution, monitoring and management of business processes.

business perspective

(*ITIL Continual Service Improvement*) An understanding of the service provider and IT services from the point of view of the business, and an understanding of the business from the point of view of the service provider.

business process

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 that helps to deliver services to its business customers. Many business processes rely on IT services.

business relationship management

(*ITIL Service Strategy*) The process responsible for maintaining a positive relationship with customers. Business relationship management identifies customer needs and ensures that the service provider is able to meet these needs with an appropriate catalogue of services. This process has strong links with service level management.

business relationship manager (BRM)

(*ITIL Service Strategy*) A role responsible for maintaining the relationship with one or more customers. This role is often combined with the service level manager role.

business service

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. A business service may consist almost entirely of an IT service – for example, an online banking service or an external website where product orders can be placed by business customers. *See also* customer-facing service.

business service management

The management of business services delivered to business customers. Business service management is performed by business units.

business unit

(*ITIL Service Strategy*) A segment of the business that 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.

call

(*ITIL 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.

call centre

(*ITIL Service Operation*) An organization or business unit that handles large numbers of incoming and outgoing telephone calls. *See also* service desk.

capability

(*ITIL Service Strategy*) The ability of an organization, person, process, application, IT service or other configuration item to carry out an activity. Capabilities are intangible assets of an organization. *See also* resource.

Capability Maturity Model Integration (CMMI)

(*ITIL Continual Service Improvement*) A process improvement approach developed by the Software Engineering Institute (SEI) of Carnegie Mellon University, US. CMMI provides organizations with the essential elements of effective processes. It can be used to guide process improvement across a project, a division or an entire organization. CMMI helps integrate traditionally separate organizational functions, set process improvement goals and priorities, provide guidance for quality processes, and provide a point of reference for appraising current processes. See www.sei.cmu.edu/cmmi for more information. *See also* maturity.

capacity

(*ITIL Service Design*) The maximum throughput that a configuration item or IT service can deliver. For some types of CI, capacity may be the size or volume – for example, a disk drive.

capacity management

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) The process responsible for ensuring that the capacity of IT services and the IT infrastructure is able to meet agreed capacity- and performance-related requirements in a cost-effective and timely manner. Capacity management considers all resources required to deliver an IT service, and is concerned with meeting both the current and future capacity and performance needs of the business. Capacity management includes three sub processes: business capacity management, service capacity management, and component capacity management. *See also* capacity management information system.

capacity management information system (CMIS)

(*ITIL Service Design*) A set of tools, data and information that is used to support capacity management. *See also* service knowledge management system.

capacity plan

(*ITIL Service Design*) A plan used to manage the resources required to deliver IT services. The plan contains details of current and historic usage of IT services and components, and any issues that need to be addressed (including related improvement activities). The plan also contains scenarios for different predictions of business demand and costed options to deliver the agreed service level targets.

capacity planning

(*ITIL Service Design*) The activity within capacity management responsible for creating a capacity plan.

capital expenditure (CAPEX)

See capital cost.

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, while 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 is also used to mean awarding a certificate to provide evidence that a person has achieved a qualification.

change

(*ITIL Service Transition*) The addition, modification or removal of anything that could have an effect on IT services. The scope should include changes to all architectures, processes, tools, metrics and documentation, as well as changes to IT services and other configuration items.

change advisory board (CAB)

(*ITIL Service Transition*) A group of people that support the assessment, prioritization, authorization and scheduling of changes. A change advisory board is usually made up of representatives from: all areas within the IT service provider; the business; and third parties such as suppliers.

change evaluation

(*ITIL Service Transition*) The process responsible for formal assessment of a new or changed IT service to ensure that risks have been managed and to help determine whether to authorize the change.

change history

(*ITIL Service Transition*) Information about all changes made to a configuration item during its life. Change history consists of all those change records that apply to the CI.

change management

(*ITIL Service Transition*) The process responsible for controlling the lifecycle of all changes, enabling beneficial changes to be made with minimum disruption to IT services.

change model

(*ITIL Service Transition*) A repeatable way of dealing with a particular category of change. A change model defines specific agreed steps that will be followed for a change of this category. Change models may be very complex with many steps that require authorization (e.g. major software release) or may be very simple with no requirement for authorization (e.g. password reset). *See also* change advisory board; standard change.

change proposal

(*ITIL Service Strategy*) (*ITIL Service Transition*) A document that includes a high level description of a potential service introduction or significant change, along with a corresponding business case and an expected implementation schedule. Change proposals are normally created by the service portfolio management process and are passed to change management for authorization. Change management will review the potential impact on other services, on shared resources, and on the overall change schedule. Once the change proposal has been authorized, service portfolio management will charter the service.

change record

(*ITIL Service Transition*) 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 may be stored in the configuration management system, or elsewhere in the service knowledge management system.

change request

See request for change.

change schedule

(*ITIL Service Transition*) A document that lists all authorized changes and their planned implementation dates, as well as the estimated dates of longer-term changes. A change schedule is sometimes called a forward schedule of change, even though it also contains information about changes that have already been implemented.

change window

(*ITIL Service Transition*) A regular, agreed time when changes or releases may be implemented with minimal impact on services. Change windows are usually documented in service level agreements.

charging

(*ITIL Service Strategy*) Requiring payment for IT services. Charging for IT services is optional, and many organizations choose to treat their IT service provider as a cost centre. *See also* charging process; charging policy.

charging policy

(*ITIL Service Strategy*) A policy specifying the objective of the charging process and the way in which charges will be calculated. *See also* cost.

charging process

(*ITIL Service Strategy*) The process responsible for deciding how much customers should pay (pricing) and recovering money from them (billing). This process is not described in detail within the core ITIL publications.

charter

(*ITIL Service Strategy*) A document that contains details of a new service, a significant change or other significant project. Charters are typically authorized by service portfolio management or by a project management office. The term charter is also used to describe the act of authorizing the work required to complete the service change or project. *See also* change proposal; service charter; project portfolio.

classification

The act of assigning a category to something. Classification is used to ensure consistent management and reporting. Configuration items, incidents, problems, changes etc. are usually classified.

client

A generic term that means a customer, the business or a business customer. For example, client manager may be used as a synonym for business relationship manager. The term is also used to mean:

- A computer that is used directly by a user – for example, a PC, a handheld computer or a work station
- The part of a client server application that the user directly interfaces with – for example, an email client.

closed

(*ITIL Service Operation*) The final status in the lifecycle of an incident, problem, change etc. When the status is closed, no further action is taken.

closure

(*ITIL Service Operation*) The act of changing the status of an incident, problem, change etc. to closed.

COBIT

(*ITIL Continual Service Improvement*) Control OBjectives for Information and related Technology (COBIT) provides guidance and best practice for the management of IT processes. COBIT is published by ISACA in conjunction with the IT Governance Institute (ITGI). See www.isaca.org for more information.

code of practice

A guideline published by a public body or a standards organization, such as ISO or BSI. Many standards consist of a code of practice and a specification. The code of practice describes recommended best practice.

cold standby

See gradual recovery.

commercial off the shelf (COTS)

(*ITIL Service Design*) Pre-existing application software or middleware that can be purchased from a third party.

compliance

Ensuring that a standard or set of guidelines is followed, or that proper, consistent accounting or other practices are being employed.

component

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.

component capacity management (CCM)

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) The sub-process of capacity management responsible for understanding the capacity, utilization and performance of configuration items. Data is collected, recorded and analysed for use in the capacity plan. *See also* business capacity management; service capacity management.

component CI

(*ITIL Service Transition*) A configuration item that is part of an assembly. For example, a CPU or memory CI may be part of a server CI.

component failure impact analysis (CFIA)

(*ITIL Service Design*) A technique that helps to identify the impact of configuration item failure on IT services and the business. A matrix is created with IT services on one axis and CIs on the other. This enables the identification of critical CIs (that could cause the failure of multiple IT services) and fragile IT services (that have multiple single points of failure).

concurrency

A measure of the number of users engaged in the same operation at the same time.

confidentiality

(*ITIL Service Design*) A security principle that requires that data should only be accessed by authorized people.

configuration

(*ITIL Service Transition*) 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 configuration items.

configuration baseline

(*ITIL Service Transition*) The 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 item (CI)

(*ITIL Service Transition*) Any component or other service asset that needs to be managed in order to deliver an IT service. Information about each configuration item is recorded in a configuration record within the configuration management system and is maintained throughout its lifecycle by service asset and configuration management. Configuration items are under the control of change management. They typically include IT services, hardware, software, buildings, people and formal documentation such as process documentation and service level agreements.

configuration management

See service asset and configuration management.

configuration management database (CMDB)

(*ITIL Service Transition*) A database used to store configuration records throughout their lifecycle. The configuration management system maintains one or more configuration management databases, and each database stores attributes of configuration items, and relationships with other configuration items.

configuration management system (CMS)

(*ITIL Service Transition*) A set of tools, data and information that is used to support service asset and configuration management. The CMS is part of an overall service knowledge management system and includes tools for collecting, storing, managing, updating, analysing and presenting data about all configuration items and their relationships. The CMS may also include information about incidents, problems, known errors, changes and releases. The CMS is maintained by service asset and configuration management and is used by all IT service management processes. *See also* configuration management database.

continual service improvement (CSI)

(*ITIL Continual Service Improvement*) A stage in the lifecycle of a service. Continual service improvement ensures that services are aligned with changing business needs by identifying and implementing improvements to IT services that support business processes. 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. Continual service improvement includes the seven-step improvement process. Although this process is associated with continual service improvement, most processes have activities that take place across multiple stages of the service lifecycle. *See also* Plan-Do-Check-Act.

continuous availability

(*ITIL Service Design*) An approach or design to achieve 100% availability. A continuously available IT service has no planned or unplanned downtime.

continuous operation

(*ITIL Service Design*) An approach or design to eliminate planned downtime of an IT service. Note that individual configuration items may be down even though the IT service is available.

contract

A legally binding agreement between two or more parties.

control

A means of managing a risk, ensuring that a business objective is achieved or that a process is followed. Examples of control 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.

Control OBjectives for Information and related Technology

See COBIT.

control perspective

(*ITIL Service Strategy*) An approach to the management of IT services, processes, functions, assets etc. There can be several different control perspectives on the same IT service, process etc., allowing different individuals or teams to focus on what is important and relevant to their specific role. Examples of control perspective include reactive and proactive management within IT operations, or a lifecycle view for an application project team.

control processes

The ISO/IEC 20000 process group that includes change management and configuration management.

core service

(*ITIL Service Strategy*) A service that delivers the basic outcomes desired by one or more customers. A core service provides a specific level of utility and warranty. Customers may be offered a choice of utility and warranty through one or more service options. *See also* enabling service; enhancing service; IT service; service package.

cost

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.

cost benefit analysis

An activity that analyses and compares the costs and the benefits involved in one or more alternative courses of action. *See also* business case; internal rate of return; net present value; return on investment; value on investment.

cost element

(*ITIL Service Strategy*) The middle level of category to which costs are assigned in budgeting and accounting. The highest-level category is cost type. For example, a cost type of 'people' could have cost elements of payroll, staff benefits, expenses, training, overtime etc. Cost elements can be further broken down to give cost units. For example, the cost element 'expenses' could include cost units of hotels, transport, meals etc.

cost model

(*ITIL Service Strategy*) A framework used in budgeting and accounting in which all known costs can be recorded, categorized and allocated to specific customers, business units or projects. *See also* cost type; cost element; cost unit.

cost type

(*ITIL Service Strategy*) The highest level of category to which costs are assigned in budgeting and accounting – for example, hardware, software, people, accommodation, external and transfer. *See also* cost element; cost unit.

cost unit

(*ITIL Service Strategy*) The lowest level of category to which costs are assigned, cost units are usually things that can be easily counted (e.g. staff numbers, software licences) or things easily measured (e.g. CPU usage, electricity consumed). Cost units are included within cost elements. For example, a cost element of 'expenses' could include cost units of hotels, transport, meals etc. *See also* cost type.

cost effectiveness

A measure of the balance between the effectiveness and cost of a service, process or activity. A cost-effective process is one that achieves its objectives at minimum cost. *See also* key performance indicator; return on investment; value for money.

countermeasure

Can be used to refer to any type of control. The term is most often used when referring to measures that increase resilience, fault tolerance or reliability of an IT service.

course corrections

Changes made to a plan or activity that has already started to ensure that it will meet its objectives. Course corrections are made as a result of monitoring progress.

crisis management

Crisis management is 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.

critical success factor (CSF)

Something that must happen if an IT service, process, plan, project or other activity is to succeed. Key performance indicators are used to measure the achievement of each critical success factor. For example, a critical success factor of 'protect IT services when making changes' could be measured by key performance indicators such as 'percentage reduction of unsuccessful changes', 'percentage reduction in changes causing incidents' etc.

CSI register

(*ITIL Continual Service Improvement*) A database or structured document used to record and manage improvement opportunities throughout their lifecycle.

culture

A set of values that is shared by a group of people, including expectations about how people should behave, their ideas, beliefs and practices. *See also* vision.

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 is also sometimes used informally to mean user – for example, 'This is a customer-focused organization.'

customer asset

Any resource or capability of a customer. *See also* asset.

customer agreement portfolio

(*ITIL Service Strategy*) A database or structured document used to manage service contracts or agreements between an IT service provider and its customers. Each IT service delivered to a customer should have a contract or other agreement that is listed in the customer agreement portfolio. *See also* customer-facing service; service catalogue; service portfolio.

customer-facing service

(*ITIL Service Design*) An IT service that is visible to the customer. These are normally services that support the customer's business processes and facilitate one or more outcomes desired by the customer. All live customer-facing services, including those available for deployment, are recorded in the service catalogue along with customer-visible information about deliverables, prices, contact points, ordering and request processes. Other information such as relationships to supporting services and other CIs will also be recorded for internal use by the IT service provider.

dashboard

(*ITIL 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 and incident diagnosis.

Data-to-Information-to-Knowledge-to-Wisdom (DIKW)

(*ITIL Service Transition*) A way of understanding the relationships between data, information, knowledge and wisdom. DIKW shows how each of these builds on the others.

definitive media library (DML)

(*ITIL Service Transition*) One or more locations in which the definitive and authorized versions of all software configuration items are securely stored. The definitive media library may also contain associated configuration items such as licences and documentation. It is a single logical storage area even if there are multiple locations. The definitive media library is controlled by service asset and configuration management and is recorded in the configuration management system.

deliverable

Something that must be provided to meet a commitment in a service level agreement or a contract. It is also used in a more informal way to mean a planned output of any process.

demand management

(*ITIL Service Design*) (*ITIL Service Strategy*) The process responsible for understanding, anticipating and influencing customer demand for services. Demand management works with capacity management to ensure that the service provider has sufficient capacity to meet the required demand. At a strategic level, demand management can involve analysis of patterns of business activity and user profiles, while at a tactical level, it can involve the use of differential charging to encourage customers to use IT services at less busy times, or require short-term activities to respond to unexpected demand or the failure of a configuration item.

Deming Cycle

See Plan-Do-Check-Act.

dependency

The direct or indirect reliance of one process or activity on another.

deployment

(*ITIL Service Transition*) The activity responsible for movement of new or changed hardware, software, documentation, process etc. to the live environment. Deployment is part of the release and deployment management process.

design

(*ITIL Service Design*) An activity or process that identifies requirements and then defines a solution that is able to meet these requirements. *See also* service design.

design coordination

(*ITIL Service Design*) The process responsible for coordinating all service design activities, processes and resources. Design coordination ensures the consistent and effective design of new or changed IT services, service management information systems, architectures, technology, processes, information and metrics.

detection

(*ITIL Service Operation*) A stage in the expanded incident lifecycle. Detection results in the incident becoming known to the service provider. Detection can be automatic or the result of a user logging an incident.

development

(*ITIL Service Design*) The process responsible for creating or modifying an IT service or application ready for subsequent release and deployment. Development is also used to mean the role or function that carries out development work. This process is not described in detail within the core ITIL publications.

development environment

(*ITIL Service Design*) An environment used to create or modify IT services or applications. Development environments are not typically subjected to the same degree of control as test or live environments. *See also* development.

diagnosis

(*ITIL 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.

differential charging

A technique used to support demand management by charging different amounts for the same function of an IT service under different circumstances. For example, reduced charges outside peak times, or increased charges for users who exceed a bandwidth allocation.

document

Information in readable form. A document may be paper or electronic – for example, a policy statement, service level agreement, incident record or diagram of a computer room layout. *See also* record.

downtime

(*ITIL Service Design*) (*ITIL Service Operation*) The time when an IT service or other configuration item is not available during its agreed service time. The availability of an IT service is often calculated from agreed service time and downtime.

driver

Something that influences strategy, objectives or requirements – for example, new legislation or the actions of competitors.

early life support (ELS)

(*ITIL Service Transition*) A stage in the service lifecycle that occurs at the end of deployment and before the service is fully accepted into operation. During early life support, the service provider reviews key performance indicators, service levels and monitoring thresholds and may implement improvements to ensure that service targets can be met. The service provider may also provide additional resources for incident and problem management during this time.

economies of scale

(*ITIL Service Strategy*) The reduction in average cost that is possible from increasing the usage of an IT service or asset. *See also* economies of scope.

economies of scope

(*ITIL Service Strategy*) The reduction in cost that is allocated to an IT service by using an existing asset for an additional purpose. For example, delivering a new IT service from an existing IT infrastructure. *See also* economies of scale.

effectiveness

(*ITIL Continual Service Improvement*) 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 also* key performance indicator.

efficiency

(*ITIL Continual Service Improvement*) A measure of whether the right amount of resource has 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 also* key performance indicator.

emergency change

(*ITIL Service Transition*) 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 also* emergency change advisory board.

emergency change advisory board (ECAB)

(*ITIL Service Transition*) A subgroup of the change advisory board that makes decisions about emergency changes. Membership may be decided at the time a meeting is called, and depends on the nature of the emergency change.

enabling service

(*ITIL Service Strategy*) A service that is needed in order to deliver a core service. Enabling services may or may not be visible to the customer, but they are not offered to customers in their own right. *See also* enhancing service.

enhancing service

(*ITIL Service Strategy*) A service that is added to a core service to make it more attractive to the customer. Enhancing services are not essential to the delivery of a core service but are used to encourage customers to use the core services or to differentiate the service provider from its competitors. *See also* enabling service; excitement factor.

enterprise financial management

(*ITIL Service Strategy*) The function and processes responsible for managing the overall organization's budgeting, accounting and charging requirements. Enterprise financial management is sometimes referred to as the 'corporate' financial department. *See also* financial management for IT services.

environment

(*ITIL Service Transition*) A subset of the IT infrastructure that is used for a particular purpose – for example, live environment, test environment, build environment. Also used in the term 'physical environment' to mean the accommodation, air conditioning, power system etc. Environment is used as a generic term to mean the external conditions that influence or affect something.

error

(*ITIL Service Operation*) A design flaw or malfunction that causes a failure of one or more IT services or other configuration items. A mistake made by a person or a faulty process that impacts a configuration item is also an error.

escalation

(*ITIL 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.

eSourcing Capability Model for Client Organizations (eSCM-CL)

(*ITIL Service Strategy*) A framework to help organizations in their analysis and decision-making on service sourcing models and strategies. It was developed by Carnegie Mellon University in the US. *See also* eSourcing Capability Model for Service Providers.

eSourcing Capability Model for Service Providers (eSCM-SP)

(*ITIL Service Strategy*) A framework to help IT service providers develop their IT service management capabilities from a service sourcing perspective. It was developed by Carnegie Mellon University in the US. *See also* eSourcing Capability Model for Client Organizations.

estimation

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.

event

(*ITIL Service Operation*) A change of state that has significance for the management of an IT service or other configuration item. The term 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

(*ITIL Service Operation*) 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 key performance indicators or other important targets that have exceeded defined thresholds. Examples include service level agreement targets being missed or about to be missed, and a performance metric indicating a potential capacity problem.

excitement factor

(*ITIL Service Strategy*) An attribute added to something to make it more attractive or more exciting to the customer. For example, a restaurant may provide a free drink with every meal. *See also* enhancing service.

expanded incident lifecycle

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) Detailed stages in the lifecycle of an incident. The stages are detection, diagnosis, repair, recovery and restoration. The expanded incident lifecycle is used to help understand all contributions to the impact of incidents and to plan for how these could be controlled or reduced.

external customer

A customer who works for a different business from the IT service provider. *See also* external service provider; internal customer.

external service provider

(*ITIL Service Strategy*) An IT service provider that is part of a different organization from its customer. An IT service provider may have both internal and external customers. *See also* outsourcing; Type III service provider.

facilities management

(*ITIL 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.

failure

(*ITIL Service Operation*) Loss of ability to operate to specification, or to deliver the required output. The term may be used when referring to IT services, processes, activities, configuration items etc. A failure often causes an incident.

fast recovery

(*ITIL Service Design*) A recovery option that is also known as hot standby. Fast recovery normally uses a dedicated fixed facility with computer systems and software configured ready to run the IT services. Fast recovery typically takes up to 24 hours but may be quicker if there is no need to restore data from backups.

fault

See error.

fault tolerance

(*ITIL Service Design*) The ability of an IT service or other configuration item to continue to operate correctly after failure of a component part. *See also* countermeasure; resilience.

fault tree analysis (FTA)

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) A technique that can be used to determine a chain of events that has caused an incident, or may cause an incident in the future. Fault tree analysis represents a chain of events using Boolean notation in a diagram.

financial management

(*ITIL Service Strategy*) A generic term used to describe the function and processes responsible for managing an organization's budgeting, accounting and charging requirements. Enterprise financial management is the specific term used to describe the function and processes from the perspective of the overall organization. Financial management for IT services is the specific term used to describe the function and processes from the perspective of the IT service provider.

financial management for IT services

(*ITIL Service Strategy*) The function and processes responsible for managing an IT service provider's budgeting, accounting and charging requirements. Financial management for IT services secures an appropriate level of funding to design, develop and deliver services that meet the strategy of the organization in a cost-effective manner. *See also* enterprise financial management.

fit for purpose

(*ITIL Service Strategy*) The ability to meet an agreed level of utility. Fit for purpose is also used informally 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.

fit for use

(*ITIL Service Strategy*) The ability to meet an agreed level of warranty. Being fit for use requires suitable design, implementation, control and maintenance.

fixed asset management

(*ITIL Service Transition*) The process responsible for tracking and reporting the value and ownership of fixed assets throughout their lifecycle. Fixed asset management maintains the asset register and is usually carried out by the overall business, rather than by the IT organization. Fixed asset management is sometimes called financial asset management and is not described in detail within the core ITIL publications.

fixed cost

(*ITIL Service Strategy*) A cost that does not vary with IT service usage – for example, the cost of server hardware. *See also* variable cost.

fixed facility

(*ITIL Service Design*) A permanent building, available for use when needed by an IT service continuity plan. *See also* portable facility; recovery option.

fulfilment

Performing activities to meet a need or requirement – for example, by providing a new IT service, or meeting a service request.

function

A team or group of people and the tools or other resources they use to carry out one or more processes or activities – for example, the service desk. The term 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, while the function of a business process may be to despatch goods to customers.
- To perform the intended purpose correctly, as in 'The computer is functioning.'

governance

Ensures 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.

gradual recovery

(*ITIL Service Design*) A recovery option that is also known as cold standby. Gradual recovery typically uses a portable or fixed facility that has environmental support and network cabling, but no computer systems. The hardware and software are installed as part of the IT service continuity plan. Gradual recovery typically takes more than three days, and may take significantly longer.

guideline

A document describing best practice, which recommends what should be done. Compliance with a guideline is not normally enforced. *See also* standard.

high availability

(*ITIL Service Design*) An approach or design that minimizes or hides the effects of configuration item failure from the users of an IT service. High availability solutions are designed to achieve an agreed level of availability and make use of techniques such as fault tolerance, resilience and fast recovery to reduce the number and impact of incidents.

hot standby

See fast recovery; immediate recovery.

immediate recovery

(*ITIL Service Design*) A recovery option that is also known as hot standby. Provision is made to recover the IT service with no significant loss of service to the customer. Immediate recovery typically uses mirroring, load balancing and split-site technologies.

impact

(*ITIL Service Operation*) (*ITIL 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.

incident

(*ITIL Service Operation*) An unplanned interruption to an IT service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident – for example, failure of one disk from a mirror set.

incident management

(*ITIL Service Operation*) The process responsible for managing the lifecycle of all incidents. Incident management ensures that normal service operation is restored as quickly as possible and the business impact is minimized.

incident record

(*ITIL Service Operation*) A record containing the details of an incident. Each incident record documents the lifecycle of a single incident.

indirect cost

(*ITIL Service Strategy*) The cost of providing an IT service which cannot be allocated in full to a specific customer – for example, the cost of providing shared servers or software licences. Also known as overhead. *See also* direct cost.

information security management (ISM)

(*ITIL Service Design*) The process responsible for ensuring that the confidentiality, integrity and availability of an organization's assets, information, data and IT services match the agreed needs of the business. Information security management supports business security and has a wider scope than that of the IT service provider, and includes handling of paper, building access, phone calls etc. for the entire organization. *See also* security management information system.

information security management system (ISMS)

(*ITIL Service Design*) The framework of policy, processes, functions, standards, guidelines and tools that ensures an organization can achieve its information security management objectives. *See also* security management information system.

information security policy

(*ITIL Service Design*) The policy that governs the organization's approach to information security management.

information system

See management information system.

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.

infrastructure service

A type of supporting service that provides hardware, network or other data centre components. The term is also used as a synonym for supporting service.

insourcing

(*ITIL Service Strategy*) Using an internal service provider to manage IT services. The term insourcing is also used to describe the act of transferring the provision of an IT service from an external service provider to an internal service provider. *See also* service sourcing.

integrity

(*ITIL Service Design*) A security principle that ensures data and configuration items are modified only by authorized personnel and activities. Integrity considers all possible causes of modification, including software and hardware failure, environmental events, and human intervention.

intermediate recovery

(*ITIL Service Design*) A recovery option that is also known as warm standby. Intermediate recovery usually uses a shared portable or fixed facility that has computer systems and network components. The hardware and software will need to be configured, and data will need to be restored, as part of the IT service continuity plan. Typical recovery times for intermediate recovery are one to three days.

internal customer

A customer who works for the same business as the IT service provider. *See also* external customer; internal service provider.

internal rate of return (IRR)

(*ITIL Service Strategy*) A technique used to help make decisions about capital expenditure. It calculates a figure that allows two or more alternative investments to be compared. A larger internal rate of return indicates a better investment. *See also* net present value; return on investment.

internal service provider

(*ITIL Service Strategy*) An IT service provider that is part of the same organization as its customer. An IT service provider may have both internal and external customers. *See also* insourcing; Type I service provider; Type II service provider.

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 that is a network of the national standards institutes of 156 countries. See www.iso.org for further information about ISO.

International Standards Organization

See International Organization for Standardization.

invocation

(*ITIL Service Design*) Initiation of the steps defined in a plan – for example, initiating the IT service continuity plan for one or more IT services.

ISO 9000

A generic term that refers to a number of international standards and guidelines for quality management systems. See www.iso.org for more information. *See also* International Organization for Standardization.

ISO 9001

An international standard for quality management systems. *See also* ISO 9000; standard.

ISO/IEC 20000

An international standard for IT service management.

ISO/IEC 27001

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) An international specification for information security management. The corresponding code of practice is ISO/IEC 27002. *See also* standard.

IT infrastructure

All of the hardware, software, networks, facilities etc. that are required to develop, test, deliver, monitor, control or support applications and IT services. The term includes all of the information technology but not the associated people, processes and documentation.

IT operations

(*ITIL Service Operation*) Activities carried out by IT operations control, including console management/operations bridge, job scheduling, backup and restore, and print and output management.
IT operations is also used as a synonym for service operation.

IT operations control

(*ITIL Service Operation*) The function responsible for monitoring and control of the IT services and IT infrastructure. *See also* operations bridge.

IT operations management

(*ITIL Service Operation*) The function within an IT service provider that 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 by an IT service provider. An IT service is made up of a combination of information technology, people and processes. A customer-facing IT service directly supports the business processes of one or more customers and its service level targets should be defined in a service level agreement. Other IT services, called supporting services, are not directly used by the business but are required by the service provider to deliver customer-facing services. *See also* core service; enabling service; enhancing service; service; service package.

IT service continuity management (ITSCM)

(*ITIL Service Design*) The process responsible for managing risks that could seriously affect IT services. IT service continuity management 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. IT service continuity management supports business continuity management.

IT service continuity plan

(*ITIL Service Design*) A plan defining the steps required to recover one or more IT services. The plan also identifies 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 also* service management.

IT service provider

(*ITIL Service Strategy*) A service provider that provides IT services to internal or external customers.

IT steering group (ISG)

(*ITIL Service Design*) (*ITIL Service Strategy*) 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. Also known as IT strategy group or IT steering committee.

ITIL

A set of best-practice publications for IT service management. Owned by the Cabinet Office (part of HM Government), ITIL gives guidance on the provision of quality IT services and the processes, functions and other capabilities needed to support them. The ITIL framework is based on a service lifecycle and consists of five lifecycle stages (service strategy, service design, service transition, service operation and continual service improvement), each of which has its own supporting publication. There is also a set of complementary ITIL publications providing guidance specific to industry sectors, organization types, operating models and technology architectures. See www.itil-officialsite.com for more information.

job description

A document that 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.

job scheduling

(*ITIL 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.

key performance indicator (KPI)

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) A metric that is used to help manage an IT service, process, plan, project or other activity. Key performance indicators are used to measure the achievement of critical success factors. Many metrics may be measured, but only the most important of these are defined as key performance indicators and used to actively manage and report on the process, IT service or activity. They should be selected to ensure that efficiency, effectiveness and cost effectiveness are all managed.

knowledge base

(*ITIL Service Transition*) A logical database containing data and information used by the service knowledge management system.

knowledge management

(*ITIL Service Transition*) The process responsible for sharing perspectives, ideas, experience and information, and for ensuring that these are available in the right place and at the right time. The knowledge management process enables informed decisions, and improves efficiency by reducing the need to rediscover knowledge. *See also* Data-to-Information-to-Knowledge-to-Wisdom; service knowledge management system.

known error

(*ITIL 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.

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, optimize
- The expanded incident lifecycle includes detection, diagnosis, repair, recovery and restoration
- The lifecycle of a server may include: ordered, received, in test, live, disposed etc.

line of service (LOS)

(*ITIL Service Strategy*) A core service or service package that has multiple service options. A line of service is managed by a service owner and each service option is designed to support a particular market segment.

live

(*ITIL Service Transition*) Refers to an IT service or other configuration item that is being used to deliver service to a customer.

live environment

(*ITIL Service Transition*) A controlled environment containing live configuration items used to deliver IT services to customers.

maintainability

(*ITIL Service Design*) A measure of how quickly and effectively an IT service or other configuration item 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

(*ITIL Service Operation*) The highest category of impact for an incident. A major incident results in significant disruption to the business.

manageability

An informal measure of how easily and effectively an IT service or other component can be managed.

management information

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 key performance indicators, such as 'percentage of changes leading to incidents' or 'first-time fix rate'.

management information system (MIS)

(*ITIL Service Design*) A set of tools, data and information that is used to support a process or function. Examples include the availability management information system and the supplier and contract management information system. *See also* service knowledge management system.

Management of Risk (M_o_R)

M_o_R 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 www.mor-officialsite.com for more details.

management system

The framework of policy, processes, functions, standards, guidelines and tools that ensures an organization or part of an organization can achieve its objectives. This term is also used with a smaller scope to support a specific process or activity – for example, an event management system or risk management system. *See also* system.

manual workaround

(*ITIL Continual Service Improvement*) 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.

market space

(*ITIL Service Strategy*) Opportunities that an IT service provider could exploit to meet the business needs of customers. Market spaces identify the possible IT services that an IT service provider may wish to consider delivering.

maturity

(*ITIL Continual Service Improvement*) A measure of the reliability, efficiency and effectiveness of a process, function, organization etc. The most mature processes and functions are formally aligned to business objectives and strategy, and are supported by a framework for continual improvement.

maturity level

A named level in a maturity model, such as the Carnegie Mellon Capability Maturity Model Integration.

mean time between failures (MTBF)

(*ITIL Service Design*) A metric for measuring and reporting reliability. MTBF is the average time that an IT service or other configuration item can perform its agreed function without interruption. This is measured from when the configuration item starts working, until it next fails.

mean time between service incidents (MTBSI)

(*ITIL Service Design*) A metric used for measuring and reporting reliability. It is the mean time from when a system or IT service fails, until it next fails. MTBSI is equal to MTBF plus MTRS.

mean time to repair (MTTR)

The average time taken to repair an IT service or other configuration item after a failure. MTTR is measured from when the configuration item fails until it is repaired. MTTR does not include the time required to recover or restore. It is sometimes incorrectly used instead of mean time to restore service.

mean time to restore service (MTRS)

The average time taken to restore an IT service or other configuration item after a failure. MTRS is measured from when the configuration item fails until it is fully restored and delivering its normal functionality. *See also* maintainability; mean time to repair.

metric

(*ITIL Continual Service Improvement*) Something that is measured and reported to help manage a process, IT service or activity. *See also* key performance indicator.

middleware

(*ITIL Service Design*) Software that connects two or more software components or applications. Middleware is usually purchased from a supplier, rather than developed within the IT service provider. *See also* commercial off the shelf.

mission

A short but complete description of the overall purpose and intentions of an organization. It states what is to be achieved, but not how this should be done. *See also* vision.

model

A representation of a system, process, IT service, configuration item etc. that is used to help understand or predict future behaviour.

modelling

A technique that is used to predict the future behaviour of a system, process, IT service, configuration item etc. Modelling is commonly used in financial management, capacity management and availability management.

monitoring

(*ITIL Service Operation*) Repeated observation of a configuration item, IT service or process to detect events and to ensure that the current status is known.

near-shore

(*ITIL Service Strategy*) Provision of services from a country near the country where the customer is based. This can be the provision of an IT service, or of supporting functions such as a service desk. *See also* offshore; onshore.

net present value (NPV)

(*ITIL Service Strategy*) A technique used to help make decisions about capital expenditure. It compares cash inflows with cash outflows. Positive net present value indicates that an investment is worthwhile. *See also* internal rate of return; return on investment.

objective

The outcomes required from a process, activity or organization in order to ensure that its purpose will be fulfilled. Objectives are usually expressed as measurable targets. The term is also informally used to mean a requirement.

off the shelf

See commercial off the shelf.

Office of Government Commerce (OGC)

OGC (former owner of Best Management Practice) and its functions have moved into the Cabinet Office as part of HM Government. See www.cabinetoffice.gov.uk

offshore

(*ITIL Service Strategy*) Provision of services from a location outside the country where the customer is based, often in a different continent. This can be the provision of an IT service, or of supporting functions such as a service desk. *See also* near-shore; onshore.

onshore

(*ITIL Service Strategy*) Provision of services from a location within the country where the customer is based. *See also* near-shore; offshore.

operate

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.

operation

(*ITIL 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.

operational

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 is also a synonym for live.

operational cost

The cost resulting from running the IT services, which often involves repeating payments – for example, staff costs, hardware maintenance and electricity (also known as current expenditure or revenue expenditure). *See also* capital expenditure.

operational level agreement (OLA)

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) An agreement between an IT service provider and another part of the same organization. It supports the IT service provider's delivery of IT services to customers and defines the goods or services to be provided and the responsibilities of both parties. For example, there could be an operational level agreement:

- 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 also service level agreement.

operations bridge

(*ITIL Service Operation*) A physical location where IT services and IT infrastructure are monitored and managed.

operations control

See IT operations control.

operations management

See IT operations management.

optimize

Review, plan and request changes, in order to obtain the maximum efficiency and effectiveness from a process, configuration item, application etc.

organization

A company, legal entity or other institution. The term is sometimes used to refer to any entity that has people, resources and budgets – for example, a project or business unit.

outcome

The result of carrying out an activity, following a process, or delivering an IT service etc. The term is used to refer to intended results as well as to actual results. *See also* objective.

outsourcing

(*ITIL Service Strategy*) Using an external service provider to manage IT services. *See also* service sourcing.

overhead

See indirect cost.

Pareto principle

(*ITIL Service Operation*) A technique used to prioritize 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 prioritize possible problem causes for investigation.

partnership

A relationship between two organizations that 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 also* value network.

passive monitoring

(*ITIL 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 also* active monitoring.

pattern of business activity (PBA)

(*ITIL Service Strategy*) 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 also* user profile.

percentage utilization

(*ITIL Service Design*) The amount of time that a component is busy over a given period of time. For example, if a CPU is busy for 1,800 seconds in a one-hour period, its utilization is 50%.

performance

A measure of what is achieved or delivered by a system, person, team, process or IT service.

performance management

Activities to ensure that something achieves its expected outcomes in an efficient and consistent manner.

pilot

(*ITIL Service Transition*) 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 also* change evaluation; test.

plan

A detailed proposal that 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.

Plan-Do-Check-Act (PDCA)

(*ITIL Continual Service Improvement*) 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.

planned downtime

(*ITIL Service Design*) Agreed time when an IT service will not be available. Planned downtime is often used for maintenance, upgrades and testing. *See also* change window; downtime.

planning

An activity responsible for creating one or more plans – for example, capacity planning.

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.

portable facility

(*ITIL Service Design*) A prefabricated building, or a large vehicle, provided by a third party and moved to a site when needed according to an IT service continuity plan. *See also* fixed facility; recovery option.

post-implementation review (PIR)

A review that takes place after a change or a project has been implemented. It determines if the change or project was successful, and identifies opportunities for improvement.

practice

A way of working, or a way in which work must be done. Practices can include activities, processes, functions, standards and guidelines. *See also* best practice.

prerequisite for success (PFS)

An activity that needs to be completed, or a condition that needs to be met, to enable successful implementation of a plan or process. It is often an output from one process that is a required input to another process.

pricing

(*ITIL Service Strategy*) Pricing is the activity for establishing how much customers will be charged.

PRINCE2

See PRojects IN Controlled Environments.

priority

(*ITIL Service Operation*) (*ITIL Service Transition*) 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 service level agreement may state that Priority 2 incidents must be resolved within 12 hours.

problem

(*ITIL 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.

problem management

(*ITIL Service Operation*) The process responsible for managing the lifecycle of all problems. Problem management proactively prevents incidents from happening and minimizes the impact of incidents that cannot be prevented.

problem record

(*ITIL Service Operation*) 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 also* 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. It 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 the 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 organizations.

process owner

The person who is held accountable 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 can be assigned to the same person who carries out the process manager role, but the two roles may be separate in larger organizations.

production environment

See live environment.

pro-forma

A template or example document containing sample data that will be replaced with real values when these are available.

programme

A number of projects and activities that are planned and managed together to achieve an overall set of related objectives and other outcomes.

project

A temporary organization, with people and other assets, that is required to achieve an objective or other outcome. Each project has a lifecycle that typically includes initiation, planning, execution, and closure. Projects are usually managed using a formal methodology such as PRojects IN Controlled Environments (PRINCE2) or the Project Management Body of Knowledge (PMBOK). *See also* charter; project management office; project portfolio.

Project Management Body of Knowledge (PMBOK)

A project management standard maintained and published by the Project Management Institute. See www.pmi.org for more information. *See also* PRojects IN Controlled Environments (PRINCE2).

Project Management Institute (PMI)

A membership association that advances the project management profession through globally recognized standards and certifications, collaborative communities, an extensive research programme, and professional development opportunities. PMI is a not-for-profit membership organization with representation in many countries around the world. PMI maintains and publishes the Project Management Body of Knowledge (PMBOK). See www.pmi.org for more information. *See also* PRojects IN Controlled Environments (PRINCE2).

project management office (PMO)

(*ITIL Service Design*) (*ITIL Service Strategy*) A function or group responsible for managing the lifecycle of projects. *See also* charter; project portfolio.

project portfolio

(*ITIL Service Design*) (*ITIL Service Strategy*) A database or structured document used to manage projects throughout their lifecycle. The project portfolio is used to coordinate projects and ensure that they meet their objectives in a cost-effective and timely manner. In larger organizations, the project portfolio is typically defined and maintained by a project management office. The project portfolio is important to service portfolio management as new services and significant changes are normally managed as projects. *See also* charter.

projected service outage (PSO)

(*ITIL Service Transition*) A document that identifies the effect of planned changes, maintenance activities and test plans on agreed service levels.

PRojects IN Controlled Environments (PRINCE2)

The standard UK government methodology for project management. See www.prince-officialsite.com for more information. *See also* Project Management Body of Knowledge (PMBOK).

qualification

(*ITIL Service Transition*) An activity that ensures that the IT infrastructure is appropriate and correctly configured to support an application or IT service. *See also* validation.

quality

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 also* quality management system.

quality assurance (QA)

(*ITIL Service Transition*) The process responsible for ensuring that the quality of a service, process or other service asset will provide its intended value. Quality assurance is also used to refer to a function or team that performs quality assurance. This process is not described in detail within the core ITIL publications. *See also* service validation and testing.

quality management system (QMS)

(*ITIL Continual Service Improvement*) The framework of policy, processes, functions, standards, guidelines and tools that ensures an organization is of a suitable quality to reliably meet business objectives or service levels. *See also* ISO 9000.

quick win

(*ITIL Continual Service Improvement*) An improvement activity that is expected to provide a return on investment in a short period of time with relatively small cost and effort. *See also* Pareto principle.

RACI

(*ITIL Service Design*) A model used to help define roles and responsibilities. RACI stands for responsible, accountable, consulted and informed.

reciprocal arrangement

(*ITIL Service Design*) A recovery option. An agreement between two organizations to share resources in an emergency – for example, high-speed printing facilities or computer room space.

record

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.

recovery

(*ITIL Service Design*) (*ITIL 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).

recovery option

(*ITIL Service Design*) A strategy for responding to an interruption to service. Commonly used strategies are manual workaround, reciprocal arrangement, gradual recovery, intermediate recovery, fast recovery, and immediate recovery. Recovery options may make use of dedicated facilities or third-party facilities shared by multiple businesses.

recovery point objective (RPO)

(*ITIL Service Design*) (*ITIL Service Operation*) The maximum amount of data that may be lost when service is restored after an interruption. The 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.

recovery time objective (RTO)

(*ITIL Service Design*) (*ITIL Service Operation*) The maximum time allowed for the 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 also* business impact analysis.

redundancy

(*ITIL Service Design*) Use of one or more additional configuration items to provide fault tolerance. The term also has a generic meaning of obsolescence, or no longer needed.

relationship

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 service asset and 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, and IT services have many links to all the configuration items that contribute to that IT service.

relationship processes

The ISO/IEC 20000 process group that includes business relationship management and supplier management.

release

(*ITIL Service Transition*) One or more changes to an IT service that are built, tested and deployed together. A single release may include changes to hardware, software, documentation, processes and other components.

release and deployment management

(*ITIL Service Transition*) The process responsible for planning, scheduling and controlling the build, test and deployment of releases, and for delivering new functionality required by the business while protecting the integrity of existing services.

release record

(*ITIL Service Transition*) A record that defines the content of a release. A release record has relationships with all configuration items that are affected by the release. Release records may be in the configuration management system or elsewhere in the service knowledge management system.

reliability

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) A measure of how long an IT service or other configuration item can perform its agreed function without interruption. Usually measured as MTBF or MTBSI. The term can also be used to state how likely it is that a process, function etc. will deliver its required outputs. *See also* availability.

remediation

(*ITIL Service Transition*) Actions taken to recover after a failed change or release. Remediation may include back-out, invocation of service continuity plans, or other actions designed to enable the business process to continue.

repair

(*ITIL Service Operation*) The replacement or correction of a failed configuration item.

request for change (RFC)

(*ITIL Service Transition*) A formal proposal for a change to be made. It includes details of the proposed change, and may be recorded on paper or electronically. The term is often misused to mean a change record, or the change itself.

request fulfilment

(*ITIL Service Operation*) The process responsible for managing the lifecycle of all service requests.

requirement

(*ITIL Service Design*) A formal statement of what is needed – for example, a service level requirement, a project requirement or the required deliverables for a process. *See also* statement of requirements.

resilience

(*ITIL Service Design*) The ability of an IT service or other configuration item to resist failure or to recover in a timely manner following a failure. For example, an armoured cable will resist failure when put under stress. *See also* fault tolerance.

resolution

(*ITIL 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.

resolution processes

The ISO/IEC 20000 process group that includes incident and problem management.

resource

(*ITIL Service Strategy*) 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 also* 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.

responsiveness

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.

restoration of service

See restore.

restore

(*ITIL 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.

retire

(*ITIL Service Transition*) Permanent removal of an IT service, or other configuration item, from the live environment. Being retired is a stage in the lifecycle of many configuration items.

return on investment (ROI)

(*ITIL Continual Service Improvement*) (*ITIL Service Strategy*) 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 also* net present value; value on investment.

return to normal

(*ITIL Service Design*) The phase of an IT service continuity plan during which full normal operations are resumed. For example, if an alternative data centre has been in use, then this phase will bring the primary data centre back into operation, and restore the ability to invoke IT service continuity plans again.

review

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 also* change evaluation; post-implementation review.

rights

(*ITIL Service Operation*) 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 can also be defined as uncertainty of outcome, and can be used in the context of measuring the probability of positive outcomes as well as negative outcomes.

risk assessment

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.

risk management

The process responsible for identifying, assessing and controlling risks. Risk management is also sometimes used to refer to the second part of the overall process after risks have been identified and assessed, as in 'risk assessment and management'. This process is not described in detail within the core ITIL publications. *See also* risk assessment.

role

A set of responsibilities, activities and authorities assigned to a person or team. A role is defined in a process or function. 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. Role is also used to describe the purpose of something or what it is used for.

root cause

(*ITIL Service Operation*) The underlying or original cause of an incident or problem.

running costs

See operational costs.

scalability

The ability of an IT service, process, configuration item etc. to perform its agreed function when the workload or scope changes.

scope

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.

security

See information security management.

security management

See information security management.

security management information system (SMIS)

(*ITIL Service Design*) A set of tools, data and information that is used to support information security management. The security management information system is part of the information security management system. *See also* service knowledge management system.

security policy

See information security policy.

separation of concerns (SoC)

An approach to designing a solution or IT service that divides the problem into pieces that can be solved independently. This approach separates what is to be done from how it is to be done.

server

(*ITIL Service Operation*) A computer that is connected to a network and provides software functions that are used by other computers.

service

A means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. The term 'service' is sometimes used as a synonym for core service, IT service or service package. *See also* utility; warranty.

service acceptance criteria (SAC)

(*ITIL Service Transition*) 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 also* acceptance.

service asset

Any resource or capability of a service provider. *See also* asset.

service asset and configuration management (SACM)

(*ITIL Service Transition*) The process responsible for ensuring that the assets required to deliver services are properly controlled, and that accurate and reliable information about those assets is available when and where it is needed. This information includes details of how the assets have been configured and the relationships between assets. *See also* configuration management system.

service capacity management (SCM)

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) The sub-process of capacity management responsible for understanding the performance and capacity of IT services. Information on 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 also* business capacity management; component capacity management.

service catalogue

(*ITIL Service Design*) (*ITIL Service Strategy*) A database or structured document with information about all live IT services, including those available for deployment. The service catalogue is part of the service portfolio and contains information about two types of IT service: customer-facing services that are visible to the business; and supporting services required by the service provider to deliver customer-facing services. *See also* customer agreement portfolio; service catalogue management.

service catalogue management

(ITIL Service Design) The process responsible for providing and maintaining the service catalogue and for ensuring that it is available to those who are authorized to access it.

service change

See change.

service charter

(*ITIL Service Design*) (*ITIL Service Strategy*) A document that contains details of a new or changed service. New service introductions and significant service changes are documented in a charter and authorized by service portfolio management. Service charters are passed to the service design lifecycle stage where a new or modified service design package will be created. The term charter is also used to describe the act of authorizing the work required by each stage of the service lifecycle with respect to the new or changed service. *See also* change proposal; service portfolio; service catalogue.

service continuity management

See IT service continuity management.

service culture

A customer-oriented culture. The major objectives of a service culture are customer satisfaction and helping customers to achieve their business objectives.

service design

(*ITIL Service Design*) A stage in the lifecycle of a service. Service design includes the design of the services, governing practices, processes and policies required to realize the service provider's strategy and to facilitate the introduction of services into supported environments. Service design includes the following processes: design coordination, service catalogue management, service level management, availability management, capacity management, IT service continuity management, information security management, and supplier management. Although these processes are associated with service design, most processes have activities that take place across multiple stages of the service lifecycle. *See also* design.

service design package (SDP)

(*ITIL Service Design*) 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

(*ITIL 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.

service failure analysis (SFA)

(*ITIL Service Design*) A technique that identifies underlying causes of one or more IT service interruptions. Service failure analysis identifies opportunities to improve the IT service provider's processes and tools, and not just the IT infrastructure. It is a time-constrained, project-like activity, rather than an ongoing process of analysis.

service hours

(*ITIL Service Design*) An agreed time period when a particular IT service should be available. For example, 'Monday–Friday 08:00 to 17:00 except public holidays'. Service hours should be defined in a service level agreement.

service improvement plan (SIP)

(*ITIL Continual Service Improvement*) A formal plan to implement improvements to a process or IT service.

service knowledge management system (SKMS)

(*ITIL Service Transition*) A set of tools and databases that is used to manage knowledge, information and data. The service knowledge management system includes the configuration management system, as well as other databases and information systems. The service knowledge management system includes tools for collecting, storing, managing, updating, analysing and presenting all the knowledge, information and data that an IT service provider will need to manage the full lifecycle of IT services. *See also* knowledge management.

service level

Measured and reported achievement against one or more service level targets. The term is sometimes used informally to mean service level target.

service level agreement (SLA)

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) An agreement between an IT service provider and a customer. A service level agreement describes the IT service, documents service level targets, and specifies the responsibilities of the IT service provider and the customer. A single agreement may cover multiple IT services or multiple customers. *See also* operational level agreement.

service level management (SLM)

(*ITIL Service Design*) The process responsible for negotiating achievable service level agreements and ensuring that these are met. It is responsible for ensuring that all IT service management processes, operational level agreements and underpinning contracts are appropriate for the agreed service level targets. Service level management monitors and reports on service levels, holds regular service reviews with customers, and identifies required improvements.

service level package (SLP)

See service option.

service level requirement (SLR)

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) A customer requirement for an aspect of an IT service. Service level requirements are based on business objectives and used to negotiate agreed service level targets.

service level target

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) A commitment that is documented in a service level agreement. Service level targets are based on service level requirements, and are needed to ensure that the IT service is able to meet business objectives. They should be SMART, and are usually based on key performance indicators.

service 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 lifecycle approach considers the strategy, design, transition, operation and continual improvement of IT services. Also known as service management lifecycle.

service management

A set of specialized organizational capabilities for providing value to customers in the form of services.

service manager

A generic term for any manager within the service provider. Most commonly used to refer to a business relationship manager, a process manager or a senior manager with responsibility for IT services overall.

service model

(*ITIL Service Strategy*) A model that shows how service assets interact with customer assets to create value. Service models describe the structure of a service (how the configuration items fit together) and the dynamics of the service (activities, flow of resources and interactions). A service model can be used as a template or blueprint for multiple services.

service operation

(*ITIL Service Operation*) A stage in the lifecycle of a service. Service operation coordinates and carries out the activities and processes required to deliver and manage services at agreed levels to business users and customers. Service operation also manages the technology that is used to deliver and support services. Service operation includes the following processes: event management, incident management, request fulfilment, problem management, and access management. Service operation also includes the following functions: service desk, technical management, IT operations management, and application management. Although these processes and functions are associated with service operation, most processes and functions have activities that take place across multiple stages of the service lifecycle. *See also* operation.

service option

(*ITIL Service Design*) (*ITIL Service Strategy*) A choice of utility and warranty offered to customers by a core service or service package. Service options are sometimes referred to as service level packages.

service owner

(*ITIL Service Strategy*) A role responsible for managing one or more services throughout their entire lifecycle. Service owners are instrumental in the development of service strategy and are responsible for the content of the service portfolio. *See also* business relationship management.

service package

(*ITIL Service Strategy*) Two or more services that have been combined to offer a solution to a specific type of customer need or to underpin specific business outcomes. A service package can consist of a combination of core services, enabling services and enhancing services. A service package provides a specific level of utility and warranty. Customers may be offered a choice of utility and warranty through one or more service options. *See also* IT service.

service pipeline

(*ITIL Service Strategy*) 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 that is not normally published to customers.

service portfolio

(*ITIL Service Strategy*) The complete set of services that is 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 also* customer agreement portfolio; service portfolio management.

service portfolio management (SPM)

(*ITIL Service Strategy*) The process responsible for managing the service portfolio. Service portfolio management ensures that the service provider has the right mix of services to meet required business outcomes at an appropriate level of investment. Service portfolio management considers services in terms of the business value that they provide.

service provider

(*ITIL Service Strategy*) 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 also* Type I service provider; Type II service provider; Type III service provider.

service reporting

(*ITIL Continual Service Improvement*) Activities that produce and deliver reports of achievement and trends against service levels. The format, content and frequency of reports should be agreed with customers.

service request

(*ITIL Service Operation*) A formal request from a user for something to be provided – for example, a request for information or advice; to reset a password; or to install a workstation for a new user. Service requests are managed by the request fulfilment process, usually in conjunction with the service desk. Service requests may be linked to a request for change as part of fulfilling the request.

service sourcing

(*ITIL Service Strategy*) The strategy and approach for deciding whether to provide a service internally, to outsource it to an external service provider, or to combine the two approaches. Service sourcing also means the execution of this strategy. *See also* insourcing; internal service provider; outsourcing.

service strategy

(*ITIL Service Strategy*) A stage in the lifecycle of a service. Service strategy defines the perspective, position, plans and patterns that a service provider needs to execute to meet an organization's business outcomes. Service strategy includes the following processes: strategy management for IT services, service portfolio management, financial management for IT services, demand management, and business relationship management. Although these processes are associated with service strategy, most processes have activities that take place across multiple stages of the service lifecycle.

service transition

(*ITIL Service Transition*) A stage in the lifecycle of a service. Service transition ensures that new, modified or retired services meet the expectations of the business as documented in the service strategy and service design stages of the lifecycle. Service transition includes the following processes: transition planning and support, change management, service asset and configuration management, release and deployment management, service validation and testing, change evaluation, and knowledge management. Although these processes are associated with service transition, most processes have activities that take place across multiple stages of the service lifecycle. *See also* transition.

service validation and testing

(*ITIL Service Transition*) 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.

serviceability

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) The ability of a third-party supplier to meet the terms of its contract. This contract will include agreed levels of reliability, maintainability and availability for a configuration item.

seven-step improvement process

(*ITIL Continual Service Improvement*) The process responsible for defining and managing the steps needed to identify, define, gather, process, analyse, present and implement improvements. The performance of the IT service provider is continually measured by this process and improvements are made to processes, IT services and IT infrastructure in order to increase efficiency, effectiveness and cost effectiveness. Opportunities for improvement are recorded and managed in the CSI register.

shift

(*ITIL 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.

simulation modelling

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) A technique that creates a detailed model to predict the behaviour of an IT service or other configuration item. A simulation model is often created by using the actual configuration items that are being modelled with artificial workloads or transactions. They are used in capacity management when accurate results are important. A simulation model is sometimes called a performance benchmark. *See also* analytical modelling; modelling.

single point of contact

(*ITIL Service Operation*) 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.

single point of failure (SPOF)

(*ITIL Service Design*) Any configuration item that can cause an incident when it fails, and for which a countermeasure has not been implemented. A single point of failure may be a person or a step in a process or activity, as well as a component of the IT infrastructure. *See also* failure.

SLAM chart

(*ITIL Continual Service Improvement*) 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.

SMART

(*ITIL Continual Service Improvement*) (*ITIL Service Design*) An acronym for helping to remember that targets in service level agreements and project plans should be specific, measurable, achievable, relevant and time-bound.

software asset management (SAM)

(*ITIL Service Transition*) The process responsible for tracking and reporting the use and ownership of software assets throughout their lifecycle. Software asset management is part of an overall service asset and configuration management process. This process is not described in detail within the core ITIL publications.

source

See service sourcing.

specification

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 organization can be audited.

stakeholder

A person who has 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 also* 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 is also used to refer to a code of practice or specification published by a standards organization such as ISO or BSI. *See also* guideline.

standard change

(*ITIL Service Transition*) A pre-authorized change that is low risk, relatively common and follows a procedure or work instruction – for example, a password reset or provision of standard equipment to a new employee. Requests for change are not required to implement a standard change, and they are logged and tracked using a different mechanism, such as a service request. *See also* change model.

standard operating procedures (SOP)

(*ITIL Service Operation*) Procedures used by IT operations management.

standby

(*ITIL Service Design*) Used to refer to resources that are not required to deliver the live IT services, but are available to support IT service continuity plans. For example, a standby data centre may be maintained to support hot standby, warm standby or cold standby arrangements.

statement of requirements (SOR)

(*ITIL Service Design*) A document containing all requirements for a product purchase, or a new or changed IT service. *See also* terms of reference.

status accounting

(*ITIL Service Transition*) The activity responsible for recording and reporting the lifecycle of each configuration item.

strategic

(*ITIL Service Strategy*) 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.

strategic asset

(*ITIL Service Strategy*) Any asset that provides the basis for core competence, distinctive performance or sustainable competitive advantage, or which allows a business unit to participate in business opportunities. Part of service strategy is to identify how IT can be viewed as a strategic asset rather than an internal administrative function.

strategy

(*ITIL Service Strategy*) A strategic plan designed to achieve defined objectives.

strategy management for IT services

(*ITIL Service Strategy*) The process responsible for defining and maintaining an organization's perspective, position, plans and patterns with regard to its services and the management of those services. Once the strategy has been defined, strategy management for IT services is also responsible for ensuring that it achieves its intended business outcomes.

supplier

(*ITIL Service Design*) (*ITIL Service Strategy*) 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 also* supply chain; underpinning contract.

supplier and contract management information system (SCMIS)

(*ITIL Service Design*) A set of tools, data and information that is used to support supplier management. *See also* service knowledge management system.

supplier management

(*ITIL Service Design*) The process responsible for obtaining value for money from suppliers, ensuring that all contracts and agreements with suppliers support the needs of the business, and that all suppliers meet their contractual commitments. *See also* supplier and contract management information system.

supply chain

(*ITIL Service Strategy*) The activities in a value chain carried out by suppliers. A supply chain typically involves multiple suppliers, each adding value to the product or service. *See also* value network.

support group

(*ITIL 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 also* technical management.

support hours

(*ITIL Service Design*) (*ITIL Service Operation*) The times or hours when support is available to the users. Typically these are 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 07:00 to 19:00.

supporting service

(*ITIL Service Design*) An IT service that is not directly used by the business, but is required by the IT service provider to deliver customer-facing services (for example, a directory service or a backup service). Supporting services may also include IT services only used by the IT service provider. All live supporting services, including those available for deployment, are recorded in the service catalogue along with information about their relationships to customer-facing services and other CIs.

SWOT analysis

(*ITIL Continual Service Improvement*) A technique that reviews and analyses the internal strengths and weaknesses of an organization and the external opportunities and threats that it faces. SWOT stands for strengths, weaknesses, opportunities and threats.

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 the framework of policy, processes, functions, standards, guidelines and tools that are planned and managed together – for example, a quality management system
- A database management system or operating system that includes many software modules which are designed to perform a set of related functions.

system management

The part of IT service management that focuses on the management of IT infrastructure rather than process.

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

(*ITIL 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.

technical support

See technical management.

terms of reference (TOR)

(*ITIL Service Design*) A document specifying the requirements, scope, deliverables, resources and schedule for a project or activity.

test

(*ITIL Service Transition*) An activity that verifies that a configuration item, IT service, process etc. meets its specification or agreed requirements. *See also* acceptance; service validation and testing.

test environment

(*ITIL Service Transition*) A controlled environment used to test configuration items, releases, IT services, processes etc.

third party

A person, organization or other entity that is not part of the service provider's own organization and is not a customer – for example, a software supplier or a hardware maintenance company. Requirements for third parties are typically specified in contracts that underpin service level agreements. *See also* underpinning contract.

threat

A threat is anything that might exploit a vulnerability. Any potential cause of an incident can be considered 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 that should cause an alert to be generated or management action to be taken. For example, 'Priority 1 incident not solved within four hours', 'More than five soft disk errors in an hour', or 'More than 10 failed changes in a month'.

throughput

(*ITIL Service Design*) A measure of the number of transactions or other operations performed in a fixed time – for example, 5,000 e-mails sent per hour, or 200 disk I/Os per second.

total cost of ownership (TCO)

(*ITIL Service Strategy*) A methodology used to help make investment decisions. It assesses the full lifecycle cost of owning a configuration item, not just the initial cost or purchase price. *See also* total cost of utilization.

total cost of utilization (TCU)

(*ITIL Service Strategy*) A methodology used to help make investment and service sourcing decisions. Total cost of utilization assesses the full lifecycle cost to the customer of using an IT service. *See also* total cost of ownership.

total quality management (TQM)

(*ITIL Continual Service Improvement*) A methodology for managing continual improvement by using a quality management system. Total quality management establishes a culture involving all people in the organization in a process of continual monitoring and improvement.

transaction

A discrete function performed by an IT service – for example, transferring money from one bank account to another. A single transaction may involve numerous additions, deletions and modifications of data. Either all of these are completed successfully or none of them is carried out.

transition

(*ITIL Service Transition*) A change in state, corresponding to a movement of an IT service or other configuration item from one lifecycle status to the next.

transition planning and support

(*ITIL Service Transition*) The process responsible for planning all service transition processes and coordinating the resources that they require.

trend analysis

(*ITIL Continual Service Improvement*) 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 most commonly used in the context of IT services and components. Tuning is part of capacity management, which also includes performance monitoring and implementation of the required changes. Tuning is also called optimization, particularly in the context of processes and other non-technical resources.

Type I service provider

(*ITIL Service Strategy*) 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

(*ITIL Service Strategy*) An internal service provider that provides shared IT services to more than one business unit. Type II service providers are also known as shared service units.

Type III service provider

(*ITIL Service Strategy*) A service provider that provides IT services to external customers.

underpinning contract (UC)

(*ITIL Service Design*) 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 one or more service level agreements.

urgency

(*ITIL Service Design*) (*ITIL Service Transition*) 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.

usability

(*ITIL Service Design*) The ease with which an application, product or IT service can be used. Usability requirements are often included in a statement of requirements.

use case

(*ITIL Service Design*) A technique used to define required functionality and objectives, and to design tests. Use cases define realistic scenarios that describe interactions between users and an IT service or other system.

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)

(*ITIL Service Strategy*) A pattern of user demand for IT services. Each user profile includes one or more patterns of business activity.

utility

(*ITIL Service Strategy*) The functionality offered by a product or service to meet a particular need. Utility can be summarized as 'what the service does', and can be used to determine whether a service is able to meet its required outcomes, or is 'fit for purpose'. The business value of an IT service is created by the combination of utility and warranty. *See also* service validation and testing.

validation

(*ITIL Service Transition*) An activity that ensures a new or changed IT service, process, plan or other deliverable meets the needs of the business. Validation ensures that business requirements are met even though these may have changed since the original design. *See also* acceptance; qualification; service validation and testing; verification.

value chain

(*ITIL Service Strategy*) A sequence of processes that creates a product or service that is of value to a customer. Each step of the sequence builds on the previous steps and contributes to the overall product or service. *See also* value network.

value for money

An informal measure of cost effectiveness. Value for money is often based on a comparison with the cost of alternatives. *See also* cost benefit analysis.

value network

(*ITIL Service Strategy*) A complex set of relationships between two or more groups or organizations. Value is generated through exchange of knowledge, information, goods or services. *See also* partnership; value chain.

value on investment (VOI)

(*ITIL Continual Service Improvement*) A measurement of the expected benefit of an investment. Value on investment considers both financial and intangible benefits. *See also* return on investment.

variable cost

(*ITIL Service Strategy*) 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.

variance

The difference between a planned value and the actual measured value. Commonly used in financial management, capacity management and service level management, but could apply in any area where plans are in place.

verification

(*ITIL Service Transition*) An activity that ensures that a new or changed IT service, process, plan or other deliverable is complete, accurate, reliable and matches its design specification. *See also* acceptance; validation; service validation and testing.

version

(*ITIL Service Transition*) A version is used to identify a specific baseline of a configuration item. Versions typically use a naming convention that enables the sequence or date of each baseline to be identified. For example, payroll application version 3 contains updated functionality from version 2.

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. *See also* mission.

vital business function (VBF)

(*ITIL Service Design*) Part of a business process that is critical to the success of the business. Vital business functions are an important consideration of business continuity management, IT service continuity management and availability management.

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.

warm standby

See intermediate recovery.

warranty

(*ITIL Service Strategy*) Assurance that a product or service will meet agreed requirements. This may be a formal agreement such as a service level agreement or contract, or it may be a marketing message or brand image. Warranty refers to the ability of a service to be available when needed, to provide the required capacity, and to provide the required reliability in terms of continuity and security. Warranty can be summarized as 'how the service is delivered', and can be used to determine whether a service is 'fit for use'. The business value of an IT service is created by the combination of utility and warranty. *See also* service validation and testing.

work instruction

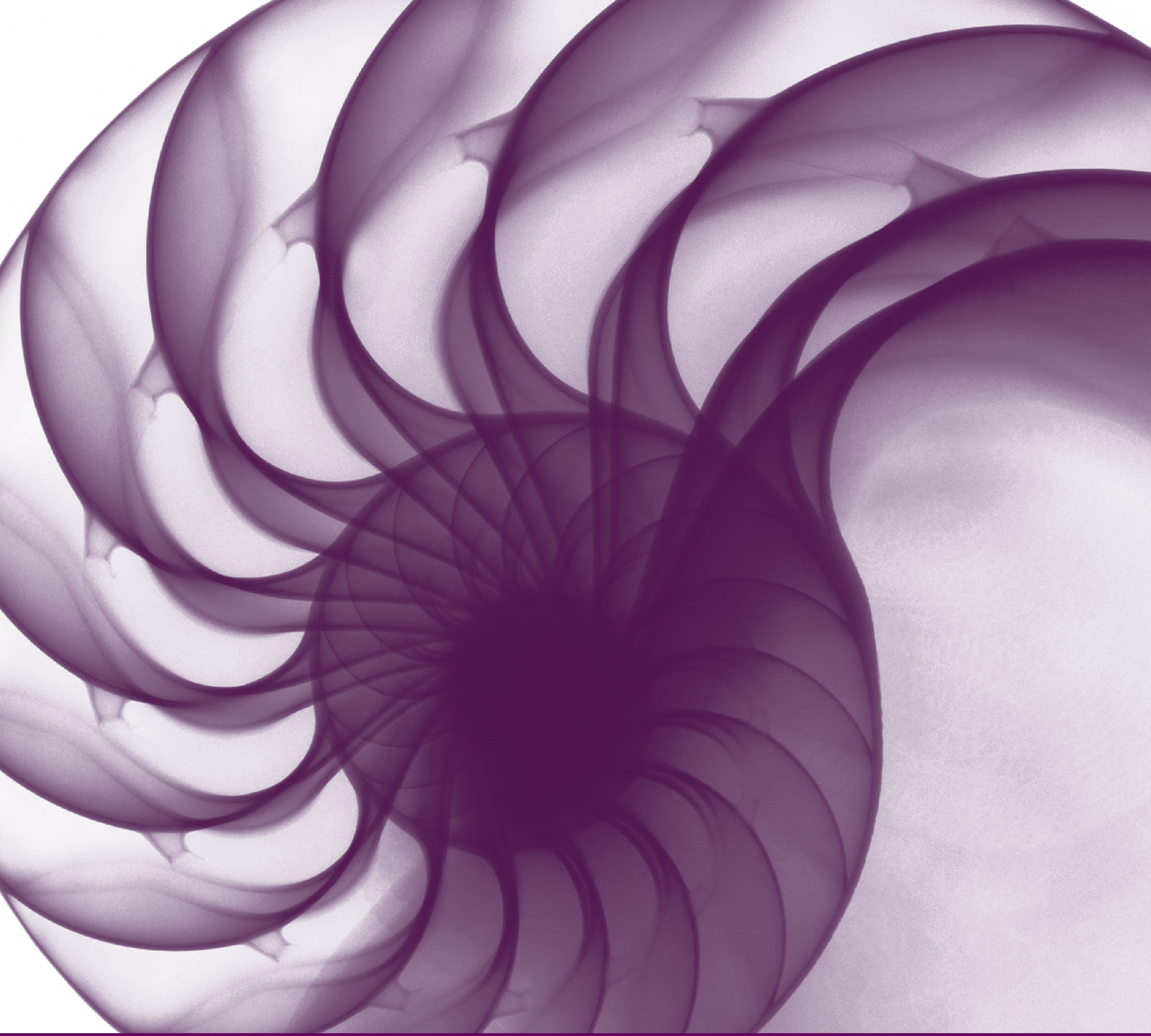
A document containing detailed instructions that specify exactly what steps to follow to carry out an activity. A work instruction contains much more detail than a procedure and is only created if very detailed instructions are needed.

workaround

(*ITIL 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.

workload

The resources required to deliver an identifiable part of an IT service. Workloads may be categorized by users, groups of users, or functions within the IT service. This is used to assist in analysing and managing the capacity, performance and utilization of configuration items and IT services. The term is sometimes used as a synonym for throughput.



Index

Index

Page numbers in *italic* refer to figures and tables.

- accelerated development 78–9, *80*
- acceptance criteria 305, 309–10
- access management
  - and availability management 155
  - and security management 204
- activity sampling 234
- agile software development 78–9, *80*
- alternative solutions, evaluation of 71
- application architecture 58
- application service provision *75, 77*
- application sizing in capacity management 173–4
- applications management
  - alternative approaches 244–5
  - application frameworks 245–6
  - and business requirements 244
  - CASE tools and repositories 246
  - coding conventions and generation 248–9
  - design of specific applications 246–7
  - diagnostic hooks 249–50
  - embedded instrumentation 249–50
  - functions within organizations 253–4
  - individual applications, development of 248–9
  - outputs
    - from design 247–8
    - from development phase 250
  - as part of service operation 23
  - patterns, design 248
  - portfolio 245, *245*
  - separation of concerns (SoC) 248
  - and service portfolio 245
  - templates 249
  - trade-offs, balancing 247
- architectural design
  - and application frameworks 246
  - defined 55–6
  - documents and standards 317
  - enterprise architecture *56*
  - IT designer/architect role 268–70
  - management architectures 60–3, *62*
  - roles in 59
  - service-oriented architecture (SOA)
- approach 73–4
  - and specific applications 246–7
  - technology architectures 60
- asset management
  - interface with service catalogue 104
  - resources and capabilities as assets 20, *21*
- authority model 64–8, *65, 67, 68,* 270
- availability management
  - activities, methods and techniques
    - business/user focus 133
    - component failure impact analysis 145–7, *146*
    - costs of failure 134–5
    - designing for availability 142–5
    - expanded incident lifecycle 135–8, *136*
    - fault tree analysis 148, *148*
    - high-availability design 143
    - proactive activities *131,* 131–2, 140–53
    - projected service outage document 153
    - reactive activities 130–1, 131, 132–40
    - redundancy 143
    - reviewing and testing 151–3
    - service failure analysis 138–40, 139
    - single point of failure analysis 147
    - unavailability analysis 134–5
    - vital business functions (VBF) 142
  - availability definition 134
  - availability plans 155–6
  - and capacity management 176
  - challenges 157
  - continual improvement 152–3
  - and continuity management 195
  - and costs 142–3
  - critical success factors 156–7
  - and design coordination process 95
  - guiding principles 127–8
  - information management 155–6
  - inputs and outputs 153–4
  - interfaces 154–5
  - key performance indicators 156–7
  - maintainability 128–9
  - maintenance strategies 150–1
  - measurement of availability 128–30, *130*
  - modelling/simulation 148–9
  - monitoring performance 128–30
  - policies 127
  - purpose and objectives 125
  - recovery, designing for 144, 145
  - reliability 128
  - requirements definition 141–2
  - risk assessment and management *149,* 149–53
  - risks 157
  - roles 262–3
  - scope 126–7

- availability management *continued*
  - and security management 205
  - service availability design 143–5
  - and service level management 121
  - serviceability 129
  - service/component levels 128
  - traditional measures 132
  - triggers 153
  - value to business 127
  - vital business functions (VBF) 129, 133–4

- balanced scorecard approach 70, 289, 376
- benefits assessments 220–1
- benefits to business of service design *see* value
- Best Management Practice portfolio 7–9, *8,* 371
- best practices in service management 18–20, *19*
- buildings, environment standards for 321
- business architects 59
- business capacity management 161, *164,* 164–5, 167
- business change process *36,* 36–7
- business focus in service management 38–9
- business impact analysis 183–5, *184,* 283
- business process outsourcing (BPO) *75, 77*
- business relationship management
  - and design coordination process 95
  - and service catalogue 104
  - and service level management 107, 121, 261
- business requirements
  - and applications management 244
  - identifying 47–8

- capabilities
  - as assets 20, *21*
  - coordination of 91
- Capability Maturity Model Integration (CMMI) 376
- capacity management
  - activities, methods and techniques
    - demand management *164,* 164–5
    - iterative activities 167–72, *168*
    - proactive activities 162–3
    - reactive activities 163
    - response time monitoring 170
    - threshold management and control 169–70
    - *see also* sub-processes
  - application sizing 173–4
  - and availability management 154
  - as balancing act 159
  - capacity plans 161
  - challenges 178–9
  - complexity planning and management 160–1
  - critical success factors 178
  - demand management in 172
  - and design coordination process 95
  - and human resource management 158
  - information management 176–8
  - inputs and outputs 184–5
  - interfaces 176
  - key performance indicators 178
  - modelling 172–3
  - overview *163*
  - plans 349–50
  - policies 159–60
  - purpose and objectives 158
  - risks 179
  - roles 263–4
  - scope 158–9
  - and security management 205
  - and service level management 121–2, 165
  - and service strategy 157, 159
  - sub-processes
    - business capacity management 161, *162, 164,* 164–5, 167
    - component capacity management 161, *162,* 166, 167
    - exploitation of new technology 167
    - resilience, designing 167
    - service capacity management 161, *162,* 165–6
    - summary 161–2, *162*
  - triggers 174
  - value to business 159
- capture of data 243
- CASE tools and repositories 246
- catalogue, requirements *237,* 237–8
- catalogue, service *see* service catalogue
- categorization of suppliers 215–16, *216*
- challenges
  - availability management 157
  - capacity management 178–9
  - continuity management 196
  - design coordination process 96
  - overcoming 293
  - security management 206
  - service catalogue 105–6
  - service level management 123–5
  - summary 293–4
  - supplier management 224–5
- change
  - business change process *36,* 36–7
  - evaluation and design coordination process 95
  - management
    - and availability management 155
    - and continuity management 192, 195
    - and design coordination process 94–5
    - and security management 204–5

and supplier management 224
organizational 375–6
cloud service 75, 77
competence of personnel 270–1
complaints and compliments, logging of 120
complexity
planning and management of 160–1
of services 14
component capacity management 161, 166, 167
component failure impact analysis 145–7, *146*
configuration management
and continuity management 195
and security management 205
and service catalogue 104
constraints on service design *72,* 72–3, *73*
contacts and relationships, development of in SLM 119–20
continual improvement
and availability management 152–3
and design coordination process 92–3
implementation of service design 284–8, *285, 286*
continual service improvement 7, *29,* 31, *31, 82,* 382
continuity management
activities, methods and techniques
business impact analysis 183–5, *184*
change management 192, 195
implementation stage 189–94
initiation stage 182–3
invocation 193–4
off-site storage 187
ongoing operation stage 192–3
policy setting 182
recovery options 187–9, *189*
requirements and strategy stage 183–9, *184, 186, 189*
risk assessment and management 185–9, *186, 189*
scope/terms of reference 182
and availability management 155
challenges 196
critical success factors 195–6
and design coordination process 95
importance of 179
information management 195
inputs and outputs 194
interfaces 194–5
key performance indicators 195–6
plans and procedures 189–92, 353–6
policies 181–2
purpose and objectives 179–80
risks 196
roles 264–5
scope 179–80
and security management 205
and service level management 121–2
and supplier management 224
triggers 194
value to business 180–1
contracts and agreements 108–9, 118–19, 210–11, 222
Control OBjectives for Information and related Technology (COBIT) 372–3
coordination in service lifecycle 28
see also design coordination process
core services 13
corporate governance 25, 372
co-sourcing *75, 77*
costs
and availability management 142–3
minimizing 61
critical success factors
availability management 156–7
capacity management 178
continuity management 195–6
defining and agreeing 294–5
design coordination process 96
security management 205–6
service catalogue 105
service level management 122–3
supplier management 224
CSI approach *88,* 89, 92
culture of the organization 23–4, 286
current capability and provision, review of 74
customer-based SLAs 110–11
customer-facing services 24, 99–100, *100,* 101–2, *102, 103*
customers
assets 20
internal/external 17
outcomes for as main concern for services 13
satisfaction of 13, 220–1
as stakeholders 17
value of a service for 17
customized vs standardized services 216–17

data architecture 58–9
data centres, environment standards for 322–3
data management and control
capture of data 243
classification of data 242–3
data as asset 240
ineffective, impact of 240
integrity of data 244
metadata 243
migration of data 243

data management and control *continued*
- ownership of data 243
- reference data 243
- retrieval and use of data 244
- role of 239–40
- scope 241
- and service lifecycle 241–2
- standards for data 243
- storage of data 244
- success factors 240
- value of data 242

delivery models/strategies
- options *75,* 75–6
- selection of 76–8, *77*

demand management
- and capacity management *164*, 164–5, 172, 176
- and service catalogue 104

departments 22

deployment management and design coordination process 95

design, service *see* service design

design coordination process
- activities, methods and techniques 89–93, *90*
- balance 89
- challenges 96
- continual improvement 92–3
- coordination of individual designs 93
- critical success factors 96
- CSI approach *88,* 89, 92
- information management 96
- inputs and outputs 94
- interfaces 94–5, 122
- key performance indicators 96
- monitoring of individual designs 93
- oversight of all activities 91–2
- policies 87–8, 90–1
- prioritization 89
- project management, integration with 89
- purpose and objectives 86
- resources and capabilities 91
- review of designs 93–4
- risk management 92
- risks 96–7
- roles 259–60
- scope 86–7
- SDP handover 93–4
- service design plans 96
- triggers for 94
- value to business 87

development of preferred solution 71–2

divisions 22

documents
- design 317
- IT plans 317–18
- procurement 359
- requirements engineering 236–9, *237*
- template for processes 313

downtime, planned 150–1

dynamic systems development method (DSDM) 78–9

enabling services 14

enhancing services 14

enterprise architecture *56,* 56–60, *57, 58*

environmental architectures and standards 47, 59, 321–4

environmental management 373–4

equipment rooms, environment standards for 321–4

expanded incident lifecycle 135–8, *136*

explicit/tacit knowledge 235–6, *236*

external customers 17

external influences on service design *72,* 72–3, *73*

Extreme Programming (XP) 79

failure of service
- component failure impact analysis 145–7, *146*
- fault tree analysis 148, *148*
- service capacity management 166
- service failure analysis 138–40, *139*
- single point of failure analysis 147
- *see also* recovery

fault tree analysis 148, *148*

feedback, continual, during service lifecycle *31*, 32

financial management
- and design coordination process 95
- and security management 205
- and service level management 122
- and supplier management 224

frameworks and standards
- benefits of 18–20, *19*
- *see also* ISO/IEC standards; standards

functional requirements 229

functions in organizations 22–3, 253–6, *256*

goals and objectives of service design 44

governance, organizational 25, 372

green IT 373–4

groups 22

human resource management
- and capacity management 158
- competence of personnel 270–1

and security management 205
training of personnel 271

impact analysis 183–5, *184,* 283
implementation of service design
business impact analysis 283
improvement process 284–8, *285, 286*
initial stages 284
measurement of service design 288–9
risks during 284
service level requirements 283
success factors 289
vision 286
improvement, continual
and availability management 152–3
and design coordination process 92–3
implementation of service design 284–8, *285, 286*
see also continual service improvement
incident management
and availability management 154
and capacity management 176
and continuity management 195
expanded incident lifecycle 135–8, *136*
and security management 205
and service level management 121
incremental development 78–9
information architecture 58–9
information management
availability management 155–6
capacity management 176–8
continuity management 195
design coordination process 96
security management 205
service catalogue 104–5
service level management 122
supplier management 224
see also data management and control
infrastructure 47
infrastructure architecture, IT 59
inputs and outputs
availability management 153–4
capacity management 184–5
continuity management 194
design coordination process 94
examples across service lifecycle 381–2
security management 204
service catalogue 104
service design *30,* 35, 49, *81–2,* 82
service level management 120–1
supplier management 223
insourcing *75, 77*

integration
design coordination role 91–2
of risk assessment and management 40
of service design across business 39–42, *40, 41*
integrity of data 244
interdependencies of services 45–6, *46*
interfaces
asset management with service catalogue 104
availability management 154–5
capacity management 176
continuity management 194–5
design coordination process 94–5
legal issues with security management 205
release management with design coordination process 95
security management 204–5
service catalogue 104
service level management 121–2
service portfolio 94, 104, 121, 224
strategy management with design coordination process 95
supplier management 224
testing with design coordination process 95
transition planning and support with design coordination process 95
internal customers 17
interviews 231–2
investigation techniques
activity sampling 234
interviews 231–2
observation 233
protocol analysis 233
prototyping 233–4
questionnaires 234
scenario analysis 233
shadowing 233
special purpose records 234
workshops *232,* 232–3
invitations to tender (ITTs) 345
ISO/IEC standards
ISO 9000:2005 371
ISO 9001:2008 371
ISO 9004 372
ISO 9241 374
ISO 14001 374
ISO 31000 364–5, *365*
ISO/IEC 12207 374
ISO/IEC 15288 374
ISO/IEC 15504 374
ISO/IEC 19770 374
ISO/IEC 20000 27–8, 373
ISO/IEC 25000 374

ISO/IEC standards *continued*
ISO/IEC 27001 365–6, 374
ISO/IEC 38500 372
ISO/IEC 42010 374
ISO/IEC JTC1 374
SC7 374
IT designer/architect role 268–70
IT infrastructure architects 59
IT infrastructure architecture 59
IT planner role 267–8
IT plans 317–18
IT service continuity management *see* continuity management
IT service management, basis of 16
iteration in development process 78–9
ITIL 371
background 3
Best Management Practice portfolio 7–9, *8*
framework 3
publications in lifecycle series 5–7
success factors 9

key performance indicators
availability management 156–7
capacity management 178
continuity management 195–6
defining and agreeing 294–5
design coordination process 96
security management 205–6
service catalogue 105
service level management 122–3
supplier management 224
knowledge
proprietary, disadvantages of 19
tacit/explicit 235–6, *236*
knowledge management systems
integration across lifecycle stages 30
as part of service management 24–5, *26*
knowledge process outsourcing (KPO) *75, 77*

legal issues, interface with security management 205
lifecycle, service *50*
actions needed from outset 40–2
and data management and control 241–2
feedback, continual *31,* 32
inputs and outputs *81–2,* 82, 381–2
integration of stages 30–2, *31*
processes in 28–30, *29, 30*
publications in series 5–7
within service design package 304–5
specialization and coordination in 28
structure, need for 28
summary *3*

maintenance strategies and availability management 150–1
management and operational requirements 229, 230–1
management architectures 38, 60–3, *62*
management information systems and tools 38, 52–5
Management of Portfolios (MoP) 7
Management of Risk (M_o_R) 7–8, 185, 363–4, *364*
Management of Value (MoV) 8
management systems 25–8, *26, 27*
Managing Successful Programmes (MSP) 8
Managing Successful Projects with PRINCE2 8
McCarthy, Jim 44
measurement
availability management 128–30, *130,* 132–40
implementation of service design 288–9
for processes 63–4, 69–71, *70*
review of methods 38
rework/improvement activities 43–4
service level agreements (SLAs) 114–16
traditional 132
see also critical success factors
mergers and acquisitions of suppliers 76
metadata 243
metrics tree 70, *70*
see also measurement
migration of data 243
mirroring 143
modelling 148–9, 172–3
monitoring
availability management 128–30, 132–40
capacity management 167–72, *168*
customer satisfaction 117–18
of individual designs 93
reviews of services 116–17
service level agreements (SLAs) 114–16
service reports 116–17
threshold management and control 169–70
multi-level SLAs 111
multi-sourcing *75, 77*
multi-vendor sourcing *75, 77*

Object Management Group (OMG) 248
objectives of service design 44
observation 233
office environments 324
off-the-shelf solutions 79–80, 82

- Open Systems Interconnection (OSI) framework 374–5
- operational level agreements (OLAs)
  - agreement of 113
  - defined 108
  - sample 330–2
- operational requirements 229, 230–1
- operations management 23
- optimization of design performance 43–4
- Organization for the Advancement of Structured Information Standards (OASIS) 73–4
- organizational architects 59
- organizations
  - application development 253–4
  - change in 375–6
  - competence and training 270–1
  - culture of the organization 23–4, 286
  - functions 253–6, *256*
  - large organizations 255–6, *256*
  - organizational development 253
  - project management 254
  - RACI model 270
  - readiness assessment 303
  - roles 23
    - availability management 262–3
    - capacity management 263–4
    - categories of 256–7
    - continuity management 264–5
    - design coordination 259–60
    - general definition of 256
    - IT designer/architect 268–70
    - IT planner 267–8
    - process manager 258
    - process owner 258
    - process practitioner 258
    - security management 265–6
    - service catalogue 260
    - service level management 260–1
    - service owner 257–8
    - supplier management 266–7
  - small organizations 254–5, *255*
  - structure of the organization 22–3, 191, 254–6, *255, 256*
- outputs of service design *see* inputs and outputs
- outsourcing *75, 77,* 239
- ownership
  - data 243
  - process 258, 262, 263, 264, 265, 266
  - service 257–8, 261

- partnering relationship with suppliers 213–15
- partnerships *75, 77*
- patterns, design 248
- performance management
  - availability management 128–30, 132–40
  - customer satisfaction 117–18
  - performance indicators
  - availability management 156–7
  - capacity management 178
  - continuity management 195–6
    - defining and agreeing 294–5
    - design coordination process 96
    - security management 205–6
    - service catalogue 105
    - service level management 122–3
    - supplier management 224
  - reviews of services 116–17
  - service level agreements (SLAs) 114–16
  - service reports 116–17
  - supplier management 219–22
- pipeline, service 24, 54
- Plan-Do-Check-Act (PDCA) cycle 27, *27,* 371–2
- planned downtime 150–1
- plans
  - availability 155–6
  - capacity 161, 349–50
  - IT 317–18
  - IT planner role 267–8
  - recovery 189–92, 353–6
  - service design 49–51, 93–4, 96
  - testing 191–2
- policies
  - availability management 127
  - capacity management 159–60
  - continuity management 181–2
  - design coordination process 87–8, 90–1
  - service catalogue 98–9
  - service level management 108
  - supplier management 209–10
- portfolio
  - application 245, *245*
  - service 24, *25,* 52–5, 94, 224, 245
- *Portfolio, Programme and Project Offices* (P3O) 8–9
- process maturity framework (PMF) 339–41
- processes
  - availability management 125–57, *130, 131, 136, 139, 142, 146, 148, 149,* 262–3
  - Capability Maturity Model Integration (CMMI) 376
  - capacity management 157–79, *162, 163, 164, 168,* 263–4
  - characteristics of 20–1
  - continuity management 179–96, *181, 184, 186, 189,* 264–5

processes *continued*
- control and measurement of 22, 63–4, 69–71, 70 *see also* measurement
- defined 63
- design coordination 86–97, *88, 90,* 259–60
- design of 63–8, *65, 67, 68*
- documentation template 313
- formal approach to design 64
- framework for 313
- inputs/outputs of 21
- ownership of 258
- practitioner role 258
- process manager role 258
- process maturity framework (PMF) 339–41
- review of 38
- review of current capability and provision *85,* 85–6
- roles, designing 64–8, *65, 67, 68*
- security management 196–207, *199, 202, 203,* 265–6
- service catalogue management 97–106, *100, 102, 103,* 260
- service level management 106–25, *110, 111,* 260
- in service lifecycle 28–30, *29, 30*
- supplier management 207–25, *209, 214, 216,* 266–7

procurement
- documents 359
- involvement of 41
- of preferred solution 71

programme management 375
project management 89, 254, 375
projected service outage document 153
proprietary knowledge, disadvantages of 19
protocol analysis 233
prototyping 233–4
providers of services 16–17

quality management systems 371–2
questionnaires 234

RACI model 64–8, *65, 67, 68,* 270
rapid application development (RAD) 78–9, *80*
readiness assessment 74
recovery
- continuity management 187–9, *189*
- designing for 144, 145
- organizational planning 191
- organizational structure during 191
- plans 189–92, 353–6
- *see also* failure of service

redundancy 143
reference data 243
release management and with design coordination process 95
reports, service 116
requirements
- actor definition 235
- business requirements, identifying 47–8
- definition of
  - availability management 141–2
  - supplier management 213
- service, identifying 45–6, *46*
- within service design package 303
- tacit/explicit knowledge 235–6, *236*
- of tools 277–8

requirements engineering
- catalogue, requirements *237,* 237–8
- defined 229
- documentation 236–9, *237*
- functional requirements 229, 230
- guidelines on 229
- investigation techniques
  - activity sampling 234
  - interviews 231–2
  - observation 233
  - protocol analysis 233
  - prototyping 233–4
  - questionnaires 234
  - scenario analysis 233
  - shadowing 233
  - special purpose records 234
  - workshops *232,* 232–3
- management and operational requirements 229, 230–1
- outsourcing 239
- problems with 234–6, *236*
- usability requirements 229, 231
- user view 231

resilience, designing 167
resources
- as assets 20, *21*
- coordination of 91

response time monitoring 170
results, focus on 49, *50*
retirement of services 24, 36, 47, 55
retrieval and use of data 244
reviews
- availability management 151–3
- current capability and provision 74, 85–6
- operational level agreements (OLAs) 118–19
- processes 38
- service level agreements (SLAs) 118
- supplier management 219–20

risk assessment and management
  availability management *149,* 149–53
  continuity management 185–9, *186*, *189*
  definition 363
  design coordination process 92
  implementation of service design 284
  initial 41
  integration of 40
  ISO 31000 364–5, *365*
  ISO/IEC 27001 365–6
  Management of Risk (M_o_R) 363–4, *364*
  methodologies 372
  purpose of 363
  Risk IT 366–7, *367*
  security management 198–9
  supplier management 218–19
Risk IT 366–7, *367*
risks
  availability management 157
  capacity management 179
  continuity management 196
  design coordination process 96–7
  security management 206–7
  service catalogue 106
  service level management 125
  summary 294
  supplier management 225
roles 23
  architectural 59
  availability management 262–3
  capacity management 263–4
  categories of 256–7
  continuity management 264–5
  design coordination process 259–60
  general definition of 256
  IT designer/architect 268–70
  IT planner 267–8
  process manager 258–9
  process owner 258
  process practitioner 259
  and processes 64–8, *67, 68*
  RACI model 64–8, *65, 67, 68*
  security management 265–6
  service catalogue 260
  service level management 260–1
  service owner 257–8
  supplier management 266–7

satisfaction, customer 117–18, 220–1
scale of activity 36
scenario analysis 233
security management
  activities, methods and techniques 201–3, *202, 203*
  and availability management 155
  challenges 206
  and continuity management 195
  critical success factors 205–6
  and design coordination process 95
  governance of 200–1
  importance of 196–7
  information management 205
  inputs and outputs 204
  interfaces 204–5
  key performance indicators 205–6
  policies 198
  purpose and objectives 197
  risk assessment and management 198–9
  risks 206–7
  roles 265–6
  scope 197–8
  and service level management 121–2
  and supplier management 224
  system for 199–200
  triggers 203–4
  value to business 198
separation of concerns (SoC) 79, 248
service acceptance criteria 305, 309–10
service architects 59
service architecture 58
service capacity management 161, 165–6
service catalogue
  activities, methods and techniques 103
  challenges 105–6
  critical success factors 105
  defined 24, 98
  defining and naming services 99
  different views of 101–3, *102, 103*
  information management 104–5
  inputs and outputs 104
  integration with service portfolio 105
  interfaces 104
  key performance indicators 105
  as part of service portfolio 54–5
  policies 98–9
  purpose and objectives 97
  risks 106
  roles 260
  sample 335
  scope 97
  and service level management 104, 121
  structure of 101, 335
  triggers 103–4
  types of service 99–100, *100*

service catalogue *continued*
uses of 100–1
value to business 98
service design
approaches to 78–82, *80, 81–2*
areas to be considered in 51–2
balance of three elements 44–5
and business change process *36,* 36–7
business requirements, identifying 47–8
constraints on *72,* 72–3, *73*
development phase 71–2
documents for 317
evaluation of alternative solutions 71
external influences on *72,* 72–3, *73*
five aspects of 36, *37,* 37–8
architectural design 55–63, *57, 58, 62*
management information systems and tools 52–5
measurement 69–71, *70*
new/changed services 51–2
processes, design of 63–8, *65, 67, 68*
formal, structured approach *50,* 51
goals and objectives of 44
holistic, result-driven approach 36, 45, 48
identifying service requirements 45–6, *46*
implementation of 283–9
importance of 39–40
inputs and outputs *30,* 35, 49, *81–2,* 82, 381
integration
across business 39–42, *40, 41*
with other stages 30, *31*
interdependencies of services 45–6, *46*
models 74–82, *75, 77, 80, 81–2*
needs for 35
optimization of performance 43–4
and other publications in series 5–7
package 303–5
plans for 49–51, 93–4, 96
processes in *29*
procurement of preferred solution 71
purpose and objective 4
results focus 49, *50*
retirement of services 36
scale of activity 36
scope and flow of 4, 37–8
service-oriented architecture (SOA) approach 73–4
as stage in lifecycle 6
target audience 5
technology domains 46–7
use of 4
value to business 4–5, 38–9
see also processes
service desks 22, 41, 115
service failure analysis 138–40, *139*
service improvement, continual *see* continual service improvement
service level management
activities, methods and techniques 109–20, *110*
and availability management 154
and business relationship management 107
and capacity management 165, 176
challenges 123–5
complaints and compliments 120
contacts and relationship, development of 119–20
and continuity management 195
contracts and agreements 108–9, 118–19
critical success factors 122–3
customer satisfaction 117–18
defined 107–8
and design coordination process 95
importance of 106
information management 122
inputs and outputs 120–1
interfaces 121–2
key performance indicators 122–3
operational level agreements (OLAs)
agreement of 113
defined 108
reviewing and revising 118–19
sample 330–2
policies 108
purpose and objectives 106
reviews of services 116–17
risks 125
roles 260–1
scope 106–7
and security management 204
service level agreements (SLAs)
and capacity management 165
customer-based 110–11
defined 16, 108
development and finalization of 113–14
in different languages 111
distinguished from underpinning contracts 109
framework design 109–12
monitoring performance against 114–16
multi-level 111
reviewing and revising 118
sample 327–30
service-based 110
templates for 111
wording of 111
service level requirements (SLRs) 112–13, 283
service reports 116

  and with supplier management 224
  triggers 120
  value to business 107
service lifecycle *50*
  actions needed from outset 40–2
  and data management and control 241–2
  feedback, continual *31,* 32
  inputs and outputs *81–2,* 82, 381–2
  integration of stages 30–2, *31*
  processes in 28–30, *29, 30*
  within service design package 304–5
  specialization and coordination in 28
  structure, need for 28
  summary 3, *3*
service management
  assets, resources and capabilities as 20, *21*
  basis of 15–16
  best practices 18–20, *19*
  business focus in 38–9
  governance, organizational 25
  ISO/IEC 20000 27–8, 373
  IT service management 16
  knowledge management system 24–5, *27*
  management systems 25–8, *26, 27*
  organization of 22–4
  process maturity framework (PMF) 339–41
  processes 20–2
  providers of services 16–17
  service portfolio 24, *25*
  services 13–14
  stakeholders 17
  utility 17–18, *18*
  warranty 18, *18*
service operation 7, *29,* 30–1, *31,* 37, 305, 382
service pipeline 24, 54
service portfolio
  and applications management 245
  contents of *25*
  defined 24
  and design coordination process 94
  designing 52–5
  and service catalogue 104
  and supplier management 224
service reports 116
service status 53–4
service strategy 6, 13, *29,* 30, *31, 81,* 157, 159, 381
service transition 6–7, *29,* 30–1, *31,* 37, *81,* 304–5, 382
service-based SLAs 110
service-oriented architecture (SOA) approach 73–4
services
  complexity of 14
  core 13
  customer outcomes as main concern 13
  customer-facing/support 24
  defining 13
  enabling 14
  enhancing 14
  packages 14
  providers of 16–17
  types of 99–100, *100*
  value of 17
shadowing 233
simulation 148–9, 173
single point of failure analysis 147
sites, environment standards for 321
Six Sigma 289, 377
Skills Framework for the Information Age (SFIA) 376
skills of personnel 61, 270–1
sourcing structures *75,* 75–6, *77*
special purpose records 234
specialization and coordination in service lifecycle 28
specification for processes 313
stakeholders 17
standardized vs customized services 216–17
standards
  and application frameworks 245–6
  benefits of 18–20, *19*
  for data 243
  see also ISO/IEC standards
statement of requirements (SoR): 345
status of services 53–4
steering groups 42–3, *43*
storage of data 244
strategic management
  balanced scorecard approach 376
  interface with design coordination process 95
  strategy groups 42–3, *43*
structure, organizational 22–3, 191, 254–6, *255, 256*
success of ITIL 9
supplier management
  activities, methods and techniques
    balanced, managed relationships 221–2
    categorization of suppliers 215–16, *216*
    contracts and agreements 217
    evaluation of new suppliers 213
    information system for 218
    new suppliers and contracts 218–19
    partnering relationship 213–15
    performance management 219–22
    renewal/termination of contracts 222
    requirements definition 213
    risk assessment and management 218–19

supplier management *continued*
    standardized vs customized services 216–17
    summary 212–13
    supplier relationships 217–18
  challenges 224–5
  contracts and agreements 210–11, 217, 222
  critical success factors 224
  and design coordination process 95
  importance of 207
  information management 224
  information system for 212
  inputs and outputs 223
  interfaces 224
  involvement of 41
  key performance indicators 224
  mergers and acquisitions of suppliers 76
  policies 209–10
  process for *214*
  procurement of preferred solution 71
  purpose and objectives 207–8
  risks 225
  roles 266–7
  scope 208, *209*
  and security management 205
  and service level management 121
  stakeholders, suppliers as 17
  strategy for 209
  triggers 222–3
  value to business 208–9
support services 24, 99–100, *100,* 101–2, *102, 103*
sustainable IT 373–4
system context diagrams 230
systems approach to service management 25–8, *26, 27*

tacit/explicit knowledge 235–6, *236*
target audience 5
teams 22
technical management 22
technology
  architectures 38
  domains of to be addressed 46–7
  exploitation of by capacity management 167
  management 60–3, *62*
  see also applications management; data management and control; requirements engineering
templates 249
testing
  continuity plans 192
  interface with design coordination process 95
  recovery plans 191–2
threshold management and control 169–70
tools for service design
  benefits of using 275–7
  evaluation *279,* 279–80
  implementation 279
  requirements definition 277–8
  selection of 275, 278–9
Total Quality Management (TQM) 371
training of personnel 271, 278
transaction response times 115
transition planning and support and design coordination process 95
trend analysis and capacity management 173
triggers
  availability management 153
  continuity management 194
  design coordination process 94
  security management 203–4
  service catalogue 103–4
  service level management 120
  supplier management 222–3

unavailability analysis 134–5
underpinning contracts 108–9, 118–19, 210–11
usability requirements 229, 231
use case models 230
users as stakeholders 17
utility aspect of services 17–18, *18*

validation and testing and design coordination process 95
value
  to business
    availability management 127
    capacity management 159
    continuity management 180–1
    of design coordination process 87
    security management 198
    service catalogue 98
    of service design 4–5, 38–9
    service level management 107
  of data 242
  of a service 17
values, organizational 23
vision 286
vital business functions (VBF) 129, 133–4, 142

warranty aspect of services 18, *18*
workshops *232,* 232–3

Well-designed services play a vital role in realizing a sound service strategy. Effective design contributes towards the provision of quality services that deliver the results the customer requires, within real business constraints such as time and money.

ITIL Service Design provides a framework for service design that considers customer requirements, both now and in the future, creating valuable IT service assets for the organization while keeping the business view firmly in sight.

Endorsed by
itSMF
IT Service Management Forum

ISBN 978-0-11-331305-1
9 780113 313051

HM Government