



Service Design



Published by TSO (The Stationery Office) and available from:

Online
www.tsoshop.co.uk

Mail, Telephone, Fax & E-mail

TSO

PO Box 29, Norwich, NR3 1GN
Telephone orders/General enquiries: 0870 600 5522
Fax orders: 0870 600 5533
E-mail: customerservices@tso.co.uk
Textphone 0870 240 3701

TSO Shops

123 Kingsway, London, WC2B 6PQ
020 7242 6393 Fax 020 7242 6394
16 Arthur Street, Belfast BT1 4GD
028 9023 8451 Fax 028 9023 5401
71 Lothian Road, Edinburgh EH3 9AZ
0870 606 5566 Fax 0870 606 5588

TSO@Blackwell and other Accredited Agents

Published for the Office of Government Commerce under licence from the Controller of Her Majesty's Stationery Office.

© Crown Copyright 2007

This is a Crown copyright value added product, reuse of which requires a Click-Use Licence for value added material issued by OPSI.

Applications to reuse, reproduce or republish material in this publication should be sent to OPSI,
Information Policy Team, St Clements House, 2-16 Colegate, Norwich, NR3 1BQ,

Tel No (01603) 621000 Fax No (01603) 723000, E-mail: hmsolicensing@cabinet-office.x.gsi.gov.uk , or
complete the application form on the OPSI website <http://www.opsi.gov.uk/click-use/value-added-licence-information/index.htm>

OPSI, in consultation with Office of Government Commerce (OGC), may then prepare a Value Added Licence based on standard terms tailored to your particular requirements including payment terms

The OGC logo ® is a Registered Trade Mark of the Office of Government Commerce

ITIL ® is a Registered Trade Mark, and a Registered Community Trade Mark of the Office of Government Commerce, and is Registered in the U.S. Patent and Trademark Office

The Swirl logo ™ is a Trade Mark of the Office of Government Commerce

First published 2007

ISBN 978 0 11 331047 0

Printed in the United Kingdom for The Stationery Office

Contents

List of figures	v	4 Service Design processes	57
List of tables	vii	4.1 Service Catalogue Management	60
OGC's foreword	viii	4.2 Service Level Management	65
Chief Architect's foreword	ix	4.3 Capacity Management	79
Preface	x	4.4 Availability Management	97
Acknowledgements	xi	4.5 IT Service Continuity Management	125
		4.6 Information Security Management	141
		4.7 Supplier Management	149
1 Introduction	1	5 Service Design technology-related activities	165
1.1 Overview	4	5.1 Requirements engineering	167
1.2 Context	4	5.2 Data and Information Management	176
1.3 Purpose	8	5.3 Application Management	180
1.4 Usage	8		
2 Service Management as a practice	9	6 Organizing for Service Design	187
2.1 What is Service Management?	11	6.1 Functional roles analysis	189
2.2 What are services?	11	6.2 Activity analysis	190
2.3 Functions and processes across lifecycle	12	6.3 Skills and attributes	190
2.4 Service Design fundamentals	13	6.4 Roles and responsibilities	190
3 Service Design principles	21	7 Technology considerations	199
3.1 Goals	25	7.1 Service Design tools	201
3.2 Balanced design	25	7.2 Service Management tools	203
3.3 Identifying service requirements	27		
3.4 Identifying and documenting business requirements and drivers	28	8 Implementing Service Design	207
3.5 Design activities	29	8.1 Business Impact Analysis	209
3.6 Design aspects	30	8.2 Service Level Requirements	209
3.7 The subsequent design activities	46	8.3 Risks to the services and processes	209
3.8 Design constraints	47	8.4 Implementing Service Design	210
3.9 Service Oriented Architecture	48	8.5 Measurement of Service Design	213
3.10 Business Service Management	49		
3.11 Service Design models	50	9 Challenges, Critical Success Factors and risks	217
		9.1 Challenges	219
		9.2 Risks	219

Afterword	221
Appendix A: The Service Design Package	225
Appendix B: Service Acceptance Criteria (example)	231
Appendix C: Process documentation templates (example)	235
C1 Process framework	237
Appendix D: Design and planning documents and their contents	239
D1 Design and architectural documents and standards	241
D2 IT plans	241
Appendix E: Environmental architectures and standards	243
Appendix F: Sample SLA and OLA	249
Appendix G: Example Service Catalogue	257
Appendix H: The Service Management process maturity Framework	261
Appendix I: Example contents of a Statement of Requirement (SoR) and/or Invitation to Tender (ITT)	267
Appendix J: The typical contents of a Capacity Plan	271
Appendix K: The typical contents of a recovery plan	275
Further information	281
References	283
Glossary	285
Acronyms list	287
Definitions list	289
Index	317

List of figures

All diagrams in this publication are intended to provide an illustration of ITIL Service Management Practice concepts and guidance. They have been artistically rendered to visually reinforce key concepts and are not intended to meet a formal method or standard of technical drawing. The ITIL Service Management Practices Integrated Service Model conforms to technical drawing standards and should be referred to for complete details. Please see www.best-management-practice.com/itil for details.

Figure 1.1	Resources and capabilities are the basis for value creation	Figure 3.12	The Metrics Tree
Figure 1.2	Sourcing of Service Management practice	Figure 3.13	Design constraints driven by strategy
Figure 1.3	ITIL Core	Figure 3.14	External influences on solution design
Figure 2.1	A conversation about the definition and meaning of services	Figure 3.15	The IT management continuum
Figure 2.2	A basic process	Figure 4.1	The key links, inputs and outputs of Service Design
Figure 2.3	Scope of Service Design	Figure 4.2	Service Design – the big picture
Figure 2.4	The Four Ps	Figure 4.3	The Business Service Catalogue and the Technical Service Catalogue
Figure 2.5	The IT Steering/Strategy Group	Figure 4.4	Example Service Catalogue
Figure 3.1	The business change process	Figure 4.5	Service Level Management
Figure 3.2	Service composition	Figure 4.6	The Service Level Management process
Figure 3.3	Project elements in a triangulated relationship	Figure 4.7	Multi-level SLAs
Figure 3.4	The service relationships and dependencies	Figure 4.8	The Capacity Management process
Figure 3.5	Aligning new services to business requirements	Figure 4.9	Capacity Management sub-processes
Figure 3.6	The Service Portfolio – a central repository	Figure 4.10	Capacity must support business requirements
Figure 3.7	The Service Portfolio and its contents	Figure 4.11	Capacity Management takes particular note of demand pattern
Figure 3.8	Enterprise Architecture	Figure 4.12	Iterative ongoing activities of Capacity Management
Figure 3.9	Architectural relationships	Figure 4.13	The Availability Management process
Figure 3.10	Integrated business-driven technology management	Figure 4.14	Availability terms and measurements
Figure 3.11	The generic process elements	Figure 4.15	The expanded incident lifecycle
		Figure 4.16	The structured approach to Service Failure Analysis (SFA)
		Figure 4.17	Relationship between levels of availability and overall costs
		Figure 4.18	Component Failure Impact Analysis
		Figure 4.19	Example Fault Tree Analysis
		Figure 4.20	Risk Analysis and Management
		Figure 4.21	Lifecycle of Service Continuity Management

- Figure 4.22 Graphical representation of business impacts
- Figure 4.23 Management of Risk
- Figure 4.24 Example summary risk profile
- Figure 4.25 Example set of recovery options
- Figure 4.26 Framework for managing IT security
- Figure 4.27 IT Security Management process
- Figure 4.28 Security controls for threats and incidents
- Figure 4.29 Supplier categorization
- Figure 4.30 Supplier Management process
- Figure 4.31 Supplier categorization
- Figure 5.1 Requirements workshop techniques
- Figure 7.1 Service Management tool evaluation process
- Figure 8.1 Implementation/improvement cycle
- Figure 8.2 Cultural maturity assessment
- Figure 8.3 Process maturity framework
- Figure H.1 Process maturity framework

List of tables

- Table 3.1 Enterprise Architecture frameworks
- Table 3.2 Main service delivery strategies
- Table 3.3 Advantages and disadvantages of service delivery strategies
- Table 3.4 Comparison between conventional ('waterfall') and RAD approaches
- Table 4.1 Examples of risks and threats
- Table 5.1 Requirements engineering – tacit and explicit knowledge
- Table 5.2 Requirements engineering; examples of tacit and explicit knowledge (Maiden and Rugg, 1995)
- Table 5.3 Requirements list
- Table 5.4 Requirements template
- Table 5.5 Applications Portfolio attributes example
- Table 6.1 Example RACI matrix
- Table A.1 Contents of the Service Design Package
- Table B.1 Service Acceptance Criteria
- Table E.1 Building/site
- Table E.2 Major equipment room
- Table E.3 Major data centres
- Table E.4 Regional data centres and major equipment centres
- Table E.5 Server or network equipment rooms
- Table E.6 Office environments
- Table G.1 Example Service Catalogue
- Table H.1 PMF Level 1: initial
- Table H.2 PMF Level 2: repeatable
- Table H.3 PMF Level 3: defined
- Table H.4 PMF Level 4: managed
- Table H.5 PMF Level 5: optimizing

OGC's foreword

Since its creation, ITIL has grown to become the most widely accepted approach to IT Service Management in the world. However, along with this success comes the responsibility to ensure that the guidance keeps pace with a changing global business environment. Service Management requirements are inevitably shaped by the development of technology, revised business models and increasing customer expectations. Our latest version of ITIL has been created in response to these developments.

This is one of five core publications describing the IT Service Management practices that make up ITIL. They are the result of a two-year project to review and update the guidance. The number of Service Management professionals around the world who have helped to develop the content of these publications is impressive. Their experience and knowledge have contributed to the content to bring you a consistent set of high-quality guidance. This is supported by the ongoing development of a comprehensive qualifications scheme, along with accredited training and consultancy.

Whether you are part of a global company, a government department or a small business, ITIL gives you access to world-class Service Management expertise. Essentially, it puts IT services where they belong – at the heart of successful business operations.



Peter Fanning
Acting Chief Executive
Office of Government Commerce

Chief Architect's foreword

Great services do not exist by accident. They have to be carefully planned and designed. Service Design is the means to achieve this. The best Service Strategy cannot be realized without well-designed services. Effective Service Design can lead organizations to greater gains in quality and cost-effectiveness. It reduces the risk of costly compensating for design flaws in the operational environment and ensures that services will perform as they are intended and bring measurable value to the business objectives.

In the past, the IT world has been viewed in two parts – the development world and the operational world. A lack of synergy between these worlds often produces a serious side effect – the business objectives are not met.

A main objective of Service Design is to eliminate this old-world view and bring IT service into a single, consolidated view of designing services within the realities, constraints and opportunities of live operation.

The opportunity to take advantage of new technologies, maximize the use of existing infrastructure, applications, data and knowledge comes to life within the pages of this publication.

Service Design broadens our horizons and helps us to see a larger, more cohesive view of IT Service Management.

Any IT organization that wants to maximize its potential to meet business objectives and business value needs this publication in its arsenal of capabilities.

Service Design is powerful guidance and a cornerstone of practical skills, tools and methods for achieving service excellence.



Sharon Taylor

Chief Architect, ITIL Service Management Practices

Preface

'Quality in a product or service is not what the supplier puts in. It is what the customer gets out and is willing to pay for.'

Peter Drucker, American management guru.

The ITIL Service Management practices are based on this idea. Services are assets from which the customer gains value. How well services are designed with the customers' needs in mind will predict the value that can be derived from them. In the absence of Service Design, service will evolve informally, often without taking advantage of the broader perspective – the business view.

The Service Design phase of the ITIL Service Lifecycle takes business requirements and, using five aspects for Service Design, creates services and their supporting practices that meet business demands for quality, reliability and flexibility. Service Design is iterative throughout the Service Lifecycle, and begins with a solid blueprint that enables the build, test and release stages of Service Transition through the Service Design Package.

Readers will learn about design principles for application, infrastructure, processes and resources, as well as sourcing models. Service Managers will also find guidance on the engineering of sound requirements, Supplier Management and key design considerations for service outsourcing.

Whether you are an internal or external service provider, you are part of a value network and fill a critical role in the Service Lifecycle, by integrating the best practices for Service Design and the ITIL Service Lifecycle into innovative products for the business customer. The Service Design publication provides the knowledge and skills required to assemble the best combination of service assets to produce measurable, scalable and innovative services, along the path to service excellence.

Any IT service provider who is expected to deliver quality to the business customer must have the capability to design services that meet expectations, then go on to exceed those expectations.

The guidance in this publication will help achieve this.

Contact information

Full details of the range of material published under the ITIL banner can be found at
www.best-management-practice.com/itil

For further information on qualifications and training accreditation, please visit www.itil-officialsite.com. Alternatively, please contact:

APMG Service Desk
Sword House
Totteridge Road
High Wycombe
Buckinghamshire
HP13 6DG

Tel: +44 (0) 1494 452450
E-mail: servicedesk@apmg.co.uk

Acknowledgements

Chief Architect and authors

Sharon Taylor (Aspect Group Inc)	Chief Architect
Vernon Lloyd (Fox IT)	Author
Colin Rudd (IT Enterprise Management Services Ltd – ITEMS)	Author

ITIL authoring team

The ITIL authoring team contributed to this guide through commenting on content and alignment across the set. So thanks are also due to the other ITIL authors, specifically Jeroen Bronkhorst (HP), David Cannon (HP), Gary Case (Pink Elephant), Ashley Hannah (HP), Majid Iqbal (Carnegie Mellon University), Shirley Lacy (ConnectSphere), Ivor Macfarlane (Guillemot Rock), Michael Nieves (Accenture), Stuart Rance (HP), George Spalding (Pink Elephant) and David Wheeldon (HP).

Mentors

Tony Jenkins
Sergio Rubinato Filho

Further contributions

A number of people generously contributed their time and expertise to this Service Design publication. Jim Clinch, as OGC Project Manager, is grateful to the support provided by Jenny Dugmore, Convenor of Working Group ISO/IEC 20000, Janine Eves, Carol Hulm, Aidan Lawes and Michiel van der Voort.

The authors would also like to thank Tony Jenkins, DOMAINetc and Steve Rudd IT Enterprise Management Service Limited (ITEMS).

In order to develop ITIL v3 to reflect current best practice and produce publications of lasting value, OGC consulted widely with different stakeholders throughout the world at every stage in the process. OGC would also like to thank the following individuals and their organisations for their contributions to refreshing the ITIL guidance:

The ITIL Advisory Group

Pippa Bass, OGC; Tony Betts, Independent; Megan Byrd, Bank of America; Alison Cartlidge, Xansa; Diane Colbeck, DIYmonde Solutions Inc; Ivor Evans, DIYmonde Solutions Inc; Karen Ferris, ProActive; Malcolm Fry, FRY-Consultants; John Gibert, Independent; Colin Hamilton, RENARD Consulting Ltd; Lex Hendriks, EXIN; Signe Marie Hernes, Det Norske Veritas; Carol Hulm, British Computer Society-ISEB; Tony Jenkins, DOMAINetc; Phil Montanaro, EDS; Alan Nance, ITPreneurs; Christian Nissen, Itelligence; Don Page, Marval Group; Bill Powell, IBM; Sergio Rubinato Filho, CA; James Siminoski, SOScorp; Robert E. Stroud, CA; Jan van Bon, Inform-IT; Ken Wendle, HP; Paul Wilkinson, Getronics PinkRoccade; Takashi Yagi, Hitachi

Reviewers

Kamal Kishore Arora, Infosys Technologies; Martin Andenmatten, Independent; Pierre Bernard, Pink Elephant; Wills Damasio, Quint Wellington Redwood; Catalin Danila, GlaxoSmithKline, SRL Romania; Juergen Dierlamm, Rechtsanwaitkanzlei Dierlamm; Thomas Dressler, EDV-Beratung; Fouad El Sioufy, TUV Rheinland Secure IT GmbH; Jaime Eduardo Facioli, Kalendae IT service Management; Juergen Feldges, DNV; Prasad Gadgil, Satyam Computer Services Ltd; Kingshuk Ghosh, HP; Sandeep Gondhalekar, Quint Wellington Redwood; John Graham, Educad; Juergen Gross, Independent; Tsuyoshi Hamada, HP; Colin Hamilton, RENARD Consulting Ltd; Christoph Herwig, Accenture; Thomas Hess, Pluralis AG; Chris Jones, Ariston Strategic Consulting; Daniel Keller, Swiss SUIT; Hendrikje Kuhne, Ktp-organisationsterberatung; Jane Link, Acerit Limited; Paul Martini, HP; Raimund Martl, HP; Alan Nance, Itpreneurs; Christian Nissen, Itelligence; Glen Notman, Pink Elephant; Tuomas Nurmiela, TietoEnator Processing & Network Oy; Benjamin Orazem, SRC.SI; Gerard Persoon, E.Novation; Neil Pinkerton, Laughingtree; Christian Probst, Quint Wellington Redwood; Rajesh Radhakrishnan, IBM; Brian Rowlett, LogicaCMG; Sutirtha Roy Chowdhury, Sierra Systems; Alexander Sapronov, HP; Frances Scarff, OGC; Alan Shepherd, Deutsche Bank AG; Rob Stroud, CA; Michael Tomkinson, BT; Ken Turbitt, BMC Software; Wiley Vasquez, BMC Software; Ettiene Vermeulen, Datacentrix; Joachim von Caron, Lufthansa Systems; Andreas Weinberger, DekaBank; Sven Werner, Unilog Avinci GmbH; Theresa Wright, Computacenter Services; Geoffrey Wyeth, Independent; Rob Young, Fox IT



1

Introduction

1 Introduction

The primary objective of Service Management is to ensure that the IT services are aligned to the business needs and actively support them. It is imperative that the IT services underpin the business processes, but it is also increasingly important that IT acts as an agent for change to facilitate business transformation.

All organizations that use IT will depend on IT to be successful. If IT processes and IT services are implemented, managed and supported in the appropriate way, the business will be more successful, suffer less disruption and loss of productive hours, reduce costs, increase revenue, improve public relations and achieve its business objectives.

Most authorities now identify four types of IT assets that need to be acquired and managed in order to contribute to effective IT service provision. These are IT infrastructure, applications, information and people. Specifically there is a strong emphasis on the acquisition, management and integration of these assets throughout their 'birth to retirement' lifecycle. The delivery of quality IT services depends on the effective and efficient management of these assets.

These assets on their own, however, are not enough to meet the Service Management needs of the business. ITIL Service Management practices use these four asset types as part of a set of capabilities and resources called 'service assets'.

An IT service, used in support of business processes, is constructed from a combination of IT assets and externally

provided 'underpinning' services. Once in place, an IT service must be supported throughout its 'life', during which time it may be modified many times, either through technological innovation, changing business environment, changing usage of the service, changing its service quality parameters, or changing its supporting IT assets or capabilities (e.g. a change in an application software component to provide additional functionality). Eventually the IT service is retired, when business processes no longer have a use for it or it is no longer cost-effective to run. Service Transition is involved in the build and deployment of the service and day-to-day support, and delivery of the service is the role of Service Operation, while Continual Service Improvement implements best practice in the optimize and retire stages.

From this perspective, Service Design can be seen as gathering service needs and mapping them to requirements for integrated services, and creating the design specifications for the service assets needed to provide services. A particular feature of this approach is a strong emphasis on re-use during design.

The main aim of Service Design is to design IT services, together with the governing IT practices, processes and policies, to realize the strategy and to facilitate the introduction of these services into the live environment ensuring quality service delivery, customer satisfaction and cost-effective service provision. Service Design should also design the IT services effectively so that they don't need a great deal of improvement during their lifecycle. However, continual improvement should be embedded in all Service

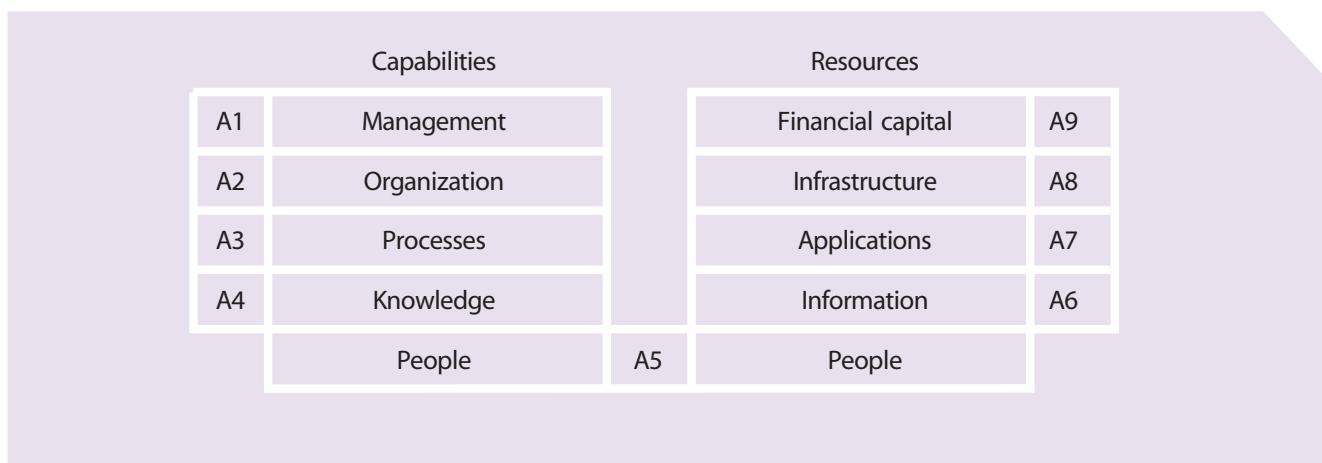


Figure 1.1 Resources and capabilities are the basis for value creation

Design activities to ensure that the solutions and designs become even more effective over time and to identify changing trends in the business that may offer improvement opportunities. Service Design activities can be periodic or exception-based when they may be triggered by a specific business need or event.

If services or processes are not designed they will evolve organically. If they evolve without proper controls, the tendency is simply to react to environmental conditions that have occurred rather than to understand clearly the overall vision and overall needs of the business. Designing to match the anticipated environment is much more effective and efficient, but often impossible – hence the need to consider iterative and incremental approaches to Service Design. Iterative and incremental approaches are essential to ensure that services introduced to the live environment adapt and continue to remain in line with evolving business needs. In the absence of formalized Service Design, services will often be unduly expensive to run, prone to failure, resources will be wasted and services will not be fully aligned to business needs. It is unlikely that any improvement programme will ever be able to achieve what proper design would achieve in the first place. Without Service Design, cost-effective service is not possible. The human aspects of Service Design are also of the utmost importance, and these will be explored in detail later in this publication.

1.1 OVERVIEW

This publication forms part of the overall ITIL Service Management practices and covers the design of appropriate and innovative IT services to meet current and future agreed business requirements. It describes the principles of Service Design and looks at identifying, defining and aligning the IT solution with the business requirements. It also introduces the concept of the Service Design Package and looks at selecting the appropriate Service Design model. The publication also discusses the fundamentals of the design processes and the five aspects of the design:

- Services
- Design of Service Management systems and tools, especially the Service Portfolio
- Technology architectures and management systems
- Processes
- Measurement methods and metrics.

The publication covers the methods, practices and tools to achieve excellence in Service Design. It enforces the principle that the initial Service Design should be driven

by a number of factors, including the functional requirements, the requirements within the Service Level Agreements (SLAs), the business benefits and the overall design constraints.

Chapter 4 explains the end-to-end process of the areas key to successful Service Design. These processes are utilized by all other stages of the Service Lifecycle, and other processes are taken into account by Service Design. However, it is here that Service Catalogue Management, Service Level Management, Capacity Management, Availability Management, IT Service Continuity Management, Information Security Management and Supplier Management are covered in detail.

The appendices to this publication give examples of the Service Design Package, Service Acceptance Criteria, process documentation templates, design and planning documents, environmental architectures and standards, sample SLAs, OLAs and Service Catalogue and the Service Management process maturity framework.

1.2 CONTEXT

1.2.1 Service Management

Information technology (IT) is a commonly used term that changes meaning with context. From the first perspective, IT systems, applications, and infrastructure are components or sub-assemblies of a larger product. They enable or are embedded in processes and services. From the second perspective, IT is an organization with its own set of capabilities and resources. IT organizations can be of various types, such as business functions, shared services units, and enterprise-level core units.

From the third perspective, IT is a category of services utilized by business. They are typically IT applications and infrastructure that are packaged and offered as services by internal IT organizations or external service providers. IT costs are treated as business expenses. From the fourth perspective, IT is a category of business assets that provide a stream of benefits for their owners, including but not limited to revenue, income and profit. IT costs are treated as investments.

1.2.2 Good practice in the public domain

Organizations operate in dynamic environments with the need to learn and adapt. There is a need to improve performance while managing trade-offs. Under similar pressure, customers seek advantage from service providers. They pursue sourcing strategies that best serve their own business interests. In many countries, government agencies and non-profits have a similar

tendency to outsource for the sake of operational effectiveness. This puts additional pressure on service providers to maintain a competitive advantage with respect to the alternatives that customers may have. The increase in outsourcing has particularly exposed internal service providers to unusual competition.

To cope with the pressure, organizations benchmark themselves against peers and seek to close gaps in capabilities. One way to close such gaps is the adoption of good practices in wide industry use. There are several sources for good practices, including public frameworks, standards, and the proprietary knowledge of organizations and individuals (Figure 1.2).

Public frameworks and standards are attractive when compared with proprietary knowledge:

- Proprietary knowledge is deeply embedded in organizations and therefore difficult to adopt, replicate or transfer, even with the cooperation of the owners. Such knowledge is often in the form of tacit knowledge that is inextricable and poorly documented.

- Proprietary knowledge is customized for the local context and specific business needs to the point of being idiosyncratic. Unless the recipients of such knowledge have matching circumstances, the knowledge may not be as effective in use.
- Owners of proprietary knowledge expect to be rewarded for their long-term investments. They may make such knowledge available only under commercial terms through purchases and licensing agreements.
- Publicly available frameworks and standards such as ITIL, COBIT, CMMI, eSCM-SP, PRINCE2, ISO 9000, ISO/IEC 20000, and ISO/IEC 27001 are validated across a diverse set of environments and situations rather than the limited experience of a single organization. They are subject to broad review across multiple organizations and disciplines. They are vetted by diverse sets of partners, suppliers and competitors.
- The knowledge of public frameworks is more likely to be widely distributed among a large community of professionals through publicly available training and certification. It is easier for organizations to acquire such knowledge through the labour market.

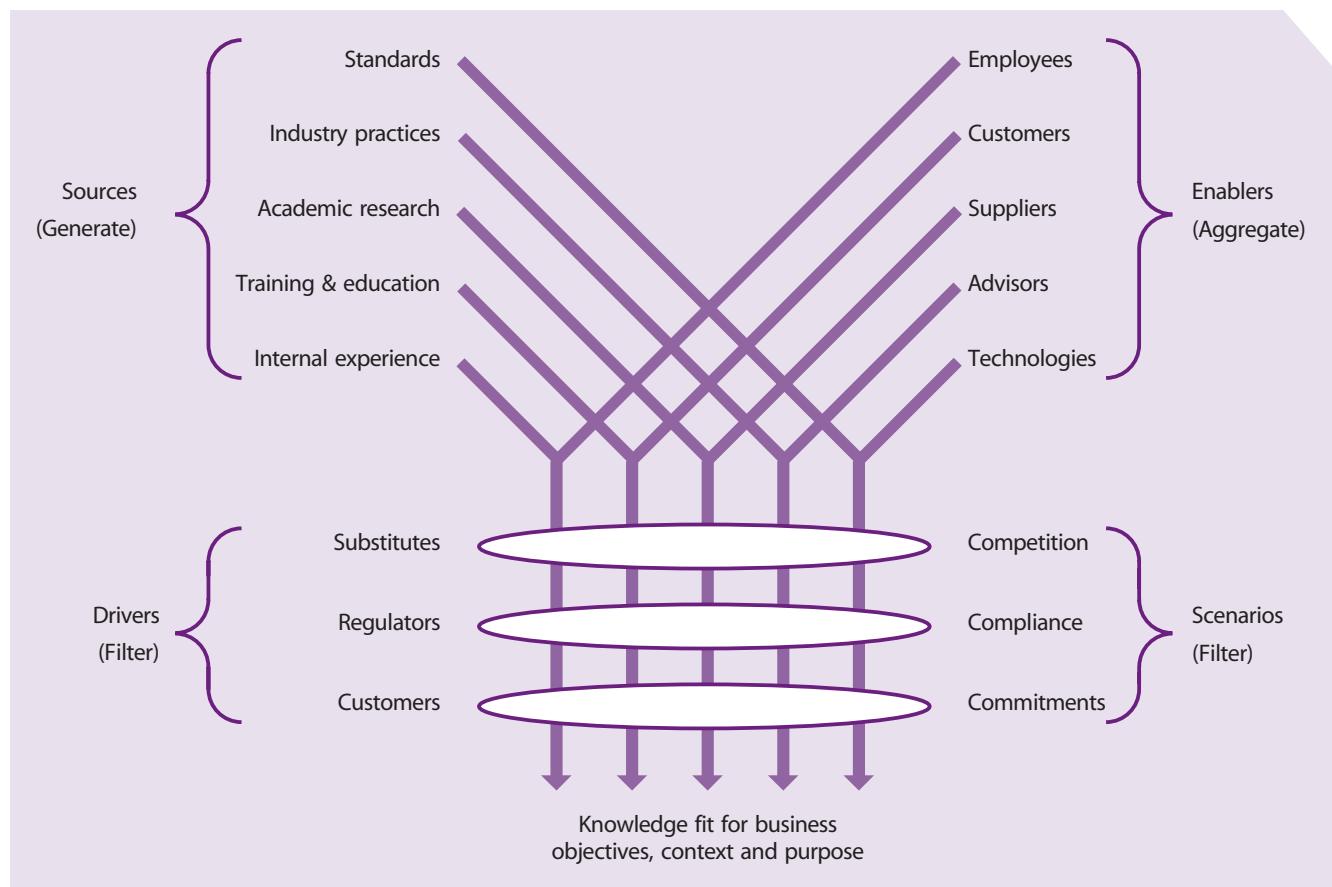


Figure 1.2 Sourcing of Service Management practice

Ignoring public frameworks and standards can needlessly place an organization at a disadvantage. Organizations should cultivate their own proprietary knowledge on top of a body of knowledge based on public frameworks and standards. Collaboration and coordination across organizations are easier on the basis of shared practices and standards.

1.2.3 ITIL and good practice in Service Management

The context of this publication is the ITIL Framework as a source of good practice in Service Management. ITIL is used by organizations worldwide to establish and improve capabilities in Service Management. ISO/IEC 20000 provides a formal and universal standard for organizations seeking to have their Service Management capabilities audited and certified. While ISO/IEC 20000 is a standard to be achieved and maintained, ITIL offers a body of knowledge useful for achieving the standard.

The ITIL Library has the following components:

- The ITIL Core – best practice guidance applicable to all types of organizations who provide services to a business
- The ITIL Complementary Guidance – a complementary set of publications with guidance specific to industry sectors, organization types, operating models and technology architectures.

The ITIL Core consists of five publications (Figure 1.3). Each provides the guidance necessary for an integrated approach, as required by the ISO/IEC 20000 standard specification:

- Service Strategy
- Service Design
- Service Transition
- Service Operation
- Continual Service Improvement.

Each publication addresses capabilities having direct impact on a service provider's performance. The structure of the Core is in the form of a lifecycle. It is iterative and multidimensional. It ensures organizations are set up to leverage capabilities in one area for learning and improvements in others. The Core is expected to provide structure, stability and strength to Service Management capabilities with durable principles, methods and tools. This serves to protect investments and provide the necessary basis for measurement, learning and improvement.

The guidance in ITIL can be adapted for use in various business environments and organizational strategies. The Complementary Guidance provides flexibility to implement the Core in a diverse range of environments. Practitioners can select Complementary Guidance as needed to provide traction for the Core in a given business context, much like tyres are selected based on the type of vehicle, purpose and road conditions. This is to increase the durability and portability of knowledge assets and to protect investments in Service Management capabilities.

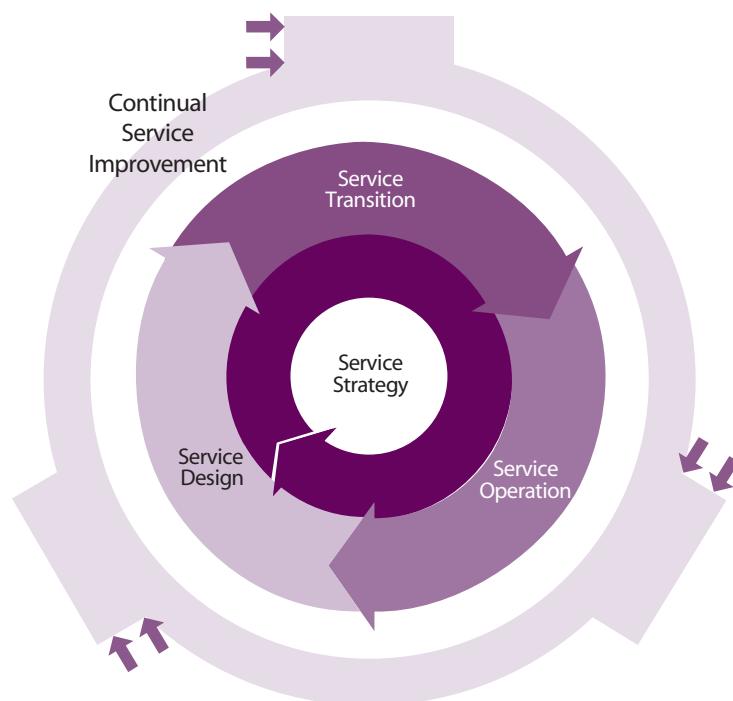


Figure 1.3 ITIL Core

1.2.3.1 Service Strategy

The Service Strategy publication provides guidance on how to design, develop and implement Service Management, not only as an organizational capability but also as a **strategic asset**. Guidance is provided on the principles underpinning the practice of Service Management, which are useful for developing Service Management policies, guidelines and processes across the ITIL Service Lifecycle. Service Strategy guidance is useful in the context of Service Design, Service Transition, Service Operation, and Continual Service Improvement. Topics covered in Service Strategy include the development of markets – internal and external, service assets, service catalogue, and implementation of strategy through the Service Lifecycle. Financial Management, Service Portfolio Management, Organizational Development and Strategic Risks are among other major topics.

Organizations use the guidance to set objectives and expectations of performance towards serving customers and market spaces, and to identify, select and prioritize opportunities. Service Strategy is about ensuring that organizations are in a position to handle the costs and risks associated with their Service Portfolios, and are set up not just for operational effectiveness but also for distinctive performance. Decisions made with respect to Service Strategy have far-reaching consequences, including those with delayed effect.

Organizations already practising ITIL use this publication to guide a strategic review of their ITIL-based Service Management capabilities and to improve the alignment between those capabilities and their business strategies. This publication of ITIL encourages readers to stop and think about why something is to be done before thinking of how. Answers to the first type of questions are closer to the customer's business. Service Strategy expands the scope of the ITIL Framework beyond the traditional audience of IT Service Management professionals.

1.2.3.2 Service Design

The Service Design publication provides guidance for the design and development of services and Service Management processes. It covers design principles and methods for converting strategic objectives into portfolios of services and service assets. The scope of Service Design is not limited to new services. It includes the changes and improvements necessary to increase or maintain value to customers over the lifecycle of services, the continuity of services, achievement of service levels and conformance to standards and regulations. It guides organizations on how to develop design capabilities for Service Management.

1.2.3.3 Service Transition

The Service Transition publication provides guidance for the development and improvement of capabilities for transitioning new and changed services into operations. This publication provides guidance on how the requirements of Service Strategy encoded in Service Design are effectively realized in service operations while controlling the risks of failure and disruption. The publication combines practices in Release Management, Programme Management and risk management, and places them in the practical context of Service Management. It provides guidance on managing the complexity related to changes to services and Service Management processes – preventing undesired consequences while allowing for innovation. Guidance is provided on transferring the control of services between customers and service providers.

1.2.3.4 Service Operation

This publication embodies practices in the management of service operations. It includes guidance on achieving effectiveness and efficiency in the delivery and support of services so as to ensure value for the customer and the service provider. Strategic objectives are ultimately realized through service operations, therefore making it a critical capability. Guidance is provided on how to maintain stability in service operations, allowing for changes in design, scale, scope and service levels. Organizations are provided with detailed process guidelines, methods and tools for use in two major control perspectives: reactive and proactive. Managers and practitioners are provided with knowledge allowing them to make better decisions in areas such as managing the availability of services, controlling demand, optimizing capacity utilization, scheduling operations and fixing problems. Guidance is provided on supporting operations through new models and architectures such as shared services, utility computing, internet services and mobile commerce.

1.2.3.5 Continual Service Improvement

This publication provides instrumental guidance in creating and maintaining value for customers through better design, transition and operation of services. It combines principles, practices and methods from quality management, Change Management and capability improvement. Organizations learn to realize incremental and large-scale improvements in service quality, operational efficiency and business continuity. Guidance is provided for linking improvement efforts and outcomes with service strategy, design, transition and operation. A closed-loop feedback system, based on the

Plan–Do–Check–Act (PDCA) model specified in ISO/IEC 20000, is established and capable of receiving inputs for change from any planning perspective.

1.3 PURPOSE

The aim of this publication is to give the reader guidance on using recommended practices when designing IT services and IT Service Management processes.

This publication follows on from the Service Strategy publication, which provides guidance on alignment and integration of the business needs to IT. It enables the reader to assess the requirements when designing a service, and documents industry best practice for the design of IT services and processes.

Although this publication can be read in isolation, it is recommended that it be used in conjunction with the other ITIL publications. The guidance in the ITIL publications is applicable generically. It is neither bureaucratic nor unwieldy if utilized sensibly and in full recognition of the business needs of the organization. Service Design is important for setting the stage to deliver services effectively to the business and meet the demand for growth and change. Enhancement is typically greater in cost and resource than development. Significant consideration should therefore be given to designing for the ease and economy of support over the whole lifecycle, but more importantly it is not possible to completely re-engineer a service once in production. It may be possible to get close, but it will be impossible to get back to a design once something is running. Retrofitting the design is difficult and costly and never achieves what could have been achieved if designed properly in the first place.

1.4 USAGE

This publication is relevant to anyone involved in the design, delivery or support of IT services. It will have relevance to the IT Architect, IT managers and practitioners at all levels. All the publications in the ITIL Service Management Core Library need to be read to fully appreciate and understand the overall lifecycle of services and of IT Service Management.

There are several ways of delivering an IT service, such as in-house, outsourced and partnership. This publication is generally relevant to all methods of service provision. So those involved in delivering IT services – within their own organization, in outsourced service provision or working in partnerships – will find that this publication is applicable to them. Business managers may find the publication helpful in understanding and establishing best practice IT services and support. Managers from supplier organizations will also find this publication relevant when setting up agreements for the delivery and support of services.



Service Management as a practice

2

2 Service Management as a practice

2.1 WHAT IS SERVICE MANAGEMENT?

Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services. The capabilities take the form of functions and processes for managing services over a lifecycle, with specializations in strategy, design, transition, operation and continual improvement. The capabilities represent a service organization's capacity, competency and confidence for action. The act of transforming resources into valuable services is at the core of Service Management. Without these capabilities, a service organization is merely a bundle of resources that by itself has relatively low intrinsic value for customers.

Service Management is a set of specialized organizational capabilities for providing value to customers in the form of services.

Organizational capabilities are shaped by the challenges they are expected to overcome. Service Management capabilities are similarly influenced by the following challenges that distinguish services from other systems of value creation such as manufacturing, mining and agriculture:

- Intangible nature of the output and intermediate products of service processes: difficult to measure, control and validate (or prove)
- Demand is tightly coupled with customer's assets: users and other customer assets such as processes, applications, documents and transactions arrive with demand and stimulate service production
- High level of contact for producers and consumers of services: little or no buffer between the customer, the front-office and back-office
- The perishable nature of service output and service capacity: there is value for the customer from assurance on the continued supply of consistent quality. Providers need to secure a steady supply of demand from customers.

Service Management, however, is more than just a set of capabilities. It is also a professional practice supported by an extensive body of knowledge, experience and skills. A global community of individuals and organizations in the public and private sectors fosters its growth and maturity. Formal schemes exist for the education, training and certification of practising organizations, and individuals

influence its quality. Industry best practices, academic research and formal standards contribute to its intellectual capital and draw from it.

The origins of Service Management are in traditional service businesses such as airlines, banks, hotels and phone companies. Its practice has grown with the adoption by IT organizations of a service-oriented approach to managing IT applications, infrastructure and processes. Solutions to business problems and support for business models, strategies and operations are increasingly in the form of services. The popularity of shared services and outsourcing has contributed to the increase in the number of organizations who are service providers, including internal organizational units. This, in turn, has strengthened the practice of Service Management, at the same time imposing greater challenges on it.

2.2 WHAT ARE SERVICES?

2.2.1 The value proposition

A service is a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks.

Services are a means of delivering value to customers by facilitating outcomes customers want to achieve without the ownership of specific costs and risks. Services facilitate outcomes by enhancing the performance of associated tasks and reducing the effect of constraints. The result is an increase in the probability of desired outcomes.

Over the years, organizations have debated the definition of a 'service'. The illustration in Figure 2.1 is an example of the realization that service is really about delivering value to customers.

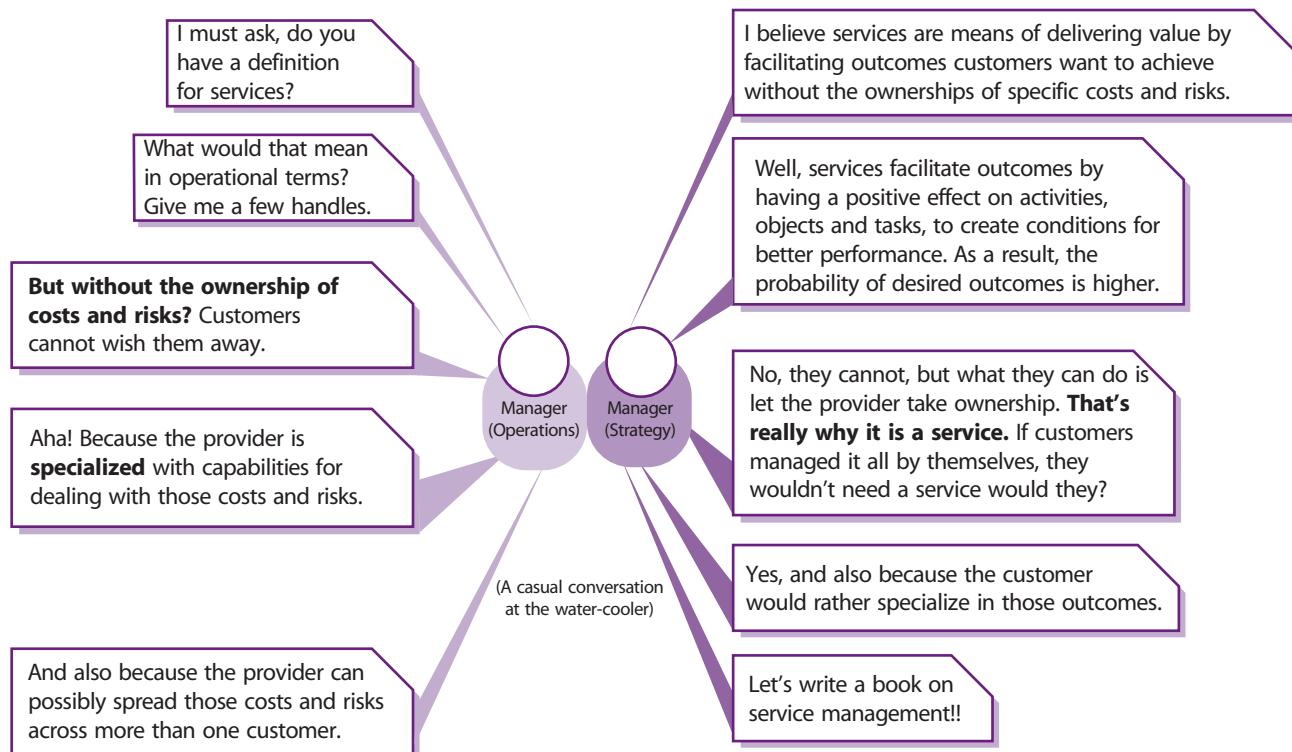


Figure 2.1 A conversation about the definition and meaning of services

2.3 FUNCTIONS AND PROCESSES ACROSS LIFECYCLE

2.3.1 Functions

Functions are units of organizations specialized to perform certain types of work and responsible for specific outcomes. They are self-contained, with capabilities and resources necessary for their performance and outcomes. Capabilities include work methods internal to the functions. Functions have their own body of knowledge, which accumulates from experience. They provide structure and stability to organizations.

Functions are means to structure organizations to implement the specialization principle. Functions typically define roles and the associated authority and responsibility for a specific performance and outcomes. Coordination between functions through shared processes is a common pattern in organization design. Functions tend to optimize their work methods locally to focus on assigned outcomes. Poor coordination between functions, combined with an inward focus, leads to functional silos that hinder the alignment and feedback that are critical to the success of the organization as a whole. Process models

help avoid this problem with functional hierarchies by improving cross-functional coordination and control. Well-defined processes can improve productivity within and across functions.

2.3.2 Processes

Processes are examples of closed-loop systems because they provide change and transformation towards a goal, and utilize feedback for self-reinforcing and self-corrective action (Figure 2.2). It is important to consider the entire process or how one process fits into another.

Process definitions describe actions, dependencies and sequence. Processes have the following characteristics:

- **Measurable** – we are able to measure the process in a relevant manner. It is performance driven. Managers want to measure cost, quality and other variables while practitioners are concerned with duration and productivity.
- **Specific results** – the reason a process exists is to deliver a specific result. This result must be individually identifiable and countable. While we can count changes, it is impossible to count how many Service Desks were completed.

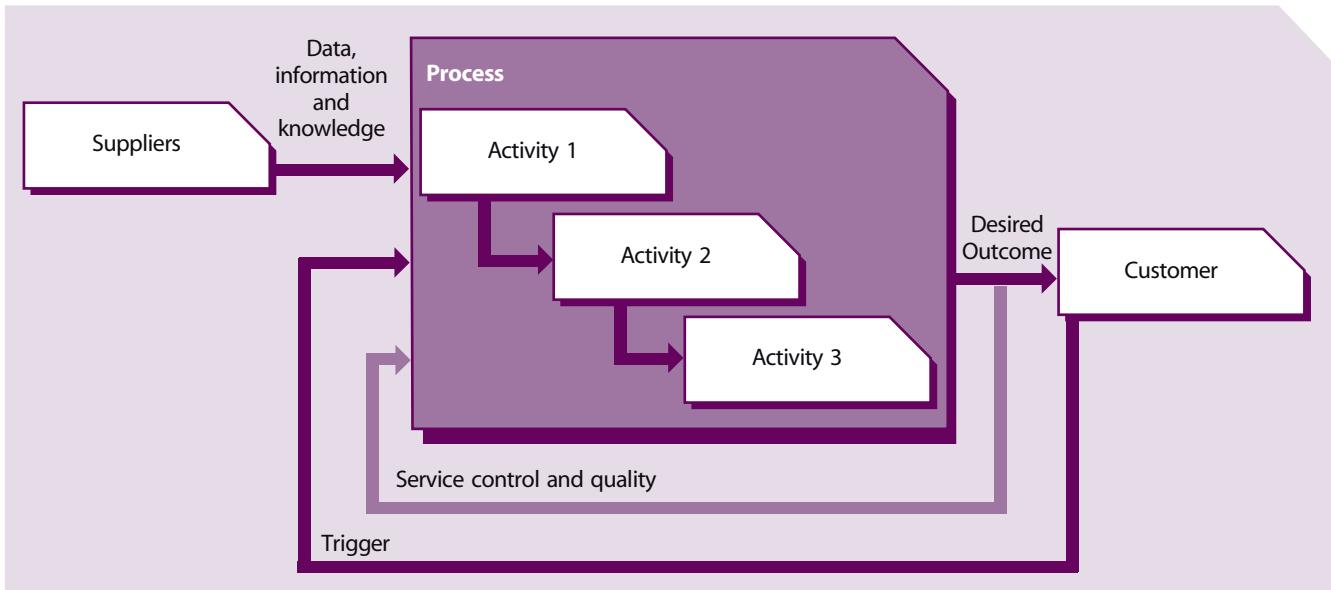


Figure 2.2 A basic process

- **Customers** – every process delivers its primary results to a customer or stakeholder. Customers may be internal or external to the organization, but the process must meet their expectations.
- **Responds to a specific event** – while a process may be ongoing or iterative, it should be traceable to a specific trigger.

There is often confusion around functions, processes, roles and activities. Functions are often mistaken for processes, and processes mistaken for functions. Service Design, as well as being a stage in the lifecycle of a service, can itself be seen by some organizations as a function, by others as a role or a set of processes or as an activity. Whether or not it is a function, role, activity or set of processes depends entirely on the size, structure and culture of an organization. It is important that however it is defined and implemented within an organisation, the success of the function, process, role or activity is measured and continually improved.

2.3.3 Specialization and coordination across the lifecycle

Specialization and coordination are necessary in the lifecycle approach. Feedback and control between the functions and processes within and across the elements of the lifecycle make this possible. The dominant pattern in the lifecycle is the sequential progress starting from SS

through SD-ST-SO and back to SS through CSI. That, however, is not the only pattern of action. Every element of the lifecycle provides points for feedback and control.

The combination of multiple perspectives allows greater flexibility and control across environments and situations. The lifecycle approach mimics the reality of most organizations, where effective management requires the use of multiple control perspectives. Those responsible for the design, development and improvement of processes for Service Management can adopt a process-based control perspective. For those responsible for managing agreements, contracts and services may be better served by a lifecycle-based control perspective with distinct phases. Both these control perspectives benefit from systems thinking. Each control perspective can reveal patterns that may not be apparent from the other.

2.4 SERVICE DESIGN FUNDAMENTALS

2.4.1 Purpose/goal/objective

The main purpose of the Service Design stage of the lifecycle is the design of new or changed services for introduction into the live environment. It is important that a holistic approach to all aspects of design is adopted, and that when changing or amending any of the individual elements of design all other aspects are considered. Thus when designing and developing a new application, this

shouldn't be done in isolation, but should also consider the impact on the overall service, the management systems and tools (e.g. Service Portfolio and Service Catalogue), the architectures, the technology, the Service Management processes and the necessary measurements and metrics. This will ensure not only that the functional elements are addressed by the design, but also that all of the management and operational requirements are addressed as a fundamental part of the design and are not added as an afterthought.

Key message

A holistic approach should be adopted for all Service Design aspects and areas to ensure consistency and integration within all activities and processes across the entire IT technology, providing end-to-end business-related functionality and quality.

Not every change within an IT service will require the instigation of Service Design activity. It will only be

required where there is 'significant' change. Every organization must define what constitutes 'significant' so that everyone within the organization is clear as to when Service Design activity is instigated. Therefore all changes should be assessed for their impact on Service Design activities to determine whether they are significant in terms of requiring Service Design activity. This should be part of the Change Management process impact assessment within the Service Transition publication of ITIL.

2.4.2 Scope

There are five individual aspects of Service Design considered within this publication. These are the design of:

- New or changed services
- Service Management systems and tools, especially the Service Portfolio, including the Service Catalogue
- Technology architecture and management systems
- The processes required
- Measurement methods and metrics.

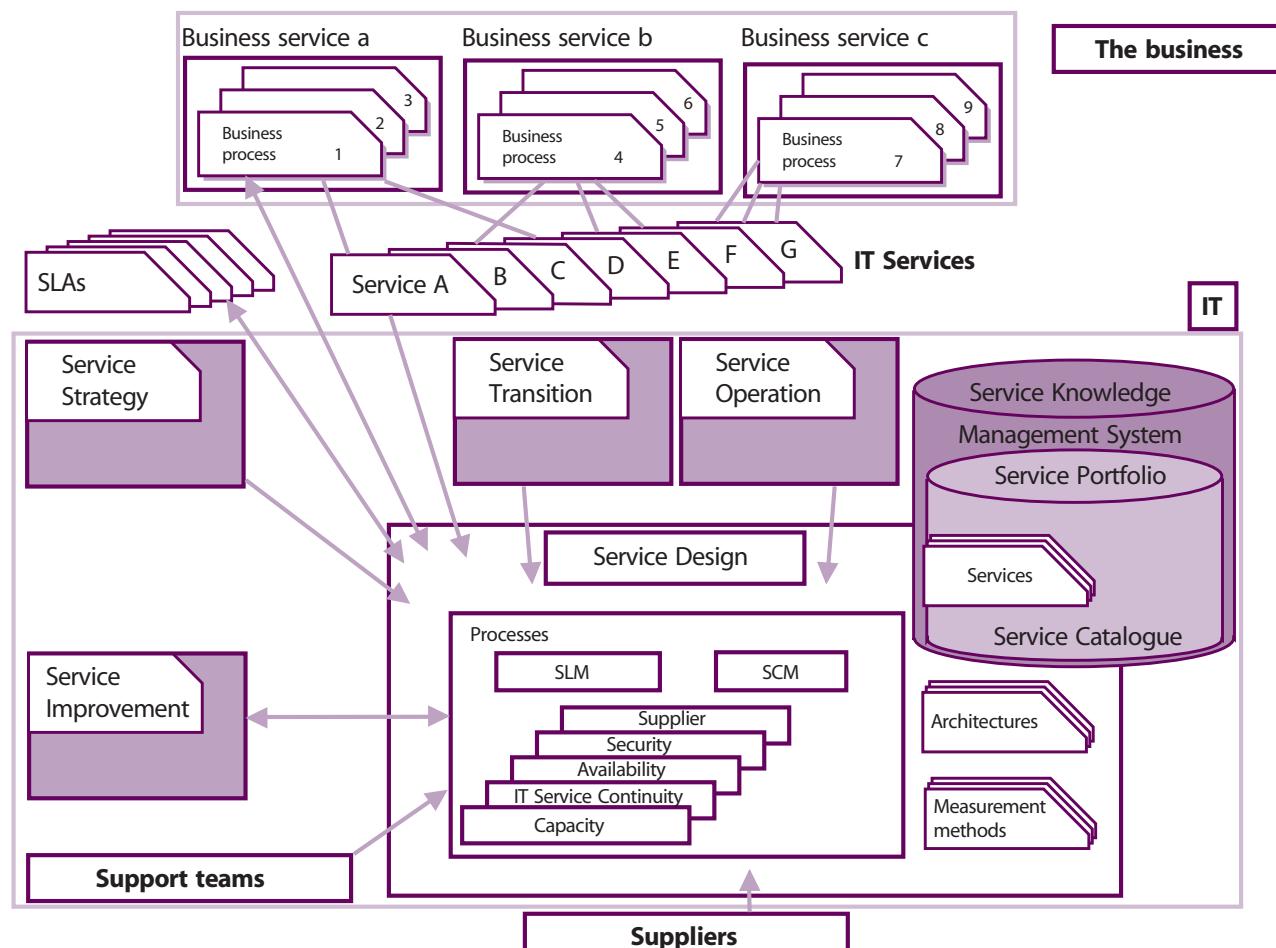


Figure 2.3 Scope of Service Design

The Service Design stage of the lifecycle starts with a set of new or changed business requirements and ends with the development of a service solution designed to meet the documented needs of the business. This developed solution, together with its Service Design Package (SDP – see Appendix A), is then passed to Service Transition to evaluate, build, test and deploy the new or changed service. On completion of these transition activities, control is transferred to the Service Operation stage of the Service Lifecycle. The activities involved in these stages are outlined in section 3. The overall scope of Service Design and the five aspects of design and how they interact are illustrated in Figure 2.3.

The main aim of Service Design is the design of new or changed services. The requirements for these new services are extracted from the Service Portfolio. Each requirement is analysed, documented and agreed, and a solution design is produced that is then compared with the strategies and constraints from Service Strategy to ensure that it conforms to corporate and IT policies. Each individual Service Design is also considered in conjunction with each of the other aspects of Service Design:

- **The Service Management systems and tools, especially the Service Portfolio:** to ensure that this new or changed service is consistent with all other services, and that all other services that interface, support or depend on the new or changed services are consistent with the new service. If not, either the design of the new service or the other existing services will need to be adapted. Also the Service Management systems and tools should be reviewed to ensure they are capable of supporting the new or changed service.
- **The technology architectures and management systems:** to ensure that all the technology architectures and management systems are consistent with the new or changed service and have the capability to operate and maintain the new service. If not, then either the architectures or management systems will need to be amended or the design of the new service will need to be revised.
- **The processes:** to ensure that the processes, roles, responsibilities and skills have the capability to operate, support and maintain the new or changed service. If not, the design of the new service will need to be revised or the existing process capabilities will need to be enhanced. This includes all IT and Service Management processes, not just the key Service Design processes.

- **The measurement methods and metrics:** to ensure that the existing measurement methods can provide the required metrics on the new or changed service. If not, then the measurement methods will need to be enhanced or the service metrics will need to be revised.

If all the above activities are completed during the Service Design stage, this will ensure that there will be minimal issues arising during the subsequent stages of the Service Lifecycle. Therefore Service Design must consolidate the key design issues and activities of all IT and Service Management processes within its own design activities, to ensure that all aspects are considered and included within all designs for new or changed services as part of everyday process operation.

The ability to measure and demonstrate value to the business requires the capability to link business outcomes, objectives and their underpinning processes and functions to the IT services and their underpinning assets, processes and functions. This value should be articulated by:

- Agreeing service levels, SLAs and targets across the whole enterprise, ensuring critical business processes receive most attention
- Measuring IT quality in business/user terms, reporting what is relevant to users (e.g. customer satisfaction, business value)
- Mapping business processes to IT infrastructure, since new components are added continuously, increasing the possibility of disruptions caused by IT and loss of focus on business services and processes
- Mapping business processes to business and service measurements, making services focus on IT measurements related to key aspects of business performance
- Mapping infrastructure resources to services in order to take full advantage of critical IT components within the Configuration Management System (CMS), which are linked to critical business processes. This may also use information within the complete Service Knowledge Management System (SKMS). More information can be found on the CMS within the Service Transition publication
- Providing end-to-end performance monitoring and measurement of online business processes, periodically reported against SLA targets.

Often the design of a major new or changed service will require that design changes are considered, and often affect or are affected by all of the other four phases of the Service Lifecycle. It is essential, therefore, that IT systems and services are designed, planned, implemented and managed appropriately for the business as a whole. The requirement then is to provide IT services that:

- Are business- and customer-oriented, focused and driven
- Are cost-effective and secure
- Are flexible and adaptable, yet fit for purpose at the point of delivery
- Can absorb an ever-increasing demand in the volume and speed of change
- Meet increasing business demands for continuous operation
- Are managed and operated to an acceptable level of risk
- Are responsive, with appropriate availability matched to business needs.

With all these pressures on both IT and the business, the temptation – and unfortunately the reality in some cases – is to ‘cut corners’ on the design and planning processes or to ignore them completely. However, in these situations the design and planning activities are even more essential to the overall delivery of quality services. Therefore, more time rather than less should be devoted to the design processes and their implementation.

In order that effective, quality design can be achieved, even when timescales are short and pressure to deliver services is high, organizations should ensure that the importance of the Service Design function is fully

understood and that support is provided to maintain and mature Service Design as a fundamental element of Service Management. Organizations should strive continually to review and improve their Service Design capability, in order that Service Design can become a consistent and repeatable practice, enabling organizations to deliver quality services against challenging timescales. Having a mature Service Design practice will also enable organizations to reduce risk in the transition and operational stages of service.

In general, the key to the successful provision of IT services is an appropriate level of design and planning to determine which projects, processes and services will have the greatest impact or benefit to the business. With the appropriate level of thought, design, preparation and planning, effort can be targeted at those areas that will yield the greatest return. Risk assessment and management are key requirements within all design activities. Therefore all five aspects of Service Design must include risk assessment and management as an integrated, inherent part of everything they do. This will ensure that the risks involved in the provision of services and the operation of processes, technology and measurement methods are aligned with business risk and impact, because risk assessment and management are embedded within all design processes and activities.

Many designs, plans and projects fail through a lack of preparation and management. The implementation of ITIL Service Management as a practice is about preparing and planning the effective and efficient use of the four Ps: the People, the Processes, the Products (services, technology and tools) and the Partners (suppliers, manufacturers and vendors), as illustrated in Figure 2.4.

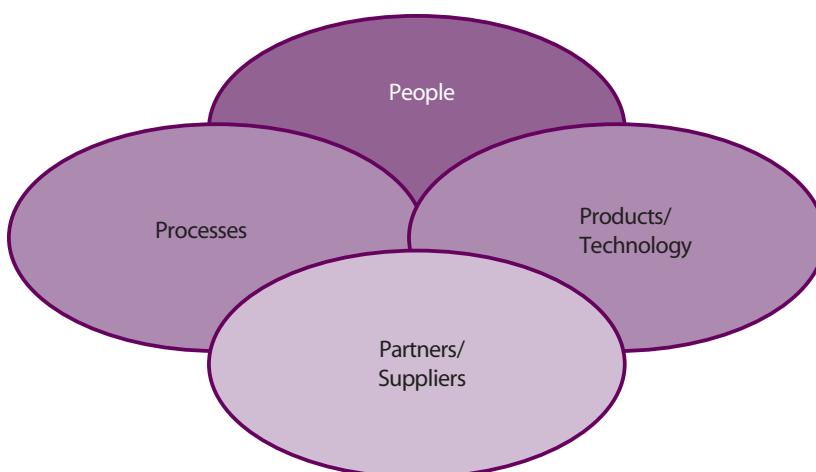


Figure 2.4 The Four Ps

However, there is no benefit in producing designs, plans, architectures and policies and keeping them to yourself. They must be published, agreed, circulated and actively used.

In order to ensure that business and IT services remain synchronized, many organizations form committees of senior management from the business and IT organizations. The committee carries the overall accountability for setting governance, direction, policy and strategy for IT services. Many organizations refer to this group as the IT Strategy or Steering Group. (ISG). The function of an ISG is to act as a partnership between IT and the business. It should meet regularly and review the business and IT strategies, designs, plans, service portfolio, architectures and policies to ensure that they are closely aligned with each other. It should provide the vision, set direction and determine priorities of individual programmes and projects to ensure that IT is aligned and focused on business targets and drivers. The group should also ensure that unrealistic timescales, which could jeopardize quality or disrupt normal operational requirements, are not imposed or attempted by either the business or IT. See Figure 2.5.

The ISG will include discussions on all aspects of the business that involve IT service, as well as proposed or possible change at a strategic level. Subjects for the ISG to discuss may include:

- **Reviewing business and IT plans:** to identify any changes in either area that would trigger the need to create, enhance or improve services
- **Demand planning:** to identify any changes in demand for both short- and long-term planning horizons; such changes may be increases or decreases in demand, and concern both business-as-usual and projects
- **Project authorization and prioritization:** to ensure that projects are authorized and prioritized to the mutual satisfaction of both the business and IT
- **Review of projects:** to ensure that the expected business benefits are being realized in accordance with project business cases, and to identify whether the projects are on schedule
- **Potential outsourcing:** to identify the need and content of sourcing strategies for the IT service provision

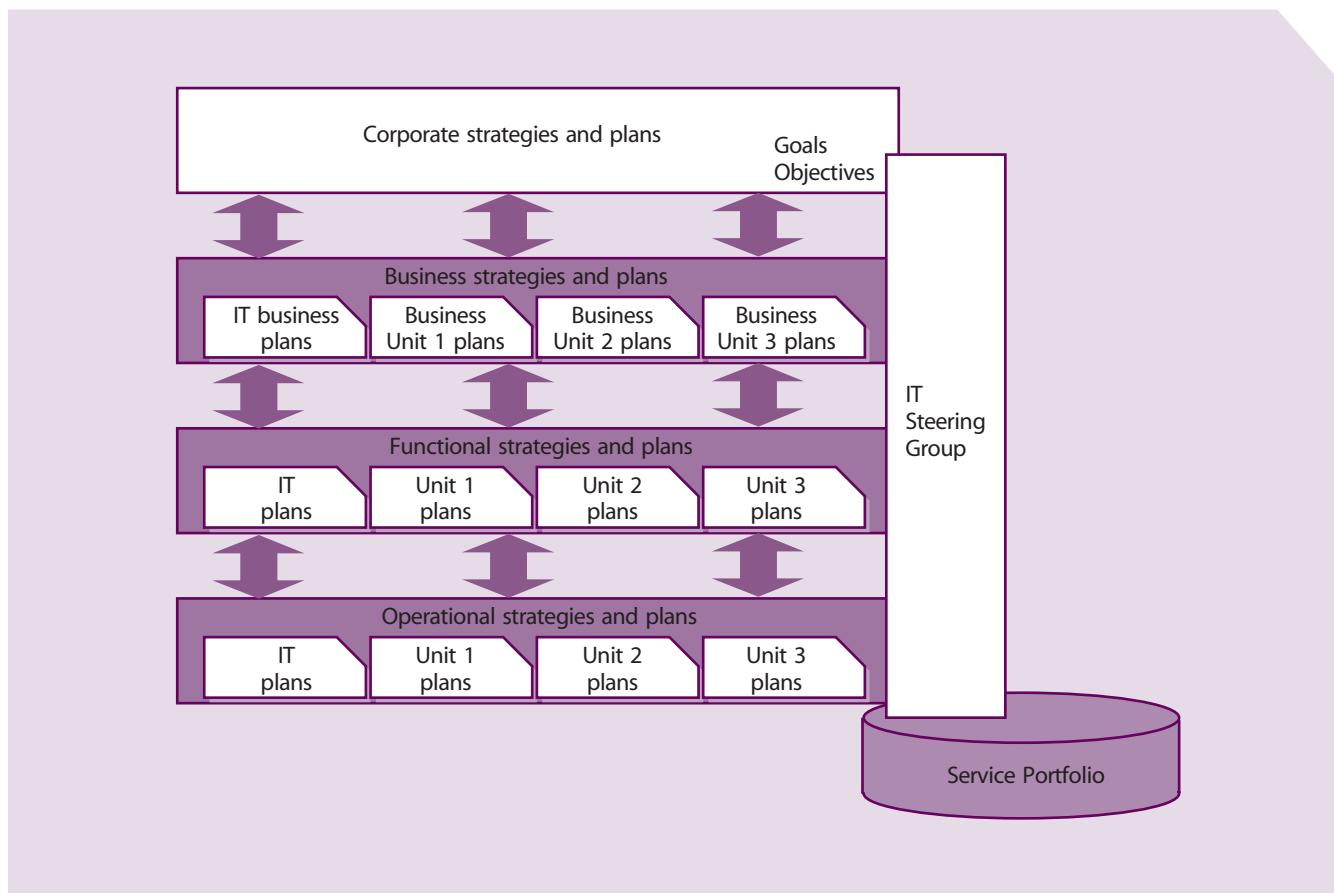


Figure 2.5 The IT Steering/Strategy Group

- **Business/IT strategy review:** to discuss major changes to business strategy and major proposed changes to IT strategy and technology, to ensure continued alignment
- **Business Continuity and IT Service Continuity:** the group, or a working party from the group, is responsible for aligning Business Continuity and IT Service Continuity strategies
- **Policies and standards:** the ISG is responsible for ensuring that IT policies and standards, particularly in relation to financial strategy and performance management, are in place and aligned with the overall corporate vision and objectives.

The IT Steering Group sets the direction for policies and plans from corporate to operational levels of IT organization and ensures that they are consistent with corporate level strategies. See Figure 2.5.

The ISG has an important role to play in the alignment of business and IT strategies and plans as illustrated in Figure 2.5. As can be seen, the Service Portfolio is a key source of input to the ISG in its decision-making role, which enables the ISG to:

- Direct and steer the selection of investment in those areas that yield the greatest business value and return on investment
- Perform effective programme and project selection, prioritization and planning
- Exercise effective ongoing governance and active management of the 'pipeline' of business requirements
- Ensure that the projected business benefits of programmes and projects are realized.

2.4.3 Value to business

With good Service Design, it is possible to deliver quality, cost-effective services and to ensure that the business requirements are being met.

The following benefits result from good Service Design practice:

- **Reduced Total Cost of Ownership (TCO):** cost of ownership can only be minimized if all aspects of services, processes and technology are designed properly and implemented against the design
- **Improved quality of service:** both service and operational quality will be enhanced

- **Improved consistency of service:** as services are designed within the corporate strategy, architectures and constraints
- **Easier implementation of new or changed services:** as there is integrated and full Service Design and the production of comprehensive SDPs
- **Improved service alignment:** involvement from the conception of the service, ensuring that new or changed services match business needs, with services designed to meet Service Level Requirements
- **More effective service performance:** with incorporation and recognition of Capacity, Financial Availability and IT Service Continuity Plans
- **Improved IT governance:** assist with the implementation and communication of a set of controls for effective governance of IT
- **More effective Service Management and IT processes:** processes will be designed with optimal quality and cost-effectiveness
- **Improved information and decision-making:** more comprehensive and effective measurements and metrics will enable better decision-making and continual improvement of Service Management practices in the design stage of the Service Lifecycle.

2.4.4 Optimizing design performance

The optimizing of design activities requires the implementation of documented processes, together with an overriding quality management system (such as ISO 9001) for their continual measurement and improvement. It is important that when considering the improvement and optimization of the Service Design activities, the impact of the activities on all stages of the lifecycle should be measured and not just the impact on the design stage. Therefore Service Design measurements and metrics should look at the amount of rework activity and improvement activity that is needed on transition, operation and improvement activities as a result of inadequacies within the design of new and changed service solutions. More information on measurement of Service Design can be found in section 8.5.

2.4.5 Processes within Service Design

This publication details processes required in the design phase of the Service Lifecycle. These processes cannot be considered in isolation, as their true value will only be realized when interfaces between the processes are identified and actioned. The following processes are detailed in this publication:

- **Service Catalogue Management:** to ensure that a Service Catalogue is produced and maintained, containing accurate information on all operational services and those being prepared to be run operationally
- **Service Level Management:** negotiates, agrees and documents appropriate IT service targets with representatives of the business, and then monitors and produces reports on the service provider's ability to deliver the agreed level of service
- **Capacity Management:** to ensure that cost-justifiable IT capacity in all areas of IT always exists and is matched to the current and future agreed needs of the business, in a timely manner
- **Availability Management:** to ensure that the level of service availability delivered in all services is matched to, or exceeds, the current and future agreed needs of the business, in a cost-effective manner
- **IT Service Continuity Management:** to ensure that the required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment, technical support and Service Desk) can be resumed within required, and agreed, business timescales
- **Information Security Management:** to align IT security with business security, and ensure that information security is effectively managed in all service and Service Management activities
- **Supplier Management:** to manage suppliers and the services they supply, to provide seamless quality of IT service to the business, ensuring value for money is obtained.

These are only some of the processes described in the ITIL Service Management practice guidance. All processes within the Service Management Lifecycle must be linked closely together for managing, designing, supporting and maintaining the services, IT infrastructure, environment, applications and data. Other processes are described in detail in other publications within the ITIL Service Management Practices core library. The interfaces between every process and every other process need to be clearly defined when designing a service or improving or implementing a process. These interfaces are described in detail in section 4 and include not only the interfaces to each of the Service Design processes, but also interfaces to processes within other stages of the lifecycle.

When designing a service or a process, it is imperative that all the roles are clearly defined. A trademark of high performing organizations is the ability to make the right decisions quickly and execute them quickly. Whether the decision involves a strategic choice or a critical operation, being clear on who has input, who decides and who takes action will enable the organization to move forward quickly.



3

Service Design principles

3 Service Design principles

See first that the design is wise and just: that ascertained, pursue it resolutely; do not for one repulse forego the purpose that you resolved to effect.

William Shakespeare (1564–1616)

The common mistake that people make when trying to design something completely foolproof is to underestimate the ingenuity of complete fools.

Douglas Adams

IT Service Design is a part of the overall business change process. This business change process and the role of IT are illustrated in Figure 3.1.

Once accurate information has been obtained on what is required and signed off, with regard to the changed needs of the business, the plan for the delivery of a service to meet the agreed need can be developed.

The role of the Service Design stage within this overall business change process can be defined as:

'The design of appropriate and innovative IT services, including their architectures, processes, policies and documentation, to meet current and future agreed business requirements.'

It is important that the right interfaces and links to the design activities exist. When designing new or changed services, it is vital that the entire Service Lifecycle and ITSM processes are involved from the outset. Often difficulties occur in operations when a newly designed service is handed over for live running at the last minute. The following are actions that need to be undertaken from the outset of a Service Design to ensure that the solution meets the requirements of the business:

- The new service solution should be added to the overall Service Portfolio from the concept phase, and the Service Portfolio should be updated to reflect the current status through any incremental or iterative development. This will be beneficial not only from the financial perspective, but also from all other areas during design.
- As part of the initial service/system analysis, there will be a need to understand the Service Level Requirements (SLRs) for the service when it goes live.
- From the SLRs, the Capacity Management team can model this within the current infrastructure to ascertain if this will be able to support the new service. If time allows, the results from the modelling activities can be built into the Capacity Plan.
- If new infrastructure is required for the new service, or extended support, Financial Management will need to be involved to set the budget.
- An initial Business Impact Analysis and risk assessment should be conducted on services well before implementation as invaluable input into IT Service Continuity Strategy, Availability Design and Capacity Planning.
- The Service Desk will need to be made aware of new services well in advance of live operation to prepare and train Service Desk staff and potentially IT customer staff.
- Service Transition can start planning the implementation and build into the change schedule.
- Supplier Management will need to be involved if procurement is required for the new service.

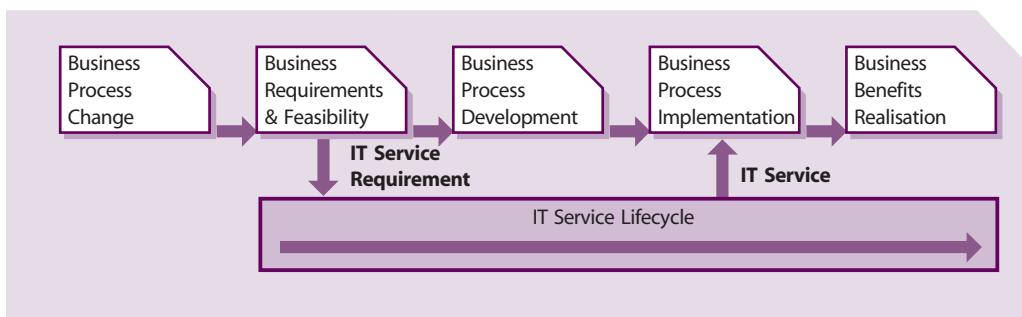


Figure 3.1 The business change process

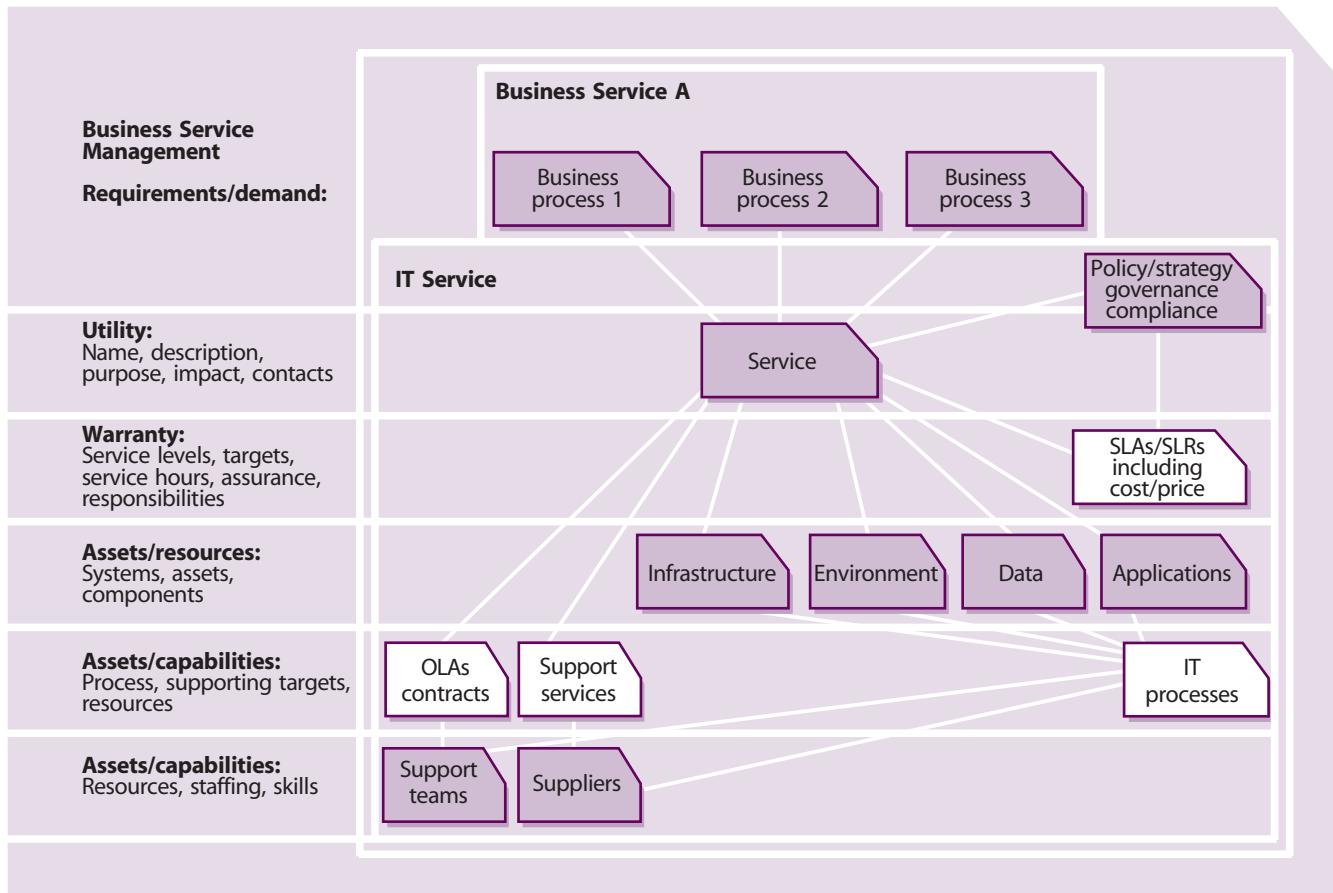


Figure 3.2 Service composition

The composition of a service and its constituent parts is illustrated in Figure 3.2.

Service Design must consider all these aspects when designing service solutions to meet new and evolving business needs:

- **Business process:** to define the functional needs of the service being provided, e.g. telesales, invoicing, orders, credit checking
- **Service:** the service itself that is being delivered to the customers and business by the service provider, e.g. e-mail, billing
- **SLAs/SLRs:** the documents agreed with the customers that specify the level, scope and quality of service to be provided
- **Infrastructure:** all of the IT equipment necessary to deliver the service to the customers and users, including servers, network circuits, switches, PCs, telephones

- **Environment:** the environment required to secure and operate the infrastructure, e.g. data centres, power, air conditioning
- **Data:** the data necessary to support the service and provide the information required by the business processes, e.g. customer records, accounts ledger
- **Applications:** all of the software applications required to manipulate the data and provide the functional requirements of the business processes, e.g. ERM, Financial, CRM
- **Support Services:** any services that are necessary to support the operation of the delivered service, e.g. a shared service, a managed network service
- **Operational Level Agreements (OLAs) and contracts:** any underpinning agreements necessary to deliver the quality of service agreed within the SLA
- **Support Teams:** any internal support teams providing second- and third-line support for any of the components required to provide the service, e.g. Unix, mainframe, networks

- **Suppliers:** any external third parties necessary to provide third- and fourth- line support for any of the components required to provide the service, e.g. networks, hardware, software.

The design activities must not just consider each of the components above in isolation, but must also consider the relationships between each of the components and their interactions and dependencies on any other components and services, in order to provide an effective and comprehensive solution that meets the business needs.

3.1 GOALS

The main goals and objectives of Service Design are to:

- Design services to satisfy business objectives, based on the quality, compliance, risk and security requirements, delivering more effective and efficient IT and business solutions and services aligned to business needs by coordinating all design activities for IT services to ensure consistency and business focus
- Design services that can be easily and efficiently developed and enhanced within appropriate timescales and costs and, wherever possible, reduce, minimize or constrain the long-term costs of service provision
- Design efficient and effective processes for the design, transition, operation and improvement of high-quality IT services, together with the supporting tools, systems and information, especially the Service Portfolio, to manage services through their lifecycle
- Identify and manage risks so that they can be removed or mitigated before services go live
- Design secure and resilient IT infrastructures, environments, applications and data/information resources and capability that meet the current and future needs of the business and customers
- Design measurement methods and metrics for assessing the effectiveness and efficiency of the design processes and their deliverables

- Produce and maintain IT plans, processes, policies, architectures, frameworks and documents for the design of quality IT solutions, to meet current and future agreed business needs
- Assist in the development of policies and standards in all areas of design and planning of IT services and processes, receiving and acting on feedback on design processes from all other areas and incorporating the actions into a continual process of improvement
- Develop the skills and capability within IT by moving strategy and design activities into operational tasks, making effective and efficient use of all IT service resources
- Contribute to the improvement of the overall quality of IT service within the imposed design constraints, especially by reducing the need for reworking and enhancing services once they have been implemented in the live environment.

3.2 BALANCED DESIGN

For any new business requirements, the design of services is a delicate balancing act, ensuring that not only the functional requirements but also the performance targets are met. All of this needs to be balanced with regard to the resources available within the required timescale and the costs for the new services. Jim McCarthy, author of *Dynamics of Software Development*, states: 'As a development manager, you are working with only three things':

- **Functionality:** the service or product and its facilities, functionality and quality, including all of the management and operational functionality required
- **Resources:** the people, technology and money available
- **Schedule:** the timescales.

These are shown in Figure 3.3.

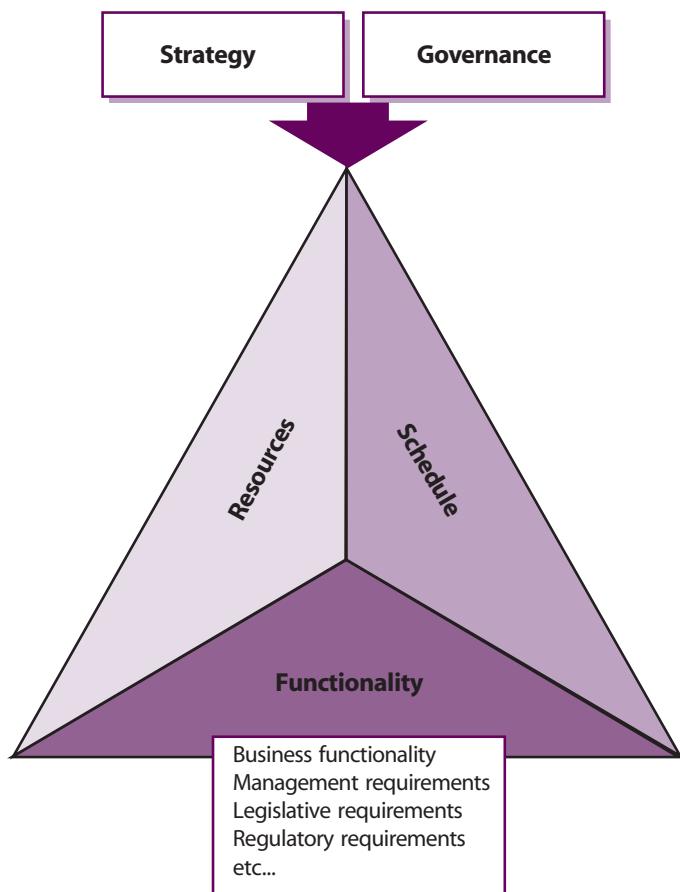


Figure 3.3 Project elements in a triangulated relationship

This concept is extremely important to Service Design activities and to the balance between the effort that is spent in the design, development and delivery of services in response to business requirements. Service Design is a delicate balancing act of all three elements and the constant dynamic adjustment of all three to meet changing business needs. Changing one side of the triangle invariably has an impact on at least one of the other sides if not both of them. It is vital therefore that the business drivers and needs are fully understood in order that the most effective business solutions are designed and delivered, using the most appropriate balance of these three elements. It is likely that business drivers and needs will change during design and delivery, due to market pressures. The functionality and resources should be considered for all stages of the Service Lifecycle, so that services are not only designed and developed effectively and efficiently, but that the effectiveness and efficiency of the service is maintained throughout all stages of its lifecycle.

Due consideration should be given within Service Design to all subsequent stages within the Service Lifecycle. Often designers and architects only consider the development of a new service up to the time of implementation of the service into the live environment. A holistic approach to

the design of IT services should be adopted to ensure that a fully comprehensive and integrated solution is designed to meet the agreed requirements of the business. This approach should also ensure that all of the necessary mechanisms and functionality are implemented within the new service so that it can be effectively managed and improved throughout its operational life to achieve all of its agreed service targets. A formal, structured approach should be adopted to ensure that all aspects of the service are addressed and ensure its smooth introduction and operation within the live environment.

The most effective IT service providers integrate all five aspects of design rather than design them in isolation. This ensures that an integrated Enterprise Architecture is produced, consisting of a set of standards, designs and architectures that satisfy all of the management and operational requirements of services as well as the functionality required by the business. This integrated design ensures that when a new or changed service is implemented, it not only provides the functionality required by the business, but also meets and continues to meet all its service levels and targets in all areas. This ensures that no (or absolute minimum) weaknesses will need to be addressed retrospectively.

In order to achieve this, the overall management of these design activities needs to ensure:

- Good communication between the various design activities and all other parties, including the business and IT planners and strategists
- The latest versions of all appropriate business and IT plans and strategies are available to all designers
- All of the architectural documents and design documents are consistent with all business and IT policies and plans
- The architectures and designs:
 - Are flexible and enable IT to respond quickly to new business needs
 - Integrate with all strategies and policies
 - Support the needs of other stages of the Service Lifecycle
 - Facilitate new or changed quality services and solutions, aligned to the needs and timescales of the business.

3.3 IDENTIFYING SERVICE REQUIREMENTS

Service Design must consider all elements of the service by taking a holistic approach to the design of a new service. This approach should consider the service and its constituent components and their inter-relationships, ensuring that the services delivered meet the functionality

and quality of service expected by the business in all areas:

- The scalability of the service to meet future requirements, in support of the long-term business objectives
- The business processes and business units supported by the service
- The IT service and the agreed business functionality and requirements
- The service itself and its Service Level Requirement (SLR) or Service Level Agreement (SLA)
- The technology components used to deploy and deliver the service, including the infrastructure, the environment, the data and the applications
- The internally supported services and components and their associated Operational Level Agreements (OLAs)
- The externally supported services and components and their associated underpinning contracts, which will often have their own related agreements and/or schedules
- The performance measurements and metrics required
- The legislated or required security levels.

The relationships and dependencies between these elements are illustrated in Figure 3.4.

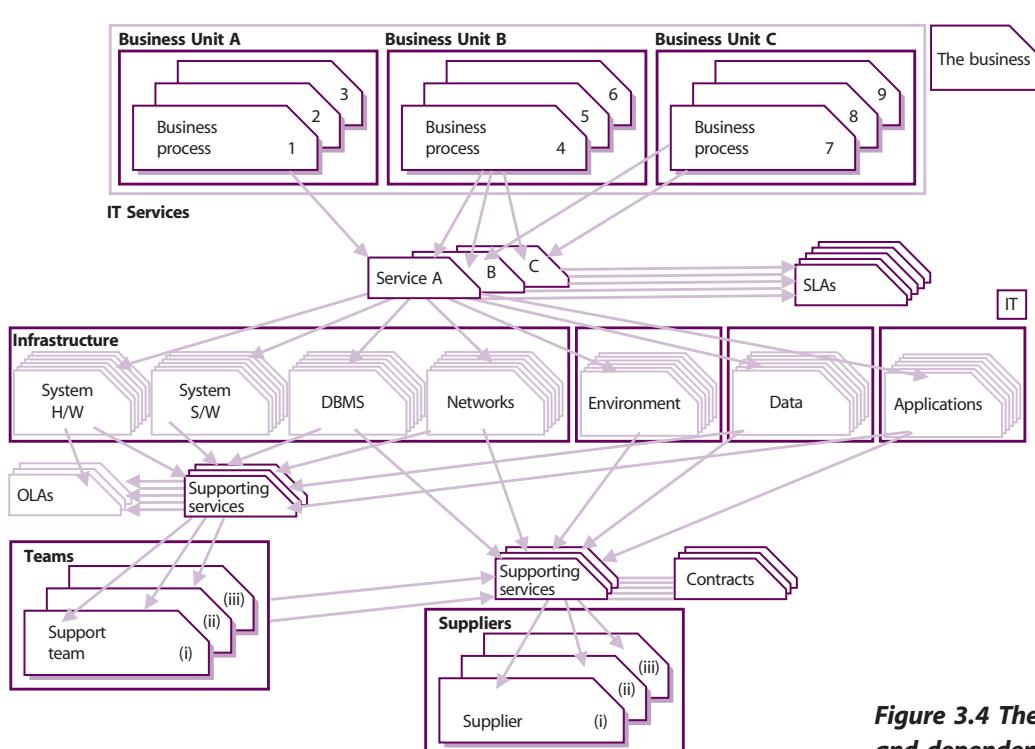


Figure 3.4 The service relationships and dependencies

No service can be designed, transitioned and operated in isolation. The relationship of each service to its supporting components and services must be clearly understood and recognized by all people within the service provider organization. It is also essential that all targets contained within supporting agreements, such as OLAs and contracts, underpin those agreed between the service provider and its customers. Some of these concepts are discussed in more detail in later sections of the publication, with respect to the individual aspects of Service Design. However, when an individual aspect of a service is changed, all other areas of the service should also be considered to ensure that any amendments necessary to support the change are included in the overall design. Increasingly, services are complex and are delivered by a number of partner or supplier organizations. Where multiple service providers are involved in delivery of a service, it is vital that a central Service Design authority is established, to ensure services and processes are fully integrated across all parties.

Within the specific area of technology there are four separate technology domains that will need to be addressed, as they are the supporting components of every service and contribute to its overall performance:

- **Infrastructure:** the management and control of all infrastructure elements, including mainframes, servers, network equipment, database systems, storage area networks (SANs), network-attached storage (NAS), systems software, utilities, backup systems, firewalls, development and test environments, management tools, etc.
- **Environmental:** the management and control of all environmental aspects of all major equipment rooms, including the physical space and layout, power, air conditioning, cabling, physical security, etc.
- **Data:** the management and control of all data and information and its associated access, including test data where applicable
- **Applications:** the management and control of all applications software, including both bought-in applications and in-house developed applications software.

3.4 IDENTIFYING AND DOCUMENTING BUSINESS REQUIREMENTS AND DRIVERS

IT must retain accurate information on business requirements and drivers if it is to provide the most appropriate catalogue of services with an acceptable level of service quality that is aligned to business needs. Business drivers are the people, information and tasks that

support the fulfilment of business objectives. This requires that IT develops and maintains close, regular and appropriate relationships and exchange of information in order to understand the operational, tactical and strategic requirements of the business. This information needs to be obtained and agreed in two main areas to maintain service alignment:

- **Information on the requirements of existing services** – what changes will be required to existing services with regard to:
 - New facilities and functionality requirements
 - Changes in business processes, dependencies, priorities, criticality and impact
 - Changes in volumes of service transactions
 - Increased service levels and service level targets due to new business driver, or reduced for old services, lowering priority for those due for replacement
 - Additional needs for Service Management information.
- **Information on the requirements of new services:**
 - Facilities and functionality required
 - Management information required and management needs
 - Business processes supported, dependencies, priorities, criticality and impact
 - Business cycles and seasonal variations
 - Service level requirements and service level targets
 - Business transaction levels, service transaction levels, numbers and types of users and anticipated future growth
 - Business justification, including the financial and strategic aspects
 - Predicted level of change, e.g. known future business requirements or enhancement
 - Level of business capability or support to be provided, e.g. local business-based support.

This collection of information is the first and most important stage for designing and delivering new services or major changes to existing services. The need for accurate and representative information from the business is paramount. This must be agreed and signed off with senior representatives within the business. If incorrect or misleading information is obtained and used at this stage, then all subsequent stages will be delivering services that do not match the needs of the business. Also, there must be some formal process for the agreement and acceptance of changes to the business requirements, as these will often change and evolve during the Service

Lifecycle. The requirements and the design must evolve with the changing business environment to ensure that the business expectations are met. However, this must be a carefully managed process to ensure that the rate of change is kept at an agreed and manageable level, and does not 'swamp' and excessively delay the project or its implementation.

In order to design and deliver IT services that meet the needs of the customers and the business, clear, concise, unambiguous specifications of the requirements must be documented and agreed. Time spent in these activities will prevent issues and discussion from arising later with regard to variances from customer and business expectation. This business requirements stage should consist of:

- Appointment of a project manager, the creation of a project team and the agreement of project governance by the application of a formal, structured project methodology
- Identification of all stakeholders, including the documentation of all requirements from all stakeholders and stakeholder benefits they will obtain from the implementation
- Requirements analysis, prioritization, agreement and documentation
- Determination and agreement of outline budgets and business benefits. The budget must be committed by management, because it is normal practice to decide next year's budget in the last quarter of the previous year, so any plans must be submitted within this cycle
- Resolution of the potential conflict between business units and agreement on corporate requirements
- Sign-off processes for the agreed requirements and a method for agreeing and accepting changes to the agreed requirements. Often the process of developing requirements is an iterative or incremental approach that needs to be carefully controlled to manage 'scope creep'
- Development of a customer engagement plan, outlining the main relationships between IT and the business and how these relationships and necessary communication to wider stakeholders will be managed.

Where service requirements are concerned, they sometimes come with a price tag (which might not be entirely known at this stage), so there always needs to be a balance between the service achievable and the cost. This may mean that some requirements may be too costly to include and may have to be dropped during the financial assessment involved within the design process.

If this is necessary, all decisions to omit any service requirements from the design of the service must be documented and agreed with the representatives of the business. There is often a difficulty when what the business wants and the budget allocated for the solution do not take into account the full service costs, including the ongoing costs.

3.5 DESIGN ACTIVITIES

All design activities are triggered by changes in business needs or service improvements. A structured and holistic approach to the design activities should be adopted, so that all available information is considered to ensure consistency and integration is achieved throughout the IT service provider organization, within all design activities.

Key message

Architectures and designs should be kept, clear, concise, simple and relevant. All too often, designs and architectures are complex and theoretical and do not relate to the 'real world'.

The main problem today is that organizations often only focus on the functional requirements. A design or architecture by definition needs to consider all design aspects. It is not a smaller organization that combines these aspects, it is a sensible one.

The design processes activities are:

- Requirements collection, analysis and engineering to ensure that business requirements are clearly documented and agreed
- Design of appropriate services, technology, processes, information and process measurements to meet business requirements
- Review and revision of all processes and documents involved in Service Design, including designs, plans, architectures and policies
- Liaison with all other design and planning activities and roles, e.g. solution design
- Production and maintenance of IT policies and design documents, including designs, plans, architectures and policies
- Revision of all design documents, and planning for the deployment and implementation of IT strategies using 'roadmaps', programmes and project plans
- Risk assessment and management of all design processes and deliverables
- Ensuring alignment with all corporate and IT strategies and policies.

The inputs to the various design activities are:

- Corporate visions, strategies, objectives, policies and plans, business visions, strategies, objectives and plans, including Business Continuity Plans (BCPs)
- Constraints and requirements for compliance with legislated standards and regulations
- IT strategies and strategic documents (from Service Strategy):
 - All IT strategies, policies and strategic plans
 - Details of business requirements
 - All constraints, financial budgets and plans
 - The Service Portfolio
 - Service Management visions, strategies, policies, objectives and plans
 - IT and Service Management processes, risks and issues registers
 - Service Transition plans (Change, Configuration and Release and Deployment Management Plans)
 - Security policies, handbooks and plans
 - The procurement and contract policy, supplier strategy and Supplier Management processes
 - The current staff knowledge, skills and capability
 - IT business plans, Business and IT Quality Plans and policies
 - Service Management plans, including Service Level Management Plans, SLAs and SLRs, Service Improvement Plan (SIP), Capacity Plans, Availability Plans, IT Service Continuity Plans
- Measurement tools and techniques.

The deliverables from the design activities are:

- Suggested revisions to IT strategies and policies
- Revised designs, plans and technology and management architectures, including:
 - The IT infrastructure and infrastructure management and environmental strategy, designs, plans, architectures and policies
 - The applications and data strategies, designs, plans, architectures and policies
- Designs for new or changed services, processes and technologies
- Process review and analysis reports, with revised and improved processes and procedures
- Revised measurement methods and processes
- Managed levels of risk, and risk assessment and management reports

- Business cases and feasibility studies, together with Statements of Requirements (SORs) and Invitations to Tender (ITTs)
- Comments and feedback on all other plans
- Business benefit and realization reviews and reports.

3.6 DESIGN ASPECTS

An overall, integrated approach should be adopted for the design activities documented in the previous section and should cover the design of:

- Service solutions, including all of the functional requirements, resources and capabilities needed and agreed
- Service Management systems and tools, especially the Service Portfolio for the management and control of services through their lifecycle
- Technology architectures and management architectures and tools required to provide the services
- Processes needed to design, transition, operate and improve the services
- Measurement systems, methods and metrics for the services, the architectures and their constituent components and the processes.

The key aspect is the design of new or changed service solutions to meet changing business needs. Every time a new service solution is produced, it needs to be checked against each of the other aspects to ensure that it will integrate and interface with all of the other services already in existence. These five aspects of Service Design are covered in more detail in the following sections. The plans produced by Service Design for the design, transition and subsequent operation of these five different aspects should include:

- The approach taken and the associated timescales
- The organizational impact of the new or changed solution on both the business and IT
- The commercial impact of the solution on the organization, including the funding, costs and budgets required
- The technical impact of the solution and the staff and their roles, responsibilities, skills, knowledge, training and competences required to deploy, operate, maintain and optimize the new solution to the business
- The commercial justification assessment of the impact of the solution on existing business – this impact must be assessed from the point of view of IT and Service Management processes, including both their capacity and performance

- The assessment and mitigation of risks to services, processes and Service Management activities
- Communication planning and all aspects of communication with all interested parties
- The impact of the solution on new or existing contracts or agreements
- The expected outcomes from the operation of the new or changed service in measurable terms, generally expressed within new or existing Service Level Agreements (SLAs), service levels and customer satisfaction
- The production of a Service Design Package (see Appendix A) containing everything necessary for the subsequent testing, introduction and operation of the solution or service
- The production of a set of Service Acceptance Criteria (SAC) (see Appendix B) that will be used to ensure that the service provider is ready to deliver and support the new or changed service in the live environment.

3.6.1 Designing service solutions

There are many activities that have to be completed within the Service Design stage for a new or changed service. A formal and structured approach is required to produce the new service at the right cost, functionality, quality and within the right time frame. This process and its constituent stages are illustrated in Figure 3.5, together with the other major areas that will need to be involved within the process. This process must be iterative/incremental to ensure that the service delivered meets the evolving and changing needs of the business during the business process development and the IT Service Lifecycle. Additional project managers and project teams may need to be allocated to manage the stages within the lifecycle for the deployment of the new service.

The role of the project team within this activity of delivering new and changing IT services to the business and its relationship to design activities is illustrated in Figure 3.5.

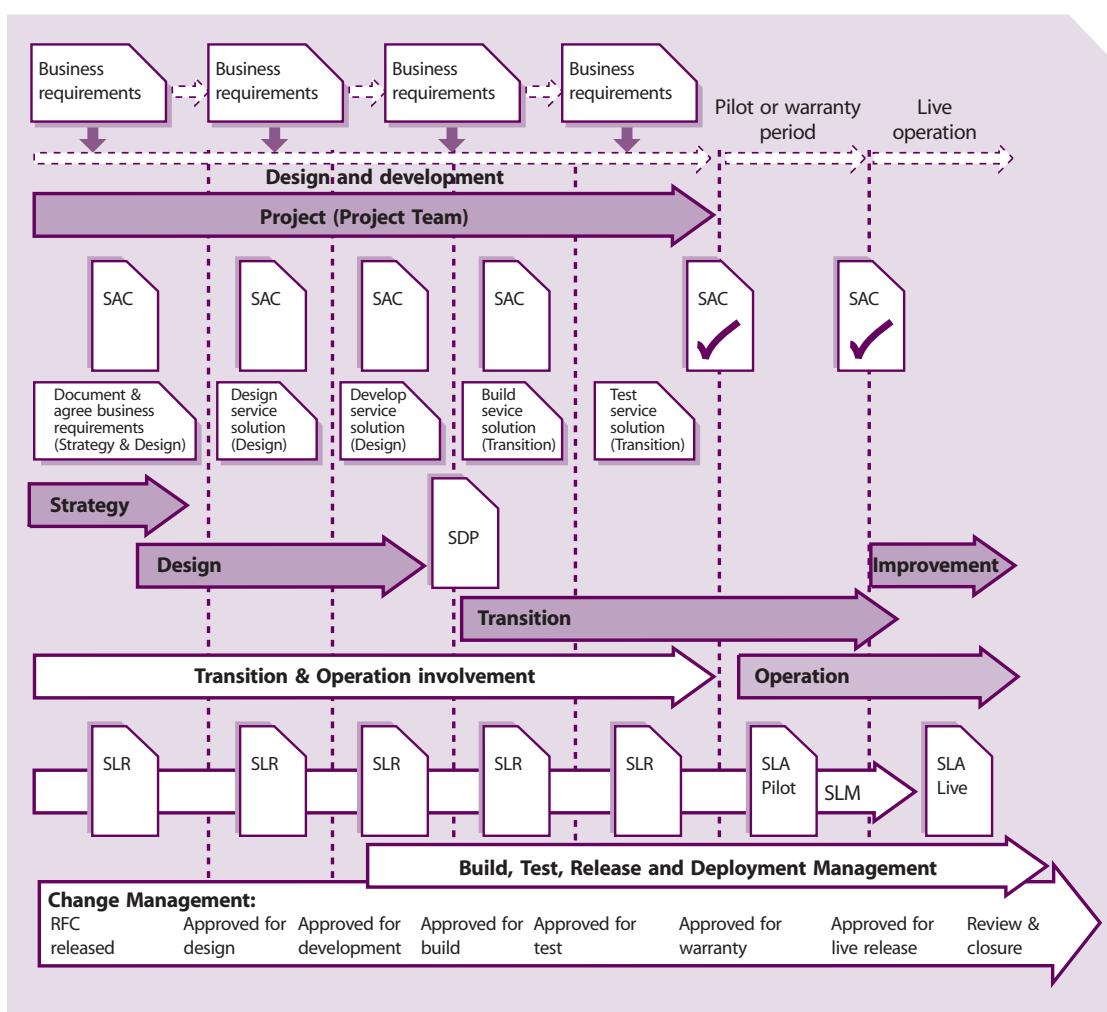


Figure 3.5 Aligning new services to business requirements

Figure 3.5 shows the lifecycle of a service from the initial or changed business requirement through the design, transition and operation stages of the lifecycle. It is important that there is effective transfer of knowledge at all stages between the operational staff and the project staff to ensure smooth progression through each of the stages illustrated.

The areas that need to be considered within the design of the service solution should include:

- Analyse the agreed business requirements
- Review the existing IT services and infrastructure and produce alternative service solutions, with a view to re-using or exploiting existing components and services wherever possible
- Design the service solutions to the new requirements, including their constituent components, in terms of the following, and document this design:
 - The facilities and functionality required, and information required for the monitoring of the performance of the service or process
 - The business processes supported, dependencies, priorities, criticality and impact of the service, together with the business benefits that will be delivered by the service
 - Business cycles and seasonal variations, and the related business transaction levels, service transaction levels, the numbers and types of users and anticipated future growth, and the business continuity requirements
 - Service Level Requirements and service level targets and the necessary service measuring, reporting and reviewing activities
 - The timescales involved and the planned outcomes from the new service and the impact on any existing services
 - The requirements for testing, including any User Acceptance Testing (UAT) and responsibilities for managing the test results
- Ensure that the contents of the Service Acceptance Criteria (SAC) are incorporated and the required achievements planned into the initial design
- Evaluate and cost alternative designs, highlighting advantages as well as disadvantages of the alternatives
- Agree the expenditure and budgets
- Re-evaluate and confirm the business benefits, including the Return on Investment (RoI) from the service, including identification and quantification of all service costs and all business benefits and increased revenues. The costs should cover the Total Cost of Ownership (TCO) of the service and include

start-up costs such as design costs, transition costs, project budget, and all ongoing operational costs, including management, support and maintenance

- Agree the preferred solution and its planned outcomes and targets (Service Level Requirement (SLR))
- Check the solution is in balance with all corporate and IT strategies, policies, plans and architectural documents. If not, revise either the solution or the strategic documentation (taking into account the effect on other strategic documents, services and components) wherever possible re-using or exploiting existing components (e.g. software objects, 'corporate' data, hardware), unless the strategy dictates otherwise. The changing of strategy will involve a significant amount of work and would be done in conjunction with Service Strategy
- Ensure that all of the appropriate corporate and IT governance and security controls are included with the solution
- Complete an IT 'organizational readiness assessment' to ensure that the service can be effectively operated to meet its agreed targets and that the organization has the appropriate capability to deliver to the agreed level. This will include:
 - The commercial impact on the organization from both a business and IT perspective, including all of the business benefits and all of the costs (both one-off project costs and the ongoing annual operation costs) involved in the design, development and ongoing operation and support of the service
 - Assessment and mitigation of the risks associated with the new or changed service, particularly with regard to the operation, security, availability and continuity of the service
 - The business capability and maturity. This activity should be performed by the business itself to ensure that all of the right processes, structure, people, roles, responsibilities and facilities are in place to operate the new service
 - The IT capability and maturity:
 - The environment and all areas of technology, having considered the impact on existing components of the infrastructure and existing services
 - The IT organizational structure and the roles and responsibilities
 - The IT processes and their documentation
 - The skills, knowledge and competence of the staff

- The IT management processes and supporting tools
- The supplier and supporting agreements necessary to maintain and deliver the service
- The assembly of a Service Design Package (SDP) for the subsequent transition, operation and improvement of the new or changed service solution.

3.6.2 Designing supporting systems, especially the Service Portfolio

The most effective way of managing all aspects of services through their lifecycle is by using appropriate management systems and tools to support and automate efficient processes. The Service Portfolio is the most critical management system used to support all processes and describes a provider's services in terms of business value. It articulates business needs and the provider's response to those needs. By definition, business value terms correspond to market terms, providing a means for comparing service competitiveness across alternative

providers. By acting as the basis of a decision framework, a service portfolio either clarifies or helps to clarify the following strategic questions:

- Why should a customer buy these services?
- Why should they buy these services from you?
- What are the pricing or chargeback models?
- What are my strengths and weaknesses, priorities and risk?
- How should my resources and capabilities be allocated?

See Figure 3.6. Ideally the Service Portfolio should form part of a comprehensive Service Knowledge Management System (SKMS) and registered as a document in the Configuration Management System (CMS). Further information is provided on both the CMS and the SKMS within the Service Transition publication.

Figure 3.6 is a depiction of the relationship of the Service Portfolio with the SKMS.

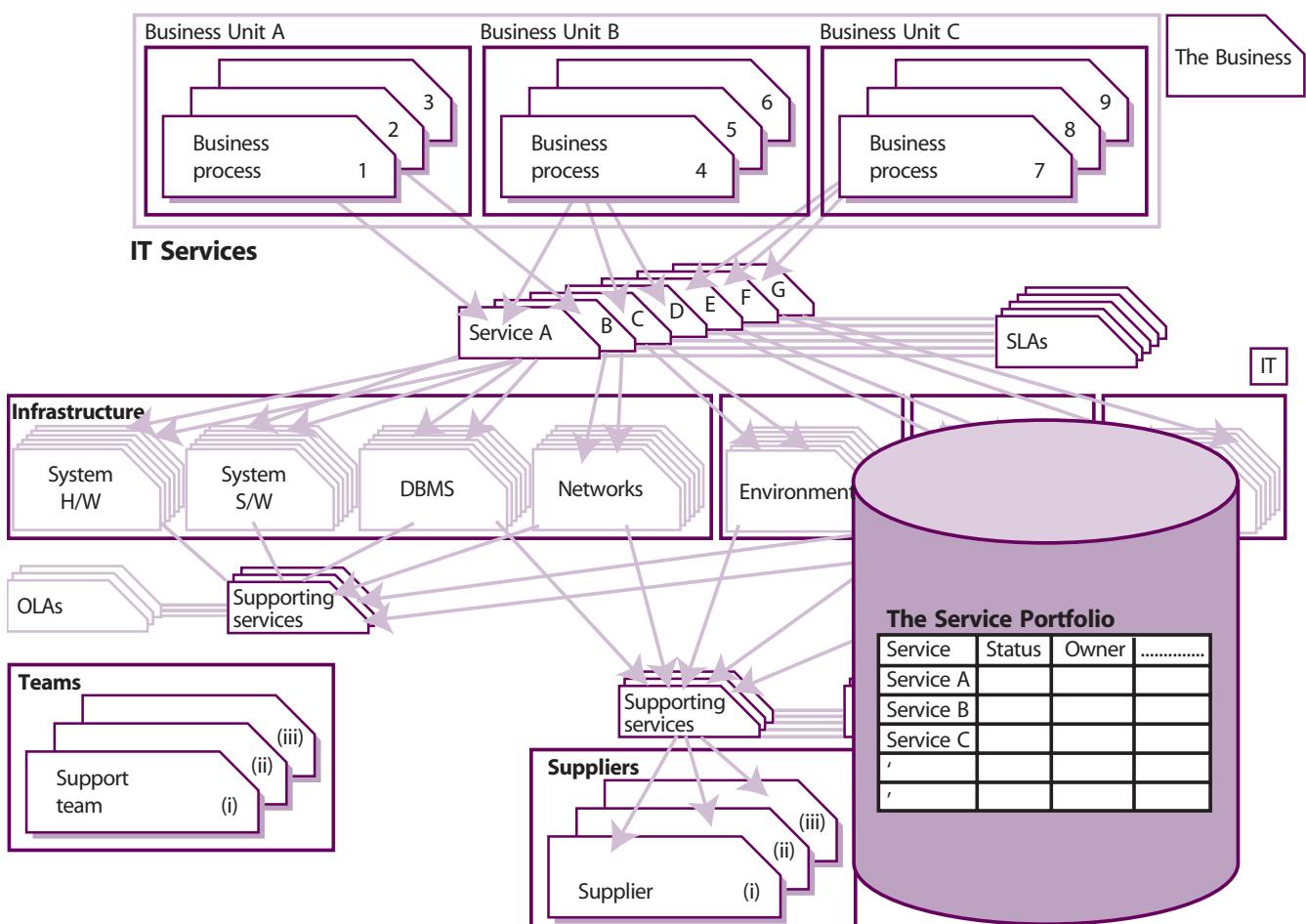


Figure 3.6 The Service Portfolio – a central repository

Once a strategic decision to charter a service is made, this is the stage in the Service Lifecycle when Service Design begins architecting the service, which will eventually become part of the Service Catalogue. The Service Portfolio should contain information relating to every service and its current status within the organization. The options of status within the Service Portfolio should include:

- **Requirements:** a set of outline requirements have been received from the business or IT for a new or changed service
- **Defined:** the set of requirements for the new service are being assessed, defined and documented and the SLR is being produced
- **Analysed:** the set of requirements for the new service are being analysed and prioritized
- **Approved:** the set of requirements for the new service have been finalized and authorized
- **Chartered:** the new service requirements are being communicated and resources and budgets allocated

- **Designed:** the new service and its constituent components are being designed – and procured, if required
- **Developed:** the service and its constituent components are being developed or harvested, if applicable
- **Built:** the service and its constituent components are being built
- **Test:** the service and its constituent components are being tested
- **Released:** the service and its constituent components are being released
- **Operational:** the service and its constituent components are operational within the live environment
- **Retired:** the service and its constituent components have been retired.

The Service Portfolio would therefore contain details of all services and their status with respect to the current stage within the Service Lifecycle, as illustrated in Figure 3.7.

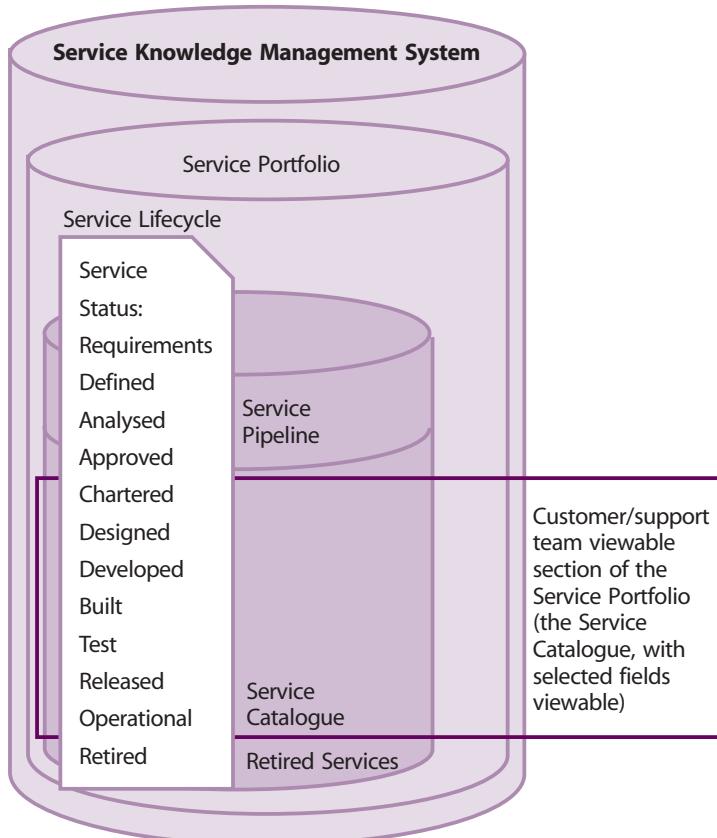


Figure 3.7 The Service Portfolio and its contents

Customers and users would only be allowed access to those services within the Service Portfolio that were of a status between 'chartered' and 'operational', as illustrated by the box in Figure 3.7, i.e. those services contained within the Service Catalogue. Service Strategy and Service Design personnel would need access to all records within the Service Portfolio, as well as other important areas such as Change Management. Other members of the service provider organization would have access to a permitted subset of the records within the Service Portfolio. Although the Service Portfolio is designed by Service Design, it is owned and managed by Service Strategy within the Service Portfolio Management process. Full details on Service Portfolio Management are discussed in the Service Strategy publication.

The Service Pipeline is a subset of the overall Service Portfolio and contains details of all of the business requirements that have not yet become services released to the live environment. It is used as a basis for the definition, analysis, prioritization and approval, by the ISG and Service Strategy, of all requests for new or changed services, to ensure that new and changed services are aligned to business requirements. It will principally be used as input to the activities of the Service Strategy and Service Design stages of the Service Lifecycle. It also provides valuable input to the activities of the Service Transition stage of the lifecycle in determining the services to be released. The Service Catalogue Management process must ensure that all of the details within the Service Portfolio are accurate and up-to-date as the requirement and its new or changed service is migrated into the live environment. This will involve close liaison with all Service Transition activities.

Various elements of the same service can have different statuses at the same time. Otherwise the Service Portfolio would be unable to support 'incremental and iterative' development. Each organization should carefully design its Service Portfolio, the content and the access allowed to the content. The content should include:

- Service name
- Service description
- Service status
- Service classification and criticality
- Applications used
- Data and/or data schema used
- Business processes supported
- Business owners
- Business users
- IT owners

- Service warranty level, SLA and SLR references
- Supporting services
- Supporting resources
- Dependent services
- Supporting OLAs, contracts and agreements
- Service costs
- Service charges (if applicable)
- Service revenue (if applicable)
- Service metrics.

The Service Portfolio is the main source of information on the requirements and services and needs to be very carefully designed to meet all the needs of all its users. The design of the Service Portfolio needs to be considered in the same way as the design of any other IT service to ensure that it meets all of these needs. This approach should also be used for all of the other Service Management information systems, including the:

- Service Knowledge Management System (SKMS)
- Configuration Management System (CMS)
- Service Desk system
- Capacity Management Information System (CMIS)
- Availability Management Information System (AMIS)
- Security Management Information System (SMIS)
- Supplier and Contracts Database (SCD).

3.6.3 Designing technology architectures

The architectural design activities within an IT organization are concerned with providing the overall strategic 'blueprints' for the development and deployment of an IT infrastructure – a set of applications and data that satisfy the current and future needs of the business. Although these aspects underpin the delivery of quality IT services, they alone cannot deliver quality IT services, and it is essential that the people, process and partner/supplier aspects surrounding these technological components (products) are also considered.

'Architecture' is a term used in many different contexts. In this context it is defined as:

The fundamental organization of a system, embodied in its components, their relationships to each other and to the environment, and the principles guiding its design and evolution.

'System' in this definition is used in the most general, not necessarily IT, sense:

'a collection of components organized to accomplish a specific function or set of functions'.

So the system could be, for example, a whole organization, a business function, a product line or an information system. Each of these systems will have an 'architecture' as defined earlier, made up of the components of the system, the relationships between them (such as control interfaces and data exchanges), the relationships between the system and its environment (political, organizational, technological, etc.) and the design principles that inform, guide and constrain its structure and operation, as well as its future development.

In essence, architectural design can be defined as:

'The development and maintenance of IT policies, strategies, architectures, designs, documents, plans and processes for the deployment and subsequent operation and improvement of appropriate IT services and solutions throughout an organization.'

The work of architectural design needs to assess and reconcile many types of needs, some of which may be in conflict with one another. The work should ensure that:

- The IT infrastructures, environments, data, applications and external services serve the needs of the business, its products and services. This activity not only includes the technology components but also the management of them
- The right balance is struck between innovation, risk and cost whilst seeking a competitive edge, where desired by the business
- There is compliance with relevant architectural frameworks, strategies, policies, regulations and standards

- A coordinated interface is provided between IT designers and planners, strategists, business designers and planners.

The architectural design activities should use input from the business, Service Strategy, its plans, designers and planners to develop appropriate designs, plans, architectures and policies for all areas of IT. These designs, plans, architectures and policies should cover all aspects of IT, including roles and responsibilities, services, technology, architecture and frameworks, processes and procedures, partners and suppliers and management methods. The architectural design process must also cover all areas of technology, including the infrastructure, environment, applications and data and be closely linked to the overall business planning and design processes.

Any enterprise is a complex system, with many types of components including its staff, business functions and processes, organizational structure and physical distribution, information resources and information systems, financial and other resources including technology, and the strategies, plans, management, policies and governance structures that drive the enterprise. An Enterprise Architecture should show how all these components (and others) are integrated in order to achieve the business objectives, both now and in the future.

The complete Enterprise Architecture can be large and complex. Here we are interested in those architectures concerned with the business of the organization and the information systems that support it. Each of these architectures calls on distinct architectural disciplines and areas of expertise, as illustrated in Figure 3.8.

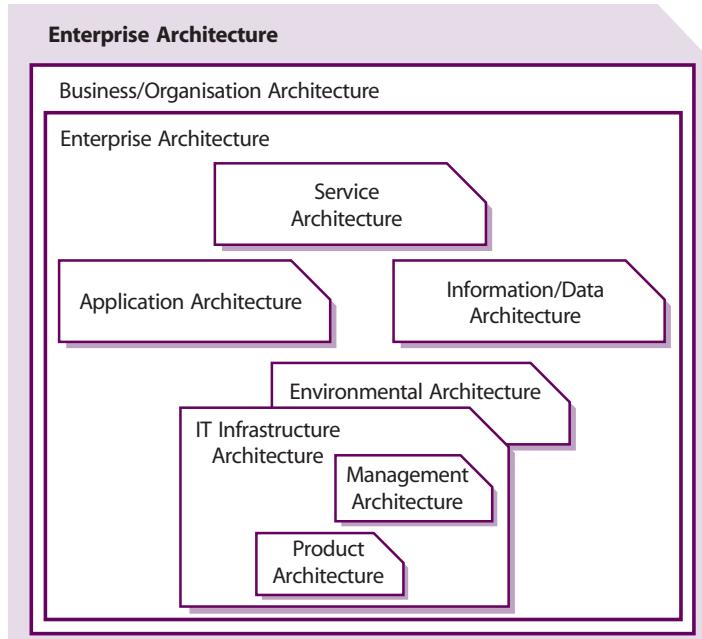


Figure 3.8 Enterprise Architecture

Enterprise Architecture is defined by Gartner as:

'the process of translating business vision and strategy into effective enterprise change, by creating, communicating and improving key principles and models that describe the enterprise's future states and enable its evolution'.

There are many proprietary and non-proprietary frameworks for the development of an Enterprise Architecture, as illustrated in Table 3.1.

These frameworks include descriptions of the organizational structure, business processes, planning and control systems, management and governance mechanisms, policies and procedures of the enterprise. They show how these components interoperate and contribute to the achievement of business goals and objectives, and provide the basis for identifying the requirements for information systems that support these business processes.

Table 3.1 Enterprise Architecture frameworks

Full framework name	Framework acronym
Architecture of Integrated Information Systems Framework	ARIS
Bredemeyer Framework	Bredemeyer
Business Transformation Enablement Programme Transformation Framework	BTEP
Command, Control, Communications, Computers Intelligences Surveillance and Reconnaissance	C4ISR
CSC Catalyst	Catalyst
Computer Integrated Manufacturing Open Systems Architecture	CIMOSA
Enterprise Architecture Framework	Gartner
Enterprise Architecture Planning	EAP
Extended Enterprise Architecture Framework	E2AF
FEA Reference Models	FEA
Generalized Enterprise Reference Architecture and Methodology	GERAM
Integrated Architecture Framework	IAF
Pillars of EA	Forrester
Reference Model for Open Distributed Processing	RM-ODP
Technical Architectural Framework Information Management	TAFIM
Treasury Enterprise Architecture Framework	TEAF
TOGAF Technical Reference Model	TOGAF
Zachman Framework	Zachman

The Enterprise Architecture should be an integrated element of the Business Architecture and should include the following major areas:

- **Service Architecture**, which translates applications, infrastructure, organization and support activities into a set of services. The Service Architecture provides the independent, business integrated approach to delivering services to the business. It provides the model for making a distinction between the Service Architecture, the Application Architecture, the Data Architecture and the Infrastructure Architecture. It also provides fault tolerance, future proofing and security controls. This means that, potentially, changes occurring within any technology architectures will be transparent to the users of the service – for example, web-based self-service delivery mechanisms. It should include not just the services themselves and their overall integration, but also the management of those services.
- **Application Architecture**, which provides a blueprint for the development and deployment of individual applications, maps business and functional requirements on to applications, and shows the inter-relationships between applications. Emerging Application Architectures are likely to be component-based. Such an approach maximizes re-use and helps to maintain flexibility in accommodating changes in sourcing policy.
- **Data/Information Architecture**, which describes the logical and physical data assets of the enterprise and the data management resources. It shows how the

information resources are managed and shared for the benefit of the enterprise. A strategy on centralized versus distributed data will almost certainly have been devised as part of such an architecture.

The Data/Information Architecture will include consideration of data warehousing technologies that facilitate the exploitation of corporate information assets. It will increasingly cover content management and the facilities for delivery of information over multiple channels.

- **IT Infrastructure Architecture**, which describes the structure, functionality and geographical distribution of the hardware, software and communications components that underpin and support the overall architecture, together with the technical standards applying to them. This should also include a 'Product Architecture' that describes the particular proprietary products and industry standards that the enterprise uses to implement the infrastructure in conformance with the IT Infrastructure Architecture principles
- **Environmental Architecture**, which describes all aspects, types and levels of environment controls and their management. An illustration of the type of environmental information required is included in Appendix E.

The relationships between these architectural perspectives can be seen in Figure 3.9. The development, documentation and maintenance of business and IT architectures will typically form part of the processes of strategic thinking and strategy development in the organization.

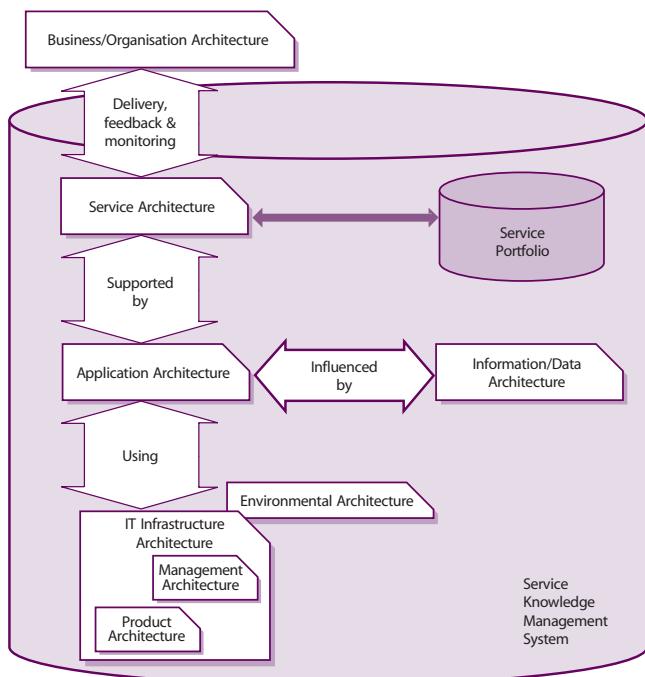


Figure 3.9 Architectural relationships

Within the framework described earlier, it is possible to identify (at least) three architectural roles. These could all report to a senior 'Enterprise Architect' in the organization:

- **Business/Organizational Architect:** concerned with business models, business processes and organizational design – the structural and functional components of the organization and their relationship, and how the business functions and activities of the organization are distributed among them; also the governance of the organization and the roles and responsibilities required
- **Service Architect** (often separate roles of Applications Architect and Information/Data Architect): concerned with the Service, Data and Application Architectures – the logical architectures supporting the business and the relationships between them
- **IT Infrastructure Architect:** concerned with the physical technology model, the infrastructure components and their relationships, including choices of technologies, interfaces and protocols, and the selection of products to implement the infrastructure.

In some organizations, the roles of Business/Organizational Architect, Information Systems Architect (or possibly separate roles of Applications Architect and Data Architect) and IT Infrastructure Architect will be separate functions. In others, some or all of the roles may be combined. The roles may reside in separate parts of the organization or even outside it. For example:

- The Business/Organizational Architect role may reside within the Business Strategy and Planning function in the corporate HQ
- The Service Architect role may form part of an internal function with responsibility for handling relationships between the business, external suppliers and IT partners relating to Service issues. A key responsibility of such a function is the maintenance of the Service Architecture. This function may be within an IT function or within the business side of an organization
- The IT Infrastructure Architect role may reside with the service provider/partner who is responsible for producing the IT Infrastructure Architecture used for the delivery of IT services to the organization.

If the necessary architectures are in place, then the role of Service Design is affected in the following ways:

- Must work within the agreed architectural framework and standards
- Will be able to re-use many of the assets created as part of the architecture
- Should work closely with all three architectural roles to

ensure maximum benefit from the work done in creating the architecture.

If architecture design is to be accomplished effectively and economically, the documents, processes and activities of the business and architectural design should be closely coordinated and synchronized. A list of these design documents and their content is contained in Appendices C and D. The individual details of technology included within architectural design are considered in the following sections.

Key message:

The real benefit and Rol of the Enterprise Architecture comes not from the architecture itself, but from the ability of an organization to design and implement projects and solutions in a rapid and consistent manner.

3.6.3.1 Technology Management

A strategic approach should be adopted with regard to the planning of an information technology and its management. This implies creating 'architectures' or 'blueprints' for the long-term framework of the technology used and planned. IT planners, designers and architects need to understand the business, the requirements and the current technology in order to develop appropriate IT architectures for the short, medium and long term.

Technology design also needs to take account of the likely IT services that it will underpin, or at least the types of service from an understanding of the business and its future direction, because the business will demand IT services, and they will need an appropriate technology to provide and deliver those services. If it is possible to provide a longer-term technology, which can underpin a number of IT services, then taking a strategic approach will provide benefit in the longer term.

Architectures need to be developed within the major areas of technology.

Technology architectures

Architectures are needed in all areas of IT infrastructure. Where relevant they need to be developed in the following areas:

- Applications and systems software
- Information, data and data base including information security and confidentiality, data warehousing and data mining
- Infrastructure design and architecture:
 - Central server, mainframe architectures, distributed regional servers, including local file and print servers

- Data networks (LANs, MANs, WANs, protocols, etc.), internet, intranet and extranet systems
- Converged network technologies, including voice networks (PABXs, Centrex, handsets, mobiles, faxes, etc.)
- Client systems (desktop PCs, laptop PCs, mobile access devices (hand-held devices, mobile phones, palmtops, PDAs, scanners, etc.)
- Storage devices, Storage Area Networks (SANs), Network Attached Storage (NAS) including backup and recovery systems and services (servers, robots, etc.)
- Document storage, handling and management
- Specialist areas of technology such as EPOS, ATMs, scanning devices, GPS systems, etc.
- Environmental systems and equipment, including their monitoring and management.

This will result in a hierarchy of architectures, which will need to be dovetailed to construct an integrated set of technology architectures for the organization. The Infrastructure Architecture should aim to provide relatively few standardized platforms for hosting applications. It must also lay down standards for application architectures that are to be hosted in controlled data centres so that these fit in with the standardized operating, monitoring and security requirements.

Management architectures

IT must manage costs, deliver the right services at the right time, secure information assets, provide dependable service and lead the business in leveraging technologies. This requires automated procedures and management tools in order to achieve this effectively and efficiently. The selection of an appropriate management architecture is key to establishing the required level of control and automation. There are two separate approaches to developing a management architecture:

- **Selecting a proprietary management architecture:** this is based on selecting a single set of management products and tools from a single proprietary management solutions supplier. This approach will normally require less effort, will support and integrate within an overall tool architecture, but will often mean that compromises will have to be made with management functionality and facilities, which may result in gaps.
- **Selecting a 'best of breed' architecture:** this approach involves the selection of a set of 'best of breed' management tools and products from a number of management solutions suppliers and then integrating them to provide a comprehensive

management solution. This will generally require more effort in the integration of the tools into a single comprehensive management solution but will often provide greater management functionality and facilities leading to long-term cost savings.

The challenges for IT management are to coordinate and work in partnership with the business in the building of these management solutions, supporting the appropriate processes and providing the required measurements and metrics. This has to be achieved while reducing or optimizing the costs involved, particularly the annual, ongoing costs. The best way of minimizing costs is to design cleverly and carefully – for example, making best use of capacity so that additional capacity is not unnecessarily bought (with its associated ongoing costs), or designing a backup/recovery solution that doesn't require a complete additional set of infrastructure. Considerable costs can be saved by intelligent and careful design, using technology that is supportable and causes few problems in the operational environment.

The main method of realizing these goals is to design solutions that give a reduction in the overall network management and support costs, while maintaining or even improving the quality of service delivered to the business.

To gain the greatest benefit from the use of the Four Ps, organizations should determine the roles of processes and people, and then implement the tools to automate the processes, facilitating people's roles and tasks. The best way of achieving this is to develop a model or architecture based on these principles. This architecture should facilitate the implementation of a set of integrated tools and processes that support 'end-to-end' management of all areas of the technology used, ensuring that there are no gaps and no 'technical silos'.

However, IT faces a big challenge in developing and maintaining the soft skills required to perform these management roles and processes effectively. In the truly efficient organizations, these roles and processes are aligned to those of the business. This ensures that the business and IT Management processes and information have similar targets and goals. However, all too often, organizations devote insufficient time and effort to the development of the soft skills (for example, interpersonal skills, communication skills, meeting skills) necessary for the processes and the business alignment to be effectively achieved.

There are five areas that need to be considered with regard to the design of a management architecture, as illustrated in Figure 3.10.

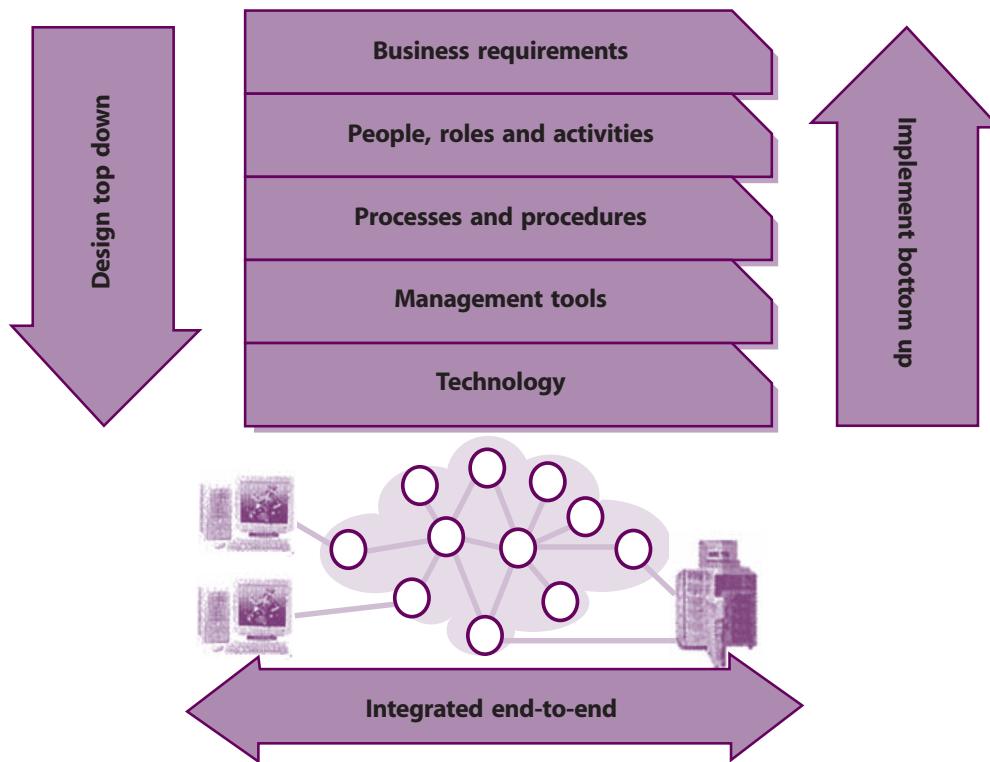


Figure 3.10 Integrated business-driven technology management

The relationships between these architectural perspectives can be seen in the diagram above. The development, documentation and maintenance of business and IT architectures will typically form part of the processes of strategic thinking and strategy development in the organization.

These five management areas to be considered can be briefly defined as:

- **Business:** the needs, requirements, processes, objectives and goals of the business units and managers within the organization
- **People:** the scope, tasks and activities of the managers and staff involved in the management of the provision of IT services
- **Processes:** the processes and procedures used to manage IT services to the business and its customers
- **Tools:** the management and support tools required to effectively manage the IT infrastructure
- **Technology:** the IT products and technology used to deliver the service and information to the right person, in the right place at the right time.

Such an architecture can be used to design and implement efficient, effective and integrated management

solutions that are aligned to the business requirements of the organization and its Business Managers. This management architecture can be applied within an organization to:

- **Design from the top down**, ensuring that the Service Management and technology management processes, tools and information are aligned with the business needs and goals
- **Implement from the bottom up**, ensuring that efficient and effective Service Management and technology management processes are fully integrated with the tools and technology in use within the organization
- **Integrate processes and tools**, ensuring greater exploitation of tools in the management and support of technology and end-to-end processes.

These bullet points are also illustrated in Figure 3.10.

The key to the development of a management architecture is to ensure that it is driven by business needs and not developed for IT needs in isolation:

Management architectures need to be:
 '... business aligned, NOT technology driven'.

Within this overall structure, a management architecture is needed that can be applied to all areas of IT Management and not just to individual isolated areas. This can then be implemented in a coordinated programme of inter-working, to provide overall end-to-end Enterprise Management so essential to the effective management of today's IT infrastructure. If only individual areas buy into the architecture, then individual 'islands of excellence' will develop and it will be impossible to provide the complete end-to-end solutions required to support today's e-business solutions.

As well as ensuring that all areas of the IT are integrated, it is vital that the management architecture is developed from the business and service perspective (i.e. 'top down'). Therefore, the key elements to agree and define before developing the management architecture are:

- Management of the business processes: What are the business processes and how do they relate to network and IT services and components?
- Management of service quality: What is service quality? How and where will it be measured?

These are the key elements that need to be determined by SLM and IT Management. They provide crucial input to the development of business-focused management architectures. All too often management tools and processes have been focused on components and component management rather than services and business processes. This needs to be changed, with emphasis clearly on the design of management systems, processes and tools that are driven by business needs and are focused on the management of business processes and IT services. If the appropriate management architecture is designed and implemented, this will allow Service Management processes to focus on managing services and service quality and operate from end-to-end across the entire IT enterprise, providing true Enterprise Service Management. This will truly facilitate the management of services to ensure that services and service quality are closely aligned to the needs of the business.

The architectures described suggest that the future of network and systems management will be less focused on the technology and become more integrated with the overall requirements of the business and IT Management. These new systems and processes are already starting to evolve as the management standards for the exchange of management information between tools become more

fully defined, by organizations such as the Distributed Management Task Force (DMTF). In essence, management systems will become:

- More focused on business needs
- More closely aligned to business processes
- Less dependent on specific technology and more 'service-centric'
- More integrated with other management tools and processes as the management standards evolve. This will involve the integration of systems management, operational management and Service Management tools and processes, with fewer 'technology silos' and 'islands of excellence'
- Part of end-to-end management systems and processes, more focused on provision of quality and customer services
- More flexible. There will be a move away from some of the more rigid, single supplier frameworks to a more open 'best-of-breed' approach.

3.6.4 Designing processes

This section provides a general introduction to process theory and practice, which is the basis for the design of ITIL processes that are used in the Service Lifecycle. A process model enables understanding and helps to articulate the distinctive features of a process.

A process is a structured set of activities designed to accomplish a specific objective. A process takes one or more inputs and turns them into defined outputs. A process includes all of the roles, responsibilities, tools and management controls required to reliably deliver the outputs. A process may also define or revise policies, standards, guidelines, activities, processes, procedures and work instructions if they are needed.

Process control can be defined as:

The activity of planning and regulating a process, with the objective of performing a process in an effective, efficient and consistent manner.

Processes, once defined, should be documented and controlled. Once under control, they can be repeated and become manageable. Degrees of control over processes can be defined, and then process measurement and metrics can be built in to the process to control and improve the process, as illustrated in Figure 3.11.

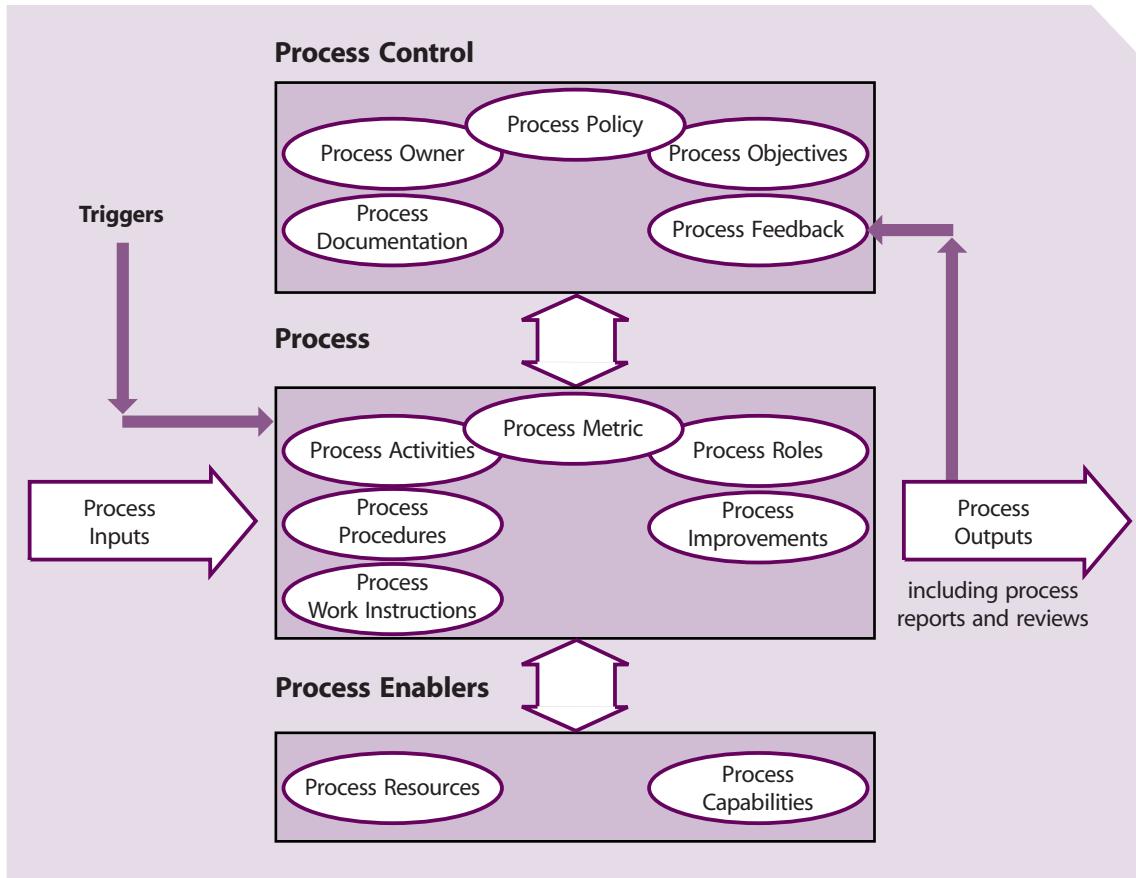


Figure 3.11 The generic process elements

The generic process elements show data enters the process, is processed, is output and the outcome is measured and reviewed. This very basic description underpins any process description. A process is always organized around a set of objectives. The main outputs from the process should be driven by the objectives and should always include process measurements (metrics), reports and process improvement.

Each process should be owned by a process owner, who should be responsible for the process and its improvement and for ensuring that a process meets its objectives. The objectives of any IT process should be defined in measurable terms and should be expressed in terms of business benefits and underpinning business strategy and goals. Service Design should assist each process owner with the design of processes, in order to ensure that all processes use standard terms and templates, are consistent and integrate with each other to provide end-to-end integration across all areas.

The output produced by a process has to conform to operational norms that are derived from business objectives. If products conform to the set norm, the process can be considered effective (because it can be repeated, measured and managed). If the activities are

carried out with a minimum use of resources, the process can also be considered efficient. Process analysis, results and metrics should be incorporated in regular management reports and process improvements.

All these areas should be included within the design of any process. These new ITIL publications have been written around 'sets of processes' that reflect the stages in the lifecycle of a service. The Service Design set of processes detailed in this publication covers the processes principally related to all aspects of design.

Working with defined processes has been the foundation of ITIL from its beginning. By defining what the organization's activities are, which inputs are necessary and which outputs will result from the process, it is possible to work in a more efficient and effective manner. Measuring and steering the activities increases this effectiveness. Finally, by adding norms to the process, it is possible to add quality measures to the output.

This approach underpins the Plan–Do–Check–Act cycle of continual improvement for any quality-management system. Plan the purpose of the process in such a way that process actions can be reviewed, assessed or audited for successful achievement and improved.

Norms define certain conditions that the results should meet. Defining norms introduces quality aspects to the process. Even before starting, it is important to think about what the process outcomes should look like. To discover whether or not process activities are contributing optimally to the business goal and the objectives of the process, aligned to business goals, the effectiveness should be measured on a regular basis. Measuring allows comparison of what has actually been done with what the organization set out to do, and to identify and implement improvements within the process.

Each organization should adopt a formalized approach to the design and implementation of Service Management processes. The objective should not be to design 'perfect processes', but to design practical and appropriate processes with 'in-built' improvement mechanisms, so that the effectiveness and efficiency of the processes are improved in the most suitable manner for the organization. Documentation standards, processes and templates should be used to ensure that the processes are easily adopted throughout the organization. Some example process documentation templates are included in Appendix C.

The goal for now and in the future is to design processes and support these with tools that can provide integration between organizations. This has now become possible because management tools are providing support of open standards, such as the Distributed Management Task Force (DMTF), that support the exchange of information based on ITIL concepts, such as incidents, problems and changes with standard formats and contents. This allows service providers to support efficient and effective process interfaces with their main suppliers with automated exchange of key operational information in real time.

3.6.5 Design of measurement systems and metrics

'If you can't measure it then you can't manage it.'

In order to manage and control the design processes, they have to be monitored and measured. This is true for all aspects of the design processes. Measurements and metrics are covered in detail in the Continual Service Improvement publication. This section covers those aspects that are particularly relevant and appropriate to measuring the quality of the design processes and their deliverables.

Care should be exercised when selecting measurements and metrics and the methods used to produce them. This

is because the metrics and measurements chosen will actually affect and change the behaviour of people working within the activities and processes being measured, particularly where this relates to objectives, personal and team performance and performance-related pay schemes. Therefore only measurements that encourage progression towards meeting business objectives or desired behavioural change should be selected.

In all the design activities the requirement should be to:

- Design solutions that are 'fit for purpose'
- Design for the appropriate level of quality – not over-engineered or under-engineered
- Design solutions that are 'right first time' and meet their expected targets
- Design solutions that minimize the amount of 'rework' or 'add-ons' that have to be rapidly developed after solutions have been deployed
- Design solutions that are effective and efficient from the perspective of the business and the customers. The emphasis should be on the solutions that are effective above all and that are efficient within the constraint of remaining effective.

Measurement methods and metrics should reflect these requirements and be designed to measure the ability of design processes to match these requirements. All of the measurements and metrics used should reflect the quality and success of the design processes from the perspective of the business, customers and users. They need to reflect the ability of the delivered solutions to meet the identified and agreed requirements of the business.

The process measurements selected need to be appropriate for the capability and maturity of the processes being measured. Immature processes are not capable of supporting sophisticated measurements, metrics and measurement methods. There are four types of metrics that can be used to measure the capability and performance of processes:

- **Progress:** milestones and deliverables in the capability of the process
- **Compliance:** compliance of the process to governance requirements, regulatory requirements and compliance of people to the use of the process.
- **Effectiveness:** the accuracy and correctness of the process and its ability to deliver the 'right result'
- **Efficiency:** the productivity of the process, its speed, throughput and resource utilization.

Measurements and metrics should develop and change as the maturity and capability of a process develops. Initially, with immature processes the first two levels of metrics should be used to measure the progress and compliance of the process as it develops in maturity. As the process maturity develops, greater use should be made of effectiveness and efficiency metrics, but not to the detriment of compromising the progress or compliance of the process.

The selection of the metrics, the point of measurement and the methods of measuring, calculating and reporting on the metrics must be carefully designed and planned. The primary metrics should always focus on determining the effectiveness and the quality of the solutions provided. Secondary metrics can then measure the efficiency of the processes used to produce and manage the solution. The priority should always be to ensure that the processes provide the correct results for the business. Therefore the measurement methods and metrics should always provide this business-focused measurement above all.

The most effective method of measurement is to establish a 'Metrics Tree' or 'KPI tree'. Too many organizations collect measurement in individual areas, but fail to aggregate them together and gain the full benefit of the measurements, and therefore suffer because:

- Measurements are not aligned with business objectives and needs
- There is no overall visibility of the 'top-level' picture
- There are gaps in areas where measurements are not recorded
- Individual areas are well measured and others are poorly measured or are not measured
- There is no consistency in the method, presentation and calculation of the measurements
- Decisions and improvement actions are based on incomplete or inaccurate information.

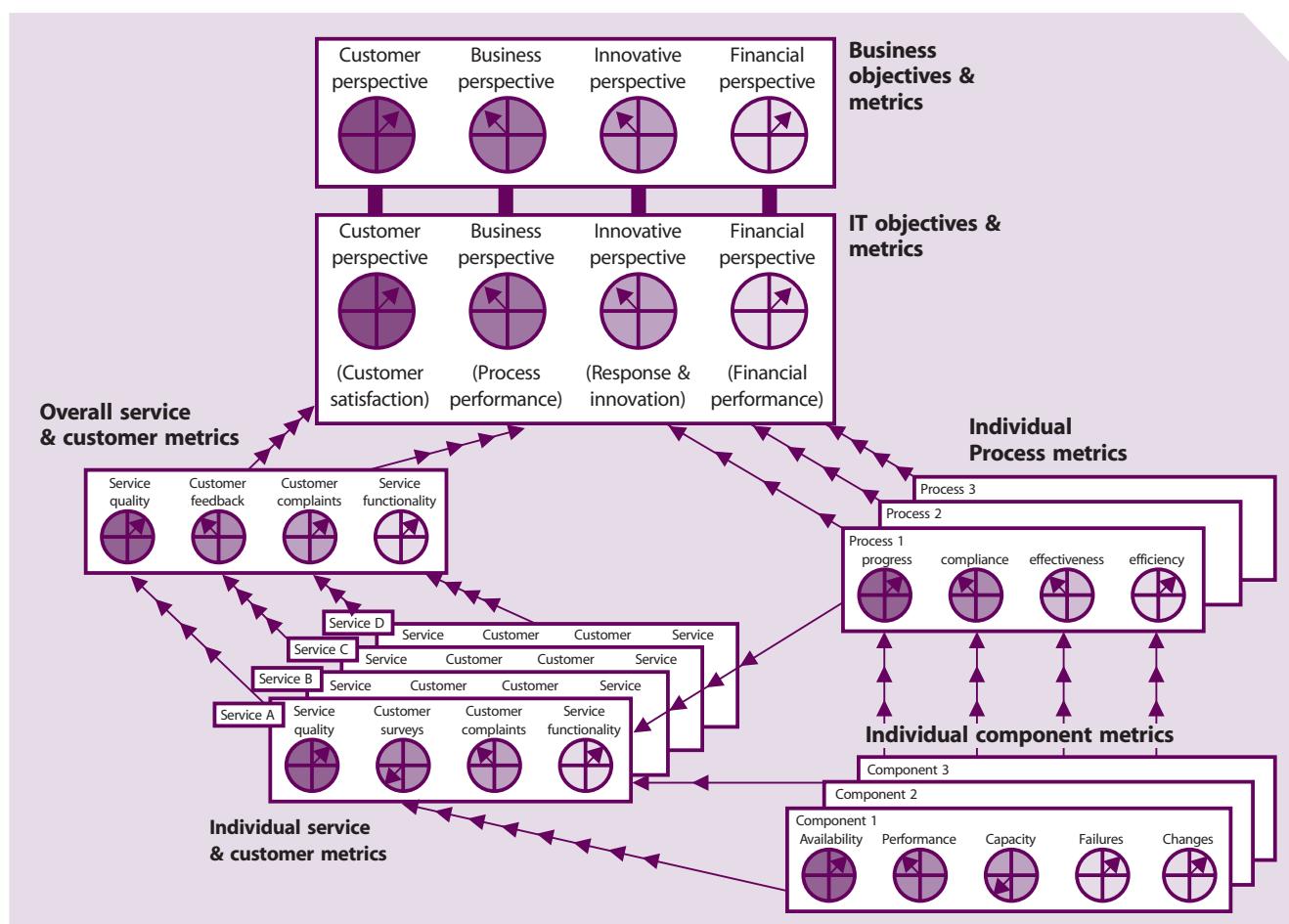


Figure 3.12 The Metrics Tree

Therefore organizations should attempt to develop automated measurement systems based on a form of 'Metrics Tree' such as that illustrated in Figure 3.12.

The tree in Figure 3.12 is illustrative of an example of a Metrics Tree based on a typical Balanced Scorecard. Balanced Scorecards represent a management system that enables increasing numbers of organizations to clarify their vision and strategy into action. They provide feedback regarding the internal business processes and external outcomes in order continually to improve strategic performance and results. This enables everybody within the organization to get a picture of the performance of the organization at the appropriate level:

- Business managers and customers can get a 'top-level' business 'dashboard', aligned with business needs and processes
- Senior IT managers and customers can focus on the top-level IT management dashboard
- Service managers and customers can focus on the performance of particular services
- Process owners and managers can view the performance of their processes
- Technical specialists can look at the performance of individual components
- The dashboard also presents an opportunity to view trends over time, rather than static data, so that potential performance degradation can be identified and rectified at an early stage.

This means that within a hierarchical metrics system, each person in the organization can get access to an appropriate level of information and measurement that suits their particular need. It gives senior management the opportunity to monitor a top-level dashboard to ensure that services continue to be delivered to their agreed levels, and it also provides the capability for technical specialists and processes owners to drill down to the detail to analyse variance from agreed service, component or process performance.

Obviously the collection, analysis and presentation of this data can be a very labour-intensive activity and therefore should be automated wherever possible. This can be achieved using analysis tools based on macros, scripts, spreadsheets, or preferably on specific web-based solutions. The measurements at each of the levels should be specifically defined to meet the needs of the business, customers and users of the information.

More detailed information on measurements, metrics and measurement methods are contained in the Continual Service Improvement publication.

3.7 THE SUBSEQUENT DESIGN ACTIVITIES

Once the desired service solution has been designed, then the subsequent activities must also be completed with the Service Design stage before the solution passes into the Service Transition stage.

3.7.1 Evaluation of alternative solutions

An additional evaluation stage may be necessary if external supplier services and solutions are involved. This consists of the following:

- Selecting a set of suppliers and completing a tendering process. This will require the production and completion of:
 - Documentation of the scope of the service and production of a Statement of Requirement (SoR) and/or a Terms of Reference (ToR) document
 - Request For Information (RFI), Request For Proposal (RFP), Request For Quotation (RFQ) and Invitation To Tender (ITT) documents
 - Producing and agreeing a set of solution and supplier evaluation criteria and a scoring process.
- Evaluation and review of supplier responses and selection of the preferred supplier(s) and their proposed solution(s). This may also involve running trials or even prototyping or proof of concept activities if significant new concepts or technology are involved in the new service in order to ensure that new components meet their expectations.
- Evaluation and costing of the alternative designs, possibly including identification of potential suppliers and evaluation of their alternative proposals, technologies, solutions and contracts. There is a need to ensure that costing covers one-off costs and ongoing costs of operation and ownership, including support and maintenance.

3.7.2 Procurement of the preferred solution

It is possible that no external elements will be required for the solution. However, this is unusual as suppliers of software at least are highly likely to be involved. Where external suppliers are involved in the preferred solution, the stages consist of:

- Completing all necessary checks on the preferred supplier
- Finalizing the terms and conditions of any new contracts, ensuring that all corporate policies are enforced
- The procurement of the selected solution.

3.7.3 Develop the service solution

The development stage consists of translating the Service Design into a plan for the development, re-use or redevelopment of the components required to deliver the service and the subsequent implementation of the developed service. It may need to be developed into a programme of plans, if this is a major service change. Each plan or project within the programme will be responsible for delivering one or more components of the service and will include:

- The needs of the business
- The strategy to be adopted for the development and or purchase of the solution
- The timescales involved
- The resources required, taking into consideration facilities, IT infrastructure and the right personnel skills in order to ensure the delivery service meets the customer's needs
- The development of the service and its constituent components, including the management and other operational mechanisms, such as measurement, monitoring and reporting
- Service and component test plans.

Careful project management will need to be used to ensure that conflict is avoided and that the compatible components are developed from the various different development activities

3.8 DESIGN CONSTRAINTS

All design activities operate within many constraints. These constraints come from the business and Service Strategy and cover many different areas, as illustrated in Figure 3.13.

This means that designers are not always 'free' to design the most appropriate solution for the business, because it does not fall within the imposed constraints, as illustrated in Figure 3.13. The most obvious constraint is the financial one. There may be insufficient budget available for the most appropriate solution, therefore a cheaper alternative service would have to be identified and agreed with the business. The designer can only provide the solution that fits within all of the currently known constraints, or else try lifting or renegotiating some of the constraints – for instance, by obtaining a bigger budget. In Figure 3.13, not only will more budget need to be obtained to implement the desired solution, but it would also be non-compliant with some of the relevant standards and regulations. So in this case an alternative, cheaper compliant solution would probably be required.

So the Service Design processes must recognize the fact that they are free to design solutions, but they are working in an environment where many external factors can influence the design.

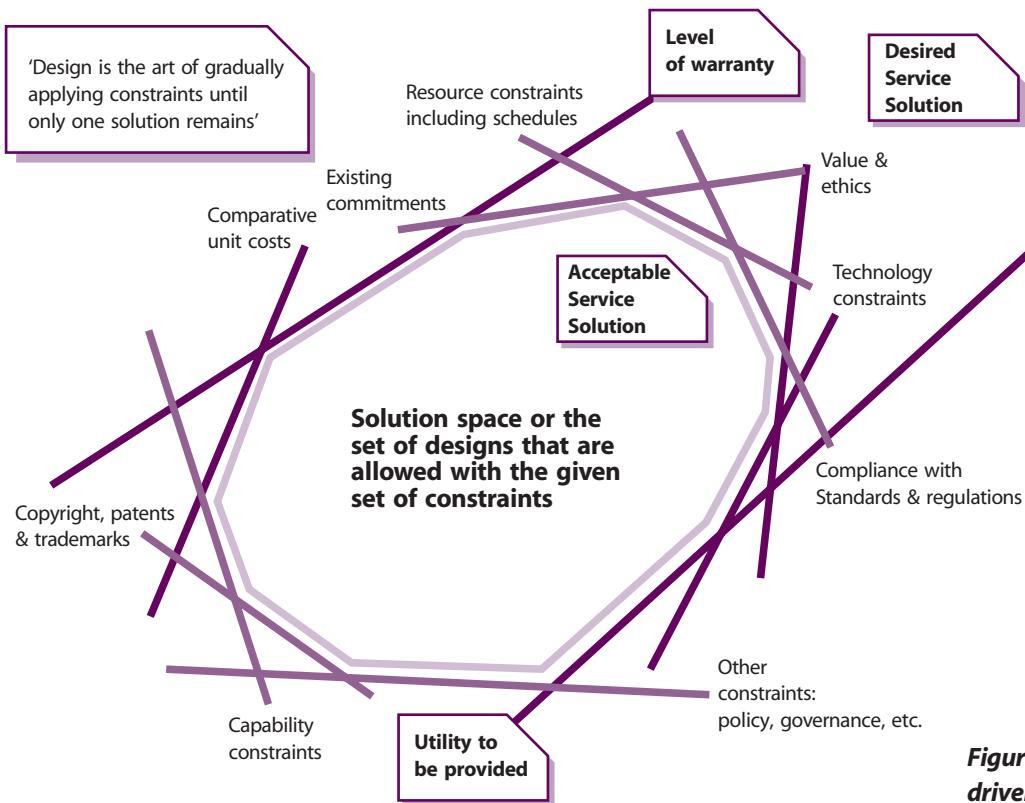


Figure 3.13 Design constraints driven by strategy

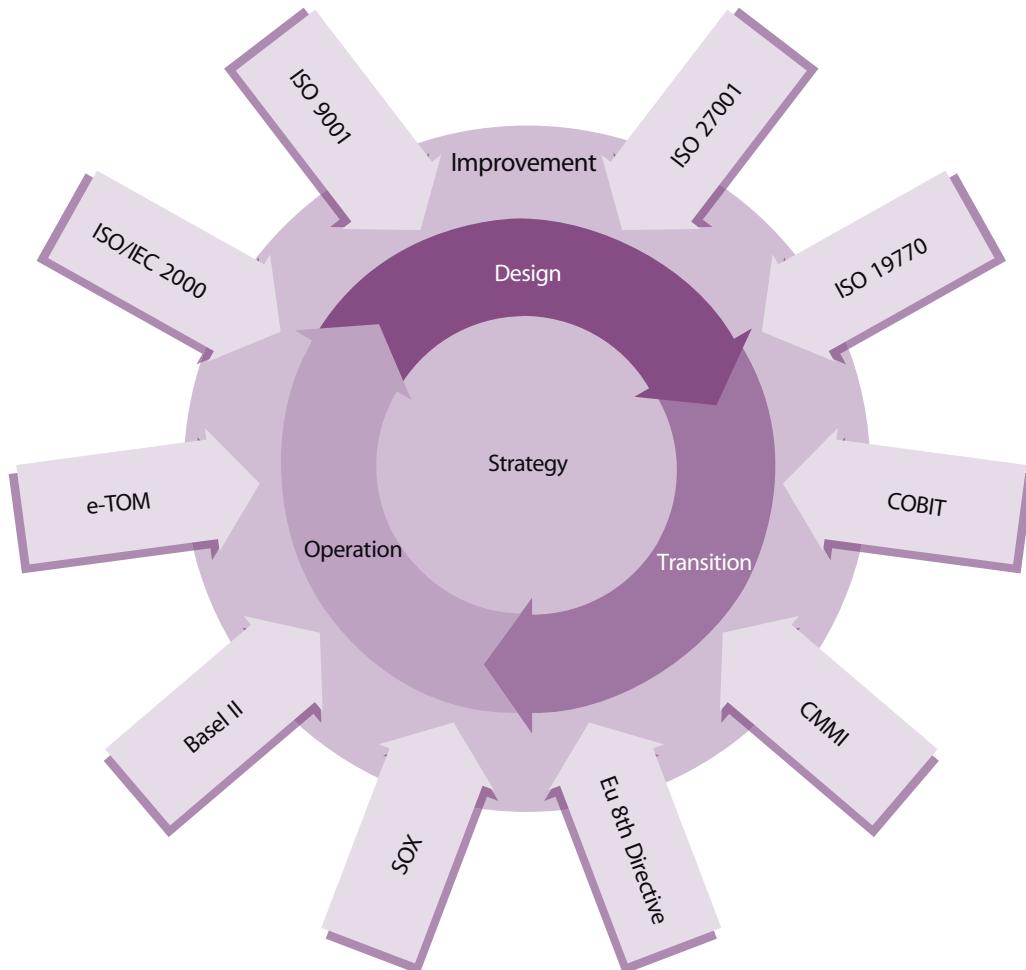


Figure 3.14 External influences on solution design

Many of these external influences are from the need for good corporate and IT governance, and others are from the requirement for compliance with regulations, legislation and international standards, as illustrated in Figure 3.14. It is essential, therefore, that all designers recognize these and ensure that the designs and solutions they produce have all of the necessary controls and capability within them.

3.9 SERVICE ORIENTED ARCHITECTURE

Business process and solutions should be designed and developed using a Service Oriented Architecture (SOA) approach. The SOA approach is considered best practice and is used by many organizations to improve their effectiveness and efficiency in the provision of IT services.

SOA is defined by OASIS (www.oasis-open.org) as:

‘A paradigm for organizing and utilizing distributed capabilities that may be under the control of different ownership domains. It provides a uniform means to offer, discover, interact with and use capabilities to produce desired effects consistent with measurable preconditions and expectations.’

OASIS (Organization for the Advancement of Structured Information Standards) is a not-for-profit, international consortium that drives the development, convergence and adoption of e-business standards. SOA brings value and agility to an organization by encouraging the development of ‘self-contained’ services that are re-usable. This, in turn, promotes a flexible and modular approach to the development of ‘shared services’ that can be used in many different areas of the business. More and more organizations are converting business processes to common ‘packaged services’ that can be used and shared by many areas of the business.

Wherever possible, IT service provider organizations should use the SOA and principles to develop flexible, re-usable IT services that are common and can be shared and exploited across many different areas of the business. When this approach is used, it is essential that IT:

- Defines and determines what a service is
- Understands and clearly identifies interfaces and dependencies between services
- Utilizes standards for the development and definition of services
- Uses common technology and tool-sets
- Investigates and understands the impact of changes to 'shared services'
- Ensures that SOA-related training has been planned and achieved for the IT people in order to establish a common language and improve the implementation and support of the new or changed services.

When SOA principles are used by the IT service provider organization, it is critical that an accurate Service Catalogue is maintained as part of an overall Service Portfolio and Configuration Management System (CMS). Adopting this approach can significantly reduce the time taken to deliver new solutions to the business and to move towards a Business Service Management (BSM) capability. The Service Catalogue will also show the relationship between services and applications. A single application could be part of more than one service, and a single service could utilize more than one application.

3.10 BUSINESS SERVICE MANAGEMENT

Business Service Management (BSM) is a strategy and an approach to enable IT components to be linked to the goals of the business. This way the impact of technology on the business and how business change may impact technology can both be predicted. The creation of a totally integrated Service Catalogue – including business units, processes and services, and their relationships and dependencies on IT services, technology and components – is crucial to increasing the IT service provider's capability to deliver BSM. All aspects of Service Design are vital elements in supporting and enhancing the Business Service Management capability of the IT service provider, particularly the design of the Service Portfolio, the Service Catalogue and the individual IT services. All of these activities will also improve the alignment of IT service provision with business and its evolving needs. See Figure 3.15.

BSM enables an IT service provider organization to:

- Align IT service provision with business goals and objectives
- Prioritize all IT activities on business impact and urgency, ensuring critical business processes and services receive the most attention
- Increase business productivity and profitability through the increased efficiency and effectiveness of IT processes

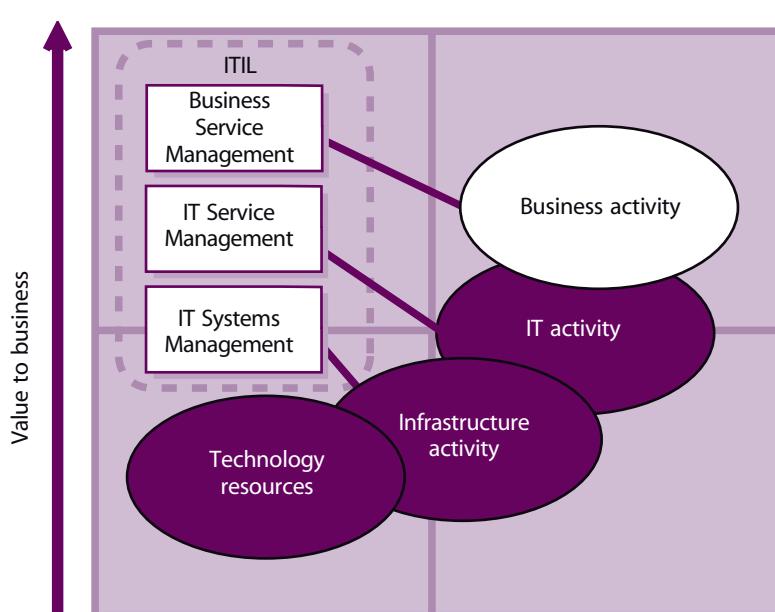


Figure 3.15 The IT management continuum

- Support the requirements for corporate governance with appropriate IT governance and controls
- Create competitive advantage through the exploitation and innovation of IT infrastructure as a whole
- Improve service quality, customer satisfaction and user perception
- Ensure regulatory and legislative compliance
- Ensure appropriate levels of protection on all IT and information assets
- Ensure that IT services are aligned and continue to be aligned with changing business needs.

Figure 3.15 illustrates the relationship of service activities and Service Management, and the reach and range they offer in value to the business and IT.

3.11 SERVICE DESIGN MODELS

The model selected for the design of IT services will depend mainly on the model selected for the delivery of IT services. Before adopting a design model for a major new service, a review of the current capability and provisions with respect to all aspects of the delivery of IT services should be conducted. This review should consider all aspects of the new service, including the:

- Business drivers and requirements
- Scope and capability of the existing service provider unit
- Demands, targets and requirements of the new service
- Scope and capability of external suppliers
- Maturity of the organizations currently involved and their processes
- Culture of the organizations involved
- IT infrastructure, applications, data, services and other components involved
- Degree of corporate and IT governance and the level of ownership and control required
- Budgets and resources available
- Staff levels and skills.

This review/assessment provides a structured mechanism for determining an organization's capabilities and state of readiness for delivering new or revised services in support of defined business drivers and requirements. The information obtained from such an assessment can be used in determining the delivery strategy for a particular IT service or IT system. The delivery strategy is the approach taken to move an organization from a known state, based on the readiness assessment, to a desired state, determined by the business drivers and needs. There are many ways to prepare an organization for deploying a

new service. The method and strategy selected should be based on the solution the organization chooses for fulfilling its key business drivers, as well as the capabilities of the IT organization and its partners. The scale of options available is quite large, and not every option needs be considered in every case. However, keeping all the options available for consideration is key for designing and operating innovative solutions to the most difficult business challenges. In the end, this may be the difference between a failed project – or even a failed company – and a successful one.

These two models, for the design and delivery of IT services, are closely related and are considered in the following two sections.

3.11.1 Delivery model options

Although the readiness assessment determines the gap between the current and desired capabilities, an IT organization should not necessarily try to bridge that gap by itself. There are many different delivery strategies that can be used. Each one has its own set of advantages and disadvantages, but all require some level of adaptation and customization for the situation at hand. Table 3.2 lists the main categories of sourcing strategies with a short abstract for each. Delivery practices tend to fall into one of these categories or some variant of them.

Table 3.2 highlights a key point: the set of delivery strategies varies widely and ranges from a relatively straightforward situation, solely managed within the boundaries of a company, all the way to a full KPO situation. This broad range of alternatives provides significant flexibility, but often with added complexity, and in some cases additional risk. The advantages and disadvantages of each type of delivery strategy are discussed in Table 3.3 below.

All of the above arrangements can be provided in both an off-shore or on-shore situation. In the on-shore case, both organizations are based within the same country/continent, whereas in the off-shore situation the organizations are in different countries/continents. Very complex sourcing arrangements exist within the IT industry and it is impossible to cover all combinations and their implications here. ITIL Service Management Practice Complementary Series will provide additional guidance on sourcing strategies.

Mergers and acquisitions can also complicate the issues. These situations occur when one company acquires or merges with another company for cash and/or equity swaps of the company's stock. Again, this occurs generally in response to industry consolidations, market expansion,

Table 3.2 Main service delivery strategies

Delivery strategy	Description
Insourcing	This approach relies on utilizing internal organizational resources in the design, development, transition, maintenance, operation and/or support of new, changed or revised services or data centre operations
Outsourcing	This approach utilizes the resources of an external organization or organizations in a formal arrangement to provide a well-defined portion of a service's design, development, maintenance, operations and/or support. This includes the consumption of services from Application Service Providers (ASPs) described below
Co-sourcing	Often a combination of insourcing and outsourcing, using a number of outsourcing organizations working together to co-source key elements within the lifecycle. This generally involves using a number of external organizations working together to design, develop, transition, maintain, operate and/or support a portion of a service
Partnership or multi-sourcing	Formal arrangements between two or more organizations to work together to design, develop, transition, maintain, operate and/or support IT service(s). The focus here tends to be on strategic partnerships that leverage critical expertise or market opportunities.
Business Process Outsourcing (BPO)	The increasing trend of relocating entire business functions using formal arrangements between organizations where one organization provides and manages the other organization's entire business process(es) or function(s) in a low-cost location. Common examples are accounting, payroll and call centre operations
Application Service Provision	Involves formal arrangements with an Application Service Provider (ASP) organization that will provide shared computer-based services to customer organizations over a network. Applications offered in this way are also sometimes referred to as on-demand software/applications. Through ASPs, the complexities and costs of such shared software can be reduced and provided to organizations that could otherwise not justify the investment
Knowledge Process Outsourcing (KPO)	The newest form of outsourcing, KPO is a step ahead of BPO in one respect. KPO organizations provide domain-based processes and business expertise rather than just process expertise, and require advanced analytical and specialized skills from the outsourcing organization

or in direct response to competitive pressures. If companies that have different service delivery strategies are acquired or merge, a period of review and consolidation is often required to determine the most appropriate sourcing strategy for the newly merged organization. However, mergers and acquisitions can often provide organizations with the opportunity to consolidate the best practice from each organization, thereby

improving the overall service capability and achieving synergies across the organization. Opportunities will also exist to provide improved career development options to Service Management personnel and to consolidate supplier contract for services.

3.11.2 Design and development options

The delivery strategies are relevant to both the design and transition stages of the Service Lifecycle as well as the operation stage. Extreme care must be taken when selecting different strategies for different stages of the

lifecycle to ensure that all organizations involved clearly understand their individual roles and responsibilities, and also every other organization's role and responsibility to ensure acceptance and handover processes are clearly defined, agreed and accepted.

Table 3.3 Advantages and disadvantages of service delivery strategies

Delivery strategy	Advantages	Disadvantages
Insourcing	Direct control Freedom of choice Rapid prototyping of leading-edge services Familiar policies and processes Company-specific knowledge	Scale limitations Cost and time to market for services readily available outside Dependent on internal resources and their skills and competencies
Outsourcing	Economies of scale Purchased expertise Supports focus on company core competencies Support for transient needs Test drive/trial of new services	Less direct control Exit barriers Solvency risk of suppliers Unknown supplier skills and competencies More challenging business process integration Increased governance and verification
Co-sourcing	Time to market Leveraged expertise Control Use of specialized providers	Project complexity Intellectual property and copyright protection Culture clash between companies
Partnership or multi-sourcing	Time to market Market expansion/entrance Competitive response Leveraged expertise Trust, alignment and mutual benefit 'Risk and reward' agreements	Project complexity Intellectual property and copyright protection Culture clash between companies
Business Process Outsourcing (BPO)	Single point of responsibility 'One-stop shop' Access to specialist skills Risk transferred to the outsource Low-cost location	Culture clash between companies Loss of business knowledge Loss of relationship with the business
Application Service Provision	Access to expensive and complex solutions Low-cost location Support and upgrades included Security and ITSCM options included	Culture clash between companies Access to facilities only, not knowledge Often usage-based charging models
Knowledge Process Outsourcing (KPO)	Access to specialist skills, knowledge and expertise Low-cost location Significant cost savings	Culture clash between companies Loss of internal expertise Loss of relationship with the business

Example

A medium size bank merged with another bank that had a complementary product portfolio. Therefore the integration of applications was simple. However, the two banks felt that consolidation of operations would be beneficial, but could not leverage the economies of scale to a sufficient extent. Outsourcing was also an option, but instead the two banks chose to partner with an outsourcing company. The banks provided the bank-specific knowledge to make their IT services organization an attractive data centre for smaller banks. The outsourcing partner provided the necessary technology expertise and new clients to benefit from the economies of scale.

So how does an organization determine the optimum delivery strategy? There is no single or simple answer to this question. It is too dependent on the unique and specific situation under consideration. For this reason, the most appropriate guidance that can be provided is to describe key advantages and disadvantages of each delivery strategy. This, in turn, can be used as a checklist to determine which delivery approach should be evaluated further and most benefit the specific project or business initiative. Table 3.3 lists each strategy and its key advantages and disadvantages for the delivery of an application or IT service.

The strategy selected will depend on the capability and needs of the specific organization, its business and people – culture and capabilities. Whichever strategy is selected, its success and operation should be measured and regularly reviewed for effectiveness and efficiency and adapted to fit the changing business needs. The selection adopted with regard to IT service provision can often be influenced by the overall business culture and its approach to outsourcing and partnering.

3.11.3 Design and development approaches

It is also important to understand the current generic lifecycle types, methods and approaches to IT service development, in order to decide on standards for the Service Design stage of the lifecycle. To achieve this, a good understanding is needed of the following aspects of the various Service Development Life Cycle (SDLC) approaches:

- The structure (for example, milestones/stages/phases)
- The activities (for example, the workflows or detailed steps/tasks described within an approach)

- The primary models associated with the chosen method, typically giving a process perspective, a data perspective, an event perspective and, often, a user perspective. Examples include use case diagrams, class diagrams and state chart diagrams from the Unified Modelling Language (UML).

There is more detail on SDLC in Chapter 5.

3.11.3.1 Rapid Application Development

It is necessary to understand the differences between object-oriented and structured systems development, the basic principles of the 'Agile' (Rapid Application Development (RAD) or accelerated development are other terms used in this area) movement and to recognize how a commitment to a software package solution changes the structure of the approach.

These approaches, which by default address a single system (and related services) only, can be supplemented by architectural approaches, such as those based on component-based re-use (see the section on architecture for further discussion).

The application lifecycle model described in the section on Applications Management (section 5.1.3) can be viewed as an example of linear or 'waterfall' (or 'V' model) based approach, and will not be discussed in further detail here, other than for comparison purposes with other approaches.

The main feature of RAD is the introduction of increments and iterations in the development process for the management of the risks associated with uncertainty and changing requirements. Traditional approaches have assumed that a complete set of requirements could be defined early in the lifecycle and that development costs could be controlled by managing change. However, discouraging change can mean being unresponsive to business conditions. RAD approaches accept that change is inevitable and attempt to minimize the costs of responding to them while still retaining the required quality.

The use of increments implies that a service is developed piece by piece, where every piece could support one of the business functions that the entire service needs. Incremental delivery could result in shorter time to market for specific business functions. The development of every increment requires traversal of all lifecycle stages.

Iterative development implies that the lifecycle will be traversed more than once, by design. Techniques such as prototyping are used to get a better understanding of the requirements (by testing functional, management and operational activities and through communication with users).

Combinations of iterative and incremental approaches are possible. It is possible to start with the specification of requirements for the entire service, followed by the design and development of the application incrementally.

RAD development methods, including the Unified Process and Dynamic Systems Development Method (DSDM) are seen as a response to business expectations, with the goal of reducing the cost of change throughout a development project. DSDM utilizes continuous user involvement in an iterative development and incremental approach, which is responsive to changing requirements, to develop a software system that satisfies the business requirements on time and on budget. Another example, Extreme Programming (XP), calls for developers to:

- Produce a first service delivery in weeks, to achieve an early win and rapid feedback
- Invent simple solutions, so there is less to modify and also facilitating change
- Improve design quality continually
- Test early for less expensive fault-finding
- Use basic disciplines such as reviews, configuration and change management to keep control.

To make good use of an incremental approach, the design process needs to be based on a separation of concerns, by grouping functions within increments in such a way that their interdependence is minimized.

In general terms, accelerated application development methods adopt a three-phase lifecycle model: accelerated analysis and design, time-boxed development and production and implementation. The methods are usually underpinned by software engineering technology, and rely on joint (IT-user) working and prototyping to quickly define requirements and create a working prototype.

From a business perspective, the use of incremental development and delivery by developers means that a valid, distinct part of the overall service can be delivered before the development team is in a position to complete the whole project. This approach offers early benefits to the business, and provides an opportunity for both the

business and development team to discover emergent service properties and learn from their experience. However, it is often difficult to find a sufficiently small first increment that can provide a meaningful service to business.

RAD methods embodying iteration and incremental delivery can be used to reduce both development and implementation risks. The actual projects may not necessarily be easier to manage, but they can facilitate implementation and acceptance. They offer more options for contingency and enable developers to deal with changing business requirements and environmental conditions. They also provide both milestones and decision points for project control purposes. These methods can additionally be used to:

- Reach or converge on a design acceptable to the customer and feasible to the development team
- Limit the project's exposure to the unpredictable elements of both business and environmental change
- Save development time, although for a successful RAD project, something other than schedule must be negotiable. (RAD has the best chance for success if the business is willing to negotiate on both functionality and quality).

Important Rapid Application Development (RAD) constraints or Critical Success Factors (CSFs) include:

- 'Fitness for business purpose' as the criterion for acceptance of deliverables
- Representation of all parties that can impact application requirements throughout the development process
- Customers, developers and management accepting informal deliverables, e.g. notes from user workshops rather than formal requirements documents
- Creating the minimum documentation necessary to facilitate future development and maintenance
- Empowerment of development teams to make decisions traditionally left to management
- Iteration being used in such a manner as to converge towards an acceptable business solution
- Prototypes that can incorporate evolving requirements quickly, to gain consensus early in the lifecycle.

The use of RAD approaches requires skilled, multidisciplinary teams, who are able to advise on when to apply such approaches.

Table 3.4 Comparison between conventional ('waterfall') and RAD approaches

Category	Conventional development	Accelerated development
General approach	Sequential phases	Evolutionary
User resource commitment	± 15% throughout the project	100% throughout project for project sponsor, ± 30% for selected others
Risk	Higher – longer-term project problems may not emerge until well into the development project	Lower – problems surface early in the development process, requiring quick resolution
Executive sponsorship	Has approval authority, but not actively involved	High participation – sets scope, reviews progress and resolves issues
Use of joint session, iteration and prototyping techniques	Optional	Required
Developer skills	Specialists, some with limited experience acceptable	Highly experienced, multi-skilled professionals required
Use of process support technology, e.g. CASE tools	Optional	Required
Team structure	Usually large with specialized skill sets	Usually small with general skill sets, supplemented by specialists as needed
Rigorous scope management	Necessary	Critical
Phase structure	4–5 phases	3 phases
Individual accountability	Difficult to assess	Precise accountability

3.11.3.2 Off-the-shelf solutions

Many organizations now choose to fulfil their IT service requirements through purchasing and implementing commercial off-the-shelf (COTS) software package solutions. A framework for selecting, customizing and implementing these off-the-shelf packaged solutions is needed and includes the need to:

- Fully understand the advantages and disadvantages of the package approach
- Define a framework for effective software package selection
- Define a framework for effective customization and integration
- Define functional requirements at the appropriate level
- Develop a checklist of management and operational requirements
- Define product and supplier requirements
- Define service integration requirements
- Identify and investigate potential off-the-shelf software package solutions
- Present recommendations about the fit of a selected off-the-shelf software package against agreed requirements, and define the implications of this.

Detailed standards will be needed on:

- Packages and prototyping
- Defining the structure of weighted evaluation matrices
- Iteration in package selection.

Additionally, procedures for evaluating and comparing competing packages in terms of customization/integration requirements are needed and should include:

- Evaluating the functional match
- Scripted demonstrations and user-driven evaluation
- Evaluating the management and operational match
- Evaluating the implementation requirements match.

Standards for documenting requirements prior to package market investigation should include ones specifically showing:

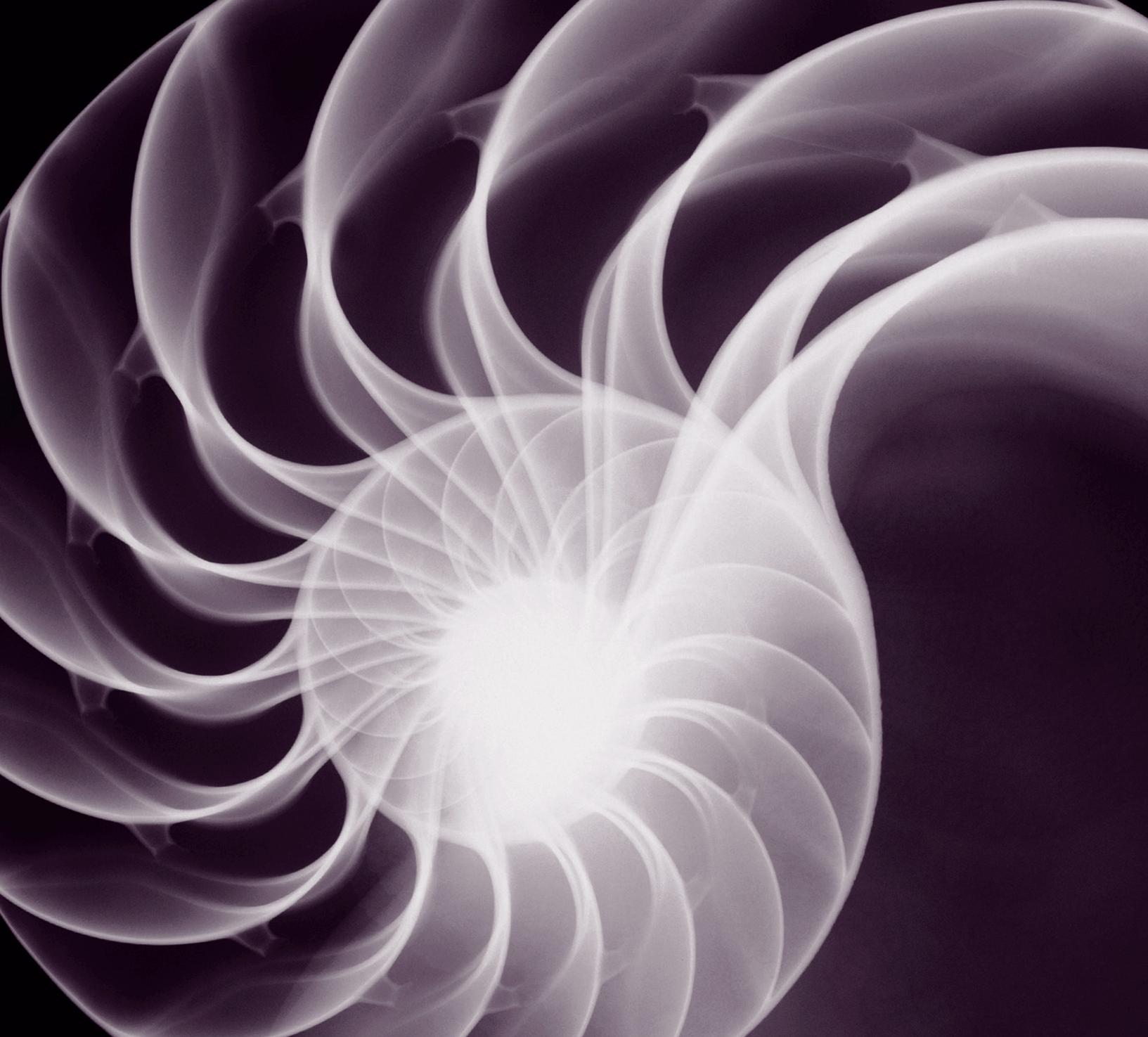
- High-level functions (for scoping purposes)
- Business functions and significant events
- Significant input and output requirements
- Data (static) structures
- Identifying relationships between those structures, functions and events
- Service-wide management and operational requirements

- Non-functional requirements such as performance, throughput, disaster recovery capabilities, infrastructure and security standards.

When evaluating COTS solutions, consider the following three ways in which a requirement can be fulfilled:

- Available off-the-shelf
- Can be configured. Estimate the effort to perform the configuration. This only needs to be done once and will be preserved over upgrades of the product
- Must be customized. Estimate the effort to perform the customization initially and to repeat it on each upgrade of the product, bearing in mind that the customization concept might not be applicable to future releases.

Also investigate the strategy and release plan of the package supplier and ascertain whether it is aligned to yours, and to what extent you can expect your future requirements to be met by the package.



4

Service Design processes

4 Service Design processes

This chapter describes and explains the fundamentals of the key supporting Service Design processes. These processes are principally responsible for providing key information to the design of new or changed service solutions. There are five aspects of design that need to be considered:

- The design of the services, including all of the functional requirements, resources and capabilities needed and agreed
- The design of Service Management systems and tools, especially the Service Portfolio, for the management and control of services through their lifecycle
- The design of the technology architectures and management systems required to provide the services
- The design of the processes needed to design, transition, operate and improve the services, the architectures and the processes themselves
- The design of the measurement methods and metrics of the services, the architectures and their constituent components and the processes.

A results-driven approach should be adopted for each of the above five aspects. In each, the desired business outcomes and planned results should be defined so that what is delivered meets the expectations of the customers and users. Thus this structured approach should be adopted within each of the five aspects to deliver quality, repeatable consistency and continual improvement throughout the organization. There are no situations within IT service provision with either internal or external service providers where there are no processes in the Service Design area. All IT service provider organizations already have some elements of their approach to these five aspects in place, no matter how basic. Before starting on the implementation of the improvement of activities and processes, a review should be conducted of what elements are in place and working successfully.

Many service provider organizations already have mature processes in place for designing IT services and solutions.

All designs and design activities need to be driven principally by the business needs and requirements of the organization. Within this context they must also reflect the needs of the strategies, plans and policies produced by Service Strategy processes, as illustrated in Figure 4.1.

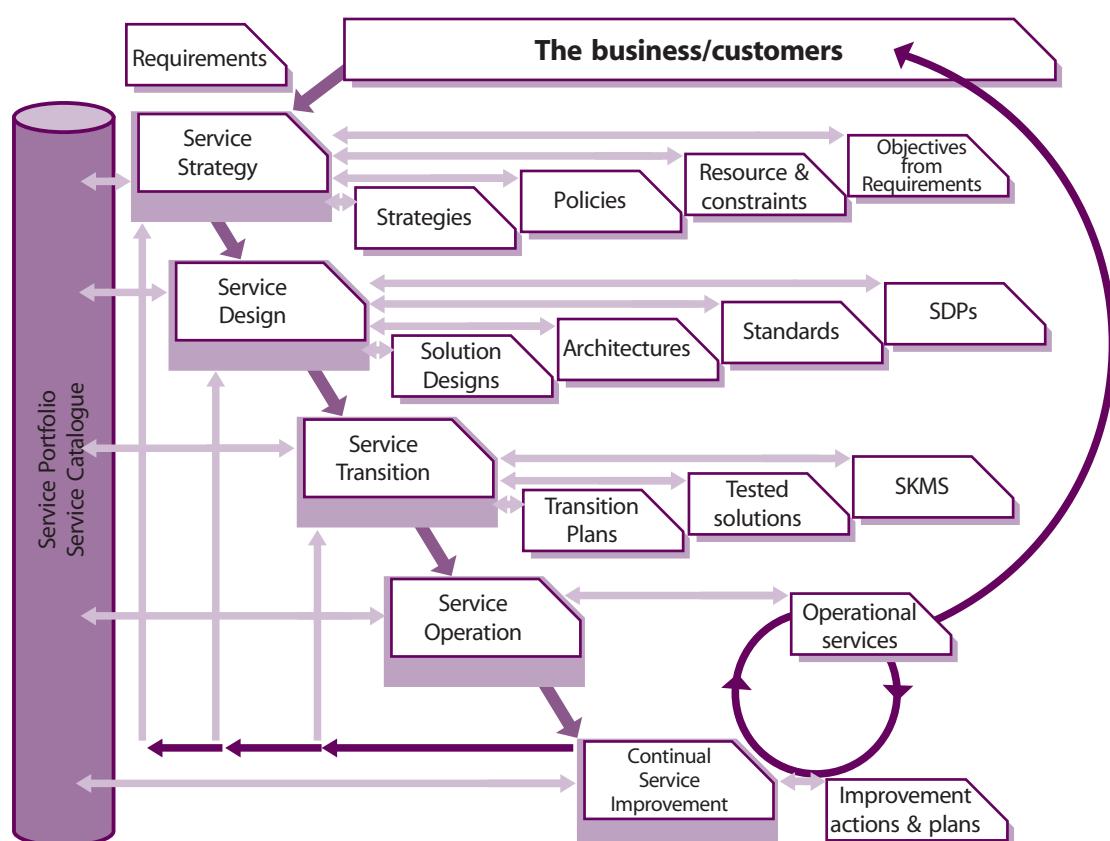


Figure 4.1 The key links, inputs and outputs of Service Design

Figure 4.1 gives a good overview of the links, inputs and outputs involved at each stage of the Service Lifecycle. It illustrates the key outputs produced by each stage, which are used as inputs by the subsequent stages. The Service Portfolio acts as ‘the spine’ of the Service Lifecycle. It is the single integrated source of information on the status of each service, together with other service details and the interfaces and dependencies between services. The information within the Service Portfolio is used by the activities within each stage of the Service Lifecycle.

The key output of the Service Design stage is the design of service solutions to meet the changing requirements of the business. However, when designing these solutions, input from many different areas needs to be considered within the various activities involved in designing the service solution, from identifying and analysing requirements, through to building a solution and SDP to hand over to Service Transition.

In order to develop effective and efficient service solutions that meet and continue to meet the requirements of the business and the needs of IT, it is essential that all the inputs and needs of all other areas and processes are

reconsidered within each of the Service Design activities, as illustrated in Figure 4.2. This will ensure that all service solutions are consistent and compatible with existing solutions and will meet the expectations of the customers and users. This will most effectively be achieved by consolidating these facets of the key processes into all of these Service Design activities, so that all inputs are automatically referenced every time a new or changed service solution is produced.

4.1 SERVICE CATALOGUE MANAGEMENT

4.1.1 Purpose/goal/objective

The purpose of Service Catalogue Management is to provide a single source of consistent information on all of the agreed services, and ensure that it is widely available to those who are approved to access it.

The goal of the Service Catalogue Management process is to ensure that a Service Catalogue is produced and maintained, containing accurate information on all operational services and those being prepared to be run operationally.

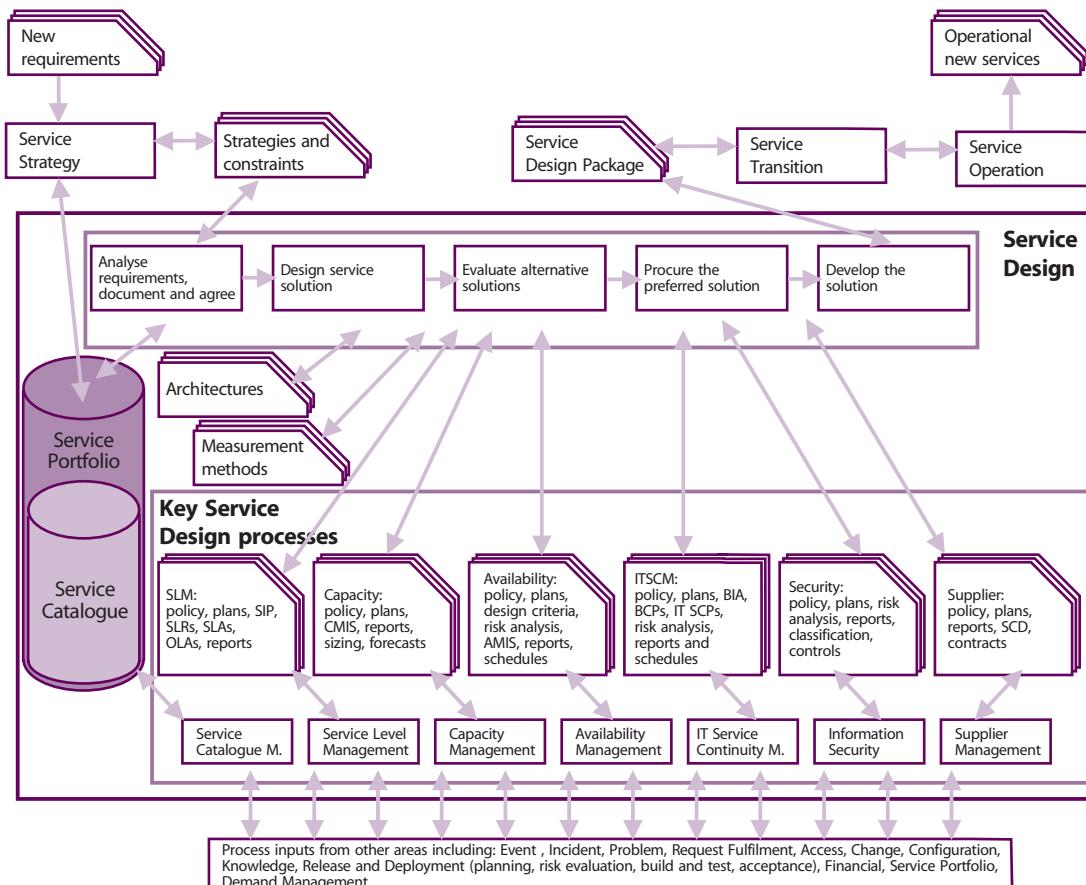


Figure 4.2 Service Design – the big picture

The objective of Service Catalogue Management is to manage the information contained within the Service Catalogue, and to ensure that it is accurate and reflects the current details, status, interfaces and dependencies of all services that are being run, or being prepared to run, in the live environment.

4.1.2 Scope

The scope of the Service Catalogue Management process is to provide and maintain accurate information on all services that are being transitioned or have been transitioned to the live environment.

The Service Catalogue Management activities should include:

- Definition of the service
- Production and maintenance of an accurate Service Catalogue
- Interfaces, dependencies and consistency between the Service Catalogue and Service Portfolio
- Interfaces and dependencies between all services and supporting services within the Service Catalogue and the CMS
- Interfaces and dependencies between all services, and supporting components and Configuration Items (CIs) within the Service Catalogue and the CMS.

4.1.3 Value to the business

The Service Catalogue provides a central source of information on the IT services delivered by the service provider organization. This ensures that all areas of the business can view an accurate, consistent picture of the IT services, their details and their status. It contains a customer-facing view of the IT services in use, how they are intended to be used, the business processes they enable, and the levels and quality of service the customer can expect for each service.

4.1.4 Policies, principles and basic concepts

Over the years, organizations' IT infrastructures have grown and developed, and there may not be a clear picture of all the services currently being provided and the customers of each service. In order to establish an accurate picture, it is recommended that an IT Service Portfolio containing a Service Catalogue is produced and maintained to provide a central, accurate set of information on all services and to develop a service-focused culture.

The Service Portfolio should contain all the future requirements for services and the Service Catalogue

should contain details of all services currently being provided or those being prepared for transition to the live environment, a summary of their characteristics, and details of the customers and maintainers of each. A degree of 'detective work' may be needed to compile this list and agree it with the customers (sifting through old documentation, searching program libraries, talking with IT staff and customers, looking at procurement records and talking with suppliers and contractors etc.). If a CMS or any sort of asset database exists, these may provide valuable sources of information, although they should be verified before inclusion within either the Service Portfolio or Service Catalogue. The Service Portfolio is produced as part of Service Strategy and should include participation by those involved in Service Design, Transition, Operation and Improvement. Once a service is 'chartered' (being developed for use by customers, Service Design produces the specifications for the service and it is at this point that the service should be added to the Service Catalogue).

Each organization should develop and maintain a policy with regard to both the Portfolio and the Catalogue, relating to the services recorded within them, what details are recorded and what statuses are recorded for each of the services. The policy should also contain details of responsibilities for each section of the overall Service Portfolio and the scope of each of the constituent sections.

The Service Catalogue Management process produces and maintains the Service Catalogue, ensuring that a central, accurate and consistent source of data is provided, recording the status of all operational services or services being transitioned to the live environment, together with appropriate details of each service.

What is a service? This question is not as easy to answer as it may first appear, and many organizations have failed to come up with a clear definition in an IT context. IT staff often confuse a 'service' as perceived by the customer with an IT system. In many cases one 'service' can be made up of other 'services' (and so on), which are themselves made up of one or more IT systems within an overall infrastructure including hardware, software, networks, together with environments, data and applications. A good starting point is often to ask customers which IT services they use and how those services map onto and support their business processes. Customers often have a greater clarity of what they believe a service to be. Each organization needs to develop a policy of what is a service and how it is defined and agreed within their own organization.

To avoid confusion, it may be a good idea to define a hierarchy of services within the Service Catalogue, by qualifying exactly what type of service is recorded, e.g. business service (that which is seen by the customer). Alternatively, supporting services, such as infrastructure services, network services, application services (all invisible to the customer, but essential to the delivery of IT services) will also need to be recorded. This often gives rise to a hierarchy of services incorporating customer services and other related services, including supporting services, shared services and commodity services, each with defined and agreed service levels.

When initially completed, the Service Catalogue may consist of a matrix, table or spreadsheet. Many organizations integrate and maintain their Service Portfolio and Service Catalogue as part of their CMS. By defining each service as a Configuration Item (CI) and, where appropriate, relating these to form a service hierarchy, the organization is able to relate events such as incidents and RFCs to the services affected, thus providing the basis for service monitoring and reporting using an integrated tool (e.g. 'list or give the number of incidents affecting this particular service'). It is therefore essential that changes within the Service Portfolio and Service Catalogue are subject to the Change Management process.

The Service Catalogue can also be used for other Service Management purposes (e.g. for performing a Business

Impact Analysis (BIA) as part of IT Service Continuity Planning, or as a starting place for re-distributing workloads, as part of Capacity Management). The cost and effort of producing and maintaining the catalogue, with its relationships to the underpinning technology components, is therefore easily justifiable. If done in conjunction with prioritization of the BIA, then it is possible to ensure that the most important services are covered first. An example of a simple Service Catalogue that can be used as a starting point is given in Appendix G.

The Service Catalogue has two aspects:

- **The Business Service Catalogue:** containing details of all the IT services delivered to the customer, together with relationships to the business units and the business process that rely on the IT services. This is the customer view of the Service Catalogue.
- **The Technical Service Catalogue:** containing details of all the IT services delivered to the customer, together with relationships to the supporting services, shared services, components and CIs necessary to support the provision of the service to the business. This should underpin the Business Service Catalogue and not form part of the customer view.

The relationship between these two aspects is illustrated in Figure 4.3.

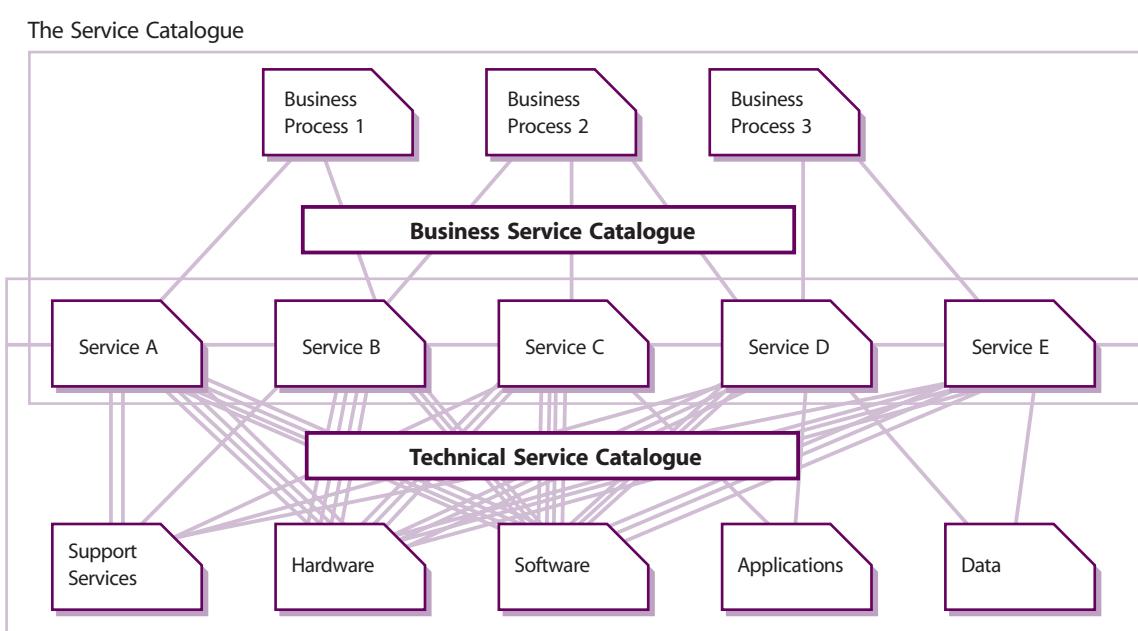


Figure 4.3 The Business Service Catalogue and the Technical Service Catalogue

Some organizations only maintain either a Business Service Catalogue or a Technical Service Catalogue. The preferred situation adopted by the more mature organizations maintains both aspects within a single Service Catalogue, which is part of a totally integrated Service Management activity and Service Portfolio. More information on the design and contents of a Service Catalogue is contained in Appendix G. The Business Service Catalogue facilitates the development of a much more proactive or even pre-emptive SLM process, allowing it to develop more into the field of Business Service Management. The Technical Service Catalogue is extremely beneficial when constructing the relationship between services, SLAs, OLAs and other underpinning agreements and components, as it will identify the technology required to support a service and the support group(s) that support the components. The combination of a Business Service Catalogue and a Technical Service Catalogue is invaluable for quickly assessing the impact of incidents and changes on the business. An example of relationships between the Business and Technical portions of a Service Catalogue is shown in Figure 4.4.

4.1.5 Process activities, methods and techniques

The key activities within the Service Catalogue Management process should include:

- Agreeing and documenting a service definition with all relevant parties
- Interfacing with Service Portfolio Management to agree the contents of the Service Portfolio and Service Catalogue
- Producing and maintaining a Service Catalogue and its contents, in conjunction with the Service Portfolio
- Interfacing with the business and IT Service Continuity Management on the dependencies of business units and their business processes with the supporting IT services, contained within the Business Service Catalogue
- Interfacing with support teams, suppliers and Configuration Management on interfaces and dependencies between IT services and the supporting services, components and CIs contained within the Technical Service Catalogue

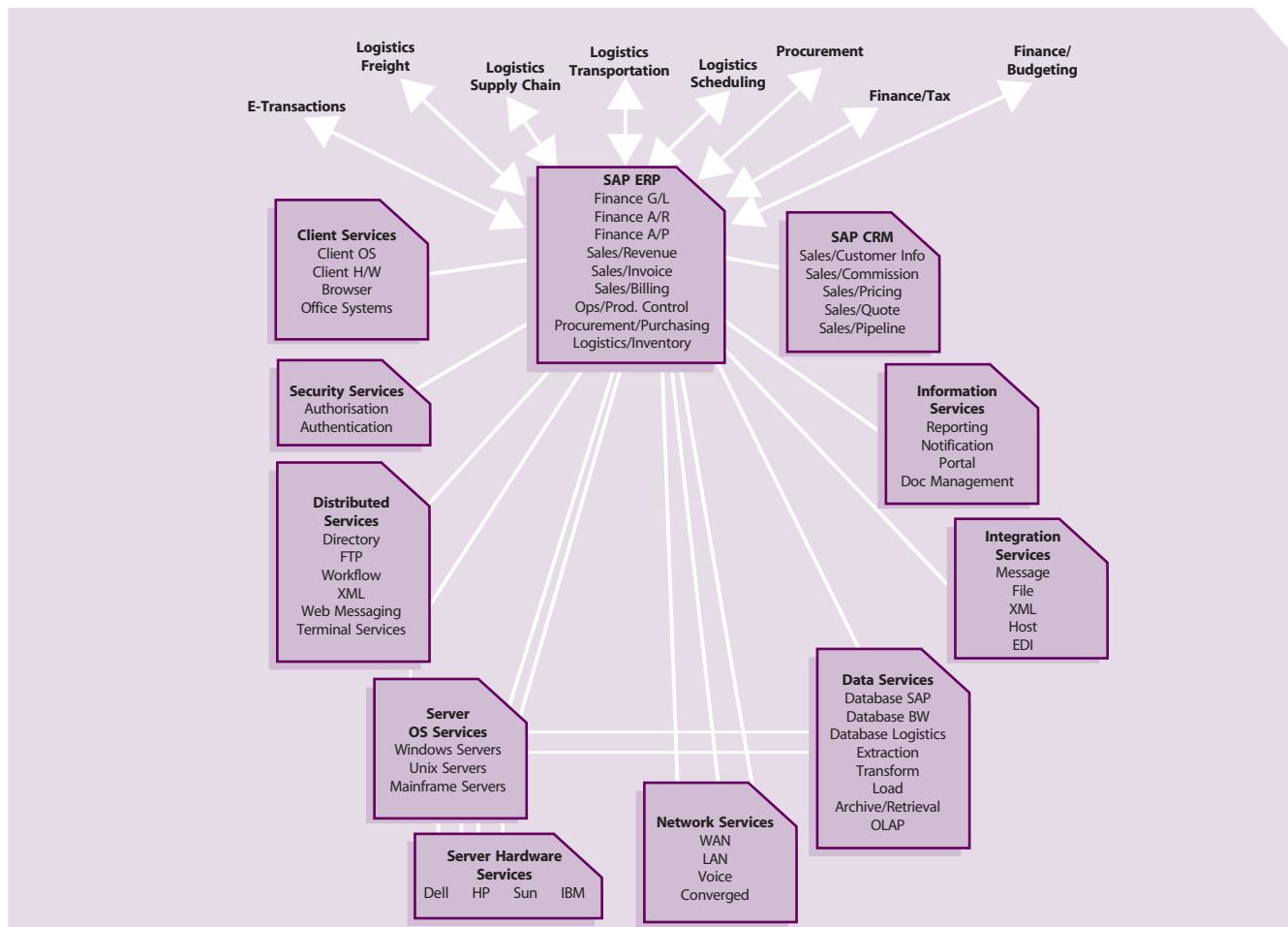


Figure 4.4 Example Service Catalogue

- Interfacing with Business Relationship Management and Service Level Management to ensure that the information is aligned to the business and business process.

4.1.6 Triggers, inputs, outputs and interfaces

There are a number of sources of information that are relevant to the Service Catalogue Management process. These should include:

- Business information from the organization's business and IT strategy, plans and financial plans, and information on their current and future requirements from the Service Portfolio
- Business Impact Analysis, providing information on the impact, priority and risk associated with each service or changes to service requirements
- Business requirements: details of any agreed, new or changed business requirements from the Service Portfolio
- The Service Portfolio
- The CMS
- Feedback from all other processes.

The triggers for the Service Catalogue Management process are changes in the business requirements and services, and therefore one of the main triggers is Request For Changes (RFCs) and the Change Management process. This will include new services, changes to existing services or services being retired.

The process outputs of SCM are:

- The documentation and agreement of a 'definition of the service'
- Updates to the Service Portfolio: should contain the current status of all services and requirements for services
- The Service Catalogue: should contain the details and the current status of every live service provided by the service provider or service being transitioned into the live environment, together with the interfaces and dependencies. An example of a Service Catalogue is contained in Appendix G.

4.1.7 Information management

The key information within the Service Catalogue Management process is that contained within the Service Catalogue. The main input for this information comes from the Service Portfolio and the business via either the Business Relationship Management (BRM) or Service Level Management (SLM) processes. This information needs to

be verified for accuracy before being recorded within the Service Catalogue. The information and the Service Catalogue itself need to be maintained using the Change Management process.

4.1.8 Key Performance Indicators

The two main Key Performance Indicators (KPIs) associated with the Service Catalogue and its management are:

- The number of services recorded and managed within the Service Catalogue as a percentage of those being delivered and transitioned in the live environment
- The number of variances detected between the information contained within the Service Catalogue and the 'real-world' situation.

Other measurements and KPIs that could be used are:

- Business users' awareness of the services being provided, i.e. percentage increase in completeness of the Business Service Catalogue against operational services
- IT staff awareness of the technology supporting the services:
 - Percentage increase in completeness of the Technical Service Catalogue against IT components that support the services
 - Service Desk having access to information to support all live services, measured by the percentage of incidents without the appropriate service-related information.

4.1.9 Challenges, Critical Success Factors and risks

The major challenge facing the Service Catalogue Management process is that of maintaining an accurate Service Catalogue as part of a Service Portfolio, incorporating both the Business Service Catalogue and the Technical Service Catalogue as part of an overall CMS and SKMS. This is best approached by developing stand-alone spreadsheets or databases before trying to integrate the Service Catalogue and Service Portfolio within the CMS or SKMS. In order to achieve this, the culture of the organization needs to accept that the Catalogue and Portfolio are essential sources of information that everyone within the IT organization needs to use and help maintain. This will often assist in the standardization of the Service Catalogue and the Service Portfolio and enable increase in cost performance through economies of scale.

The main Critical Success Factors for the Service Catalogue Management process are:

- An accurate Service Catalogue
- Business users' awareness of the services being provided
- IT staff awareness of the technology supporting the services.

The risks associated with the provision of an accurate Service Catalogue are:

- Inaccuracy of the data in the catalogue and it not being under rigorous Change control
- Poor acceptance of the Service Catalogue and its usage in all operational processes. The more active the catalogue is, the more likely it is to be accurate in its content
- Inaccuracy of information received from the business, IT and the Service Portfolio, with regard to service information
- The tools and resources required to maintain the information
- Poor access to accurate Change Management information and processes
- Poor access to and support of appropriate and up-to-date CMS and SKMS
- Circumvention of the use of the Service Portfolio and Service Catalogue
- The information is either too detailed to maintain accurately or at too high a level to be of any value. It should be consistent with the level of detail within the CMS and the SKMS.

4.2 SERVICE LEVEL MANAGEMENT

Service Level Management (SLM) negotiates, agrees and documents appropriate IT service targets with representatives of the business, and then monitors and produces reports on the service provider's ability to deliver the agreed level of service. SLM is a vital process for every IT service provider organization in that it is responsible for agreeing and documenting service level targets and responsibilities within SLAs and SLRs, for every activity within IT. If these targets are appropriate and accurately reflect the requirements of the business, then the service delivered by the service providers will align with business requirements and meet the expectations of the customers and users in terms of service quality. If the targets are not aligned with business needs, then service provider activities and service levels will not be aligned with business expectations and problems will develop. The SLA is effectively a level of assurance or warranty with regard to the level of service quality delivered by the service provider for each of the services delivered to the business.

The success of SLM is very dependent on the quality of the Service Portfolio and the Service Catalogue and their contents, because they provide the necessary information on the services to be managed within the SLM process.

4.2.1 Purpose/goal/objective

The goal of the Service Level Management process is to ensure that an agreed level of IT service is provided for all current IT services, and that future services are delivered to agreed achievable targets. Proactive measures are also taken to seek and implement improvements to the level of service delivered.

The purpose of the SLM process is to ensure that all operational services and their performance are measured in a consistent, professional manner throughout the IT organization, and that the services and the reports produced meet the needs of the business and customers.

The objectives of SLM are to:

- Define, document, agree, monitor, measure, report and review the level of IT services provided
- Provide and improve the relationship and communication with the business and customers
- Ensure that specific and measurable targets are developed for all IT services
- Monitor and improve customer satisfaction with the quality of service delivered
- Ensure that IT and the customers have a clear and unambiguous expectation of the level of service to be delivered
- Ensure that proactive measures to improve the levels of service delivered are implemented wherever it is cost-justifiable to do so.

4.2.2 Scope

SLM should provide a point of regular contact and communication to the customers and business managers of an organization. It should represent the IT service provider to the business, and the business to the IT service provider. This activity should encompass both the use of existing services and the potential future requirements for new or changed services. SLM needs to manage the expectation and perception of the business, customers and users and ensure that the quality of service delivered by the service provider is matched to those expectations and needs. In order to do this effectively, SLM should establish and maintain SLAs for all current live services and manage the level of service provided to meet the targets and quality measurements contained within the SLAs. SLM should also produce and agree SLRs for all planned new or changed services.

This will enable SLM to ensure that all the services and components are designed and delivered to meet their targets in terms of business needs. The SLM processes should include the:

- Development of relationships with the business
- Negotiation and agreement of current requirements and targets, and the documentation and management of SLAs for all operational services
- Negotiation and agreement of future requirements and targets, and the documentation and management of SLRs for all proposed new or changed services
- Development and management of appropriate Operational Level Agreements (OLAs) to ensure that targets are aligned with SLA targets
- Review of all underpinning supplier contracts and agreements with Supplier Management to ensure that targets are aligned with SLA targets
- Proactive prevention of service failures, reduction of service risks and improvement in the quality of service, in conjunction with all other processes
- Reporting and management of all services and review of all SLA breaches and weaknesses
- Instigation and coordination of a Service Improvement Plan (SIP) for the management, planning and implementation of all service and process improvements.

4.2.3 Value to the business

SLM provides a consistent interface to the business for all service-related issues. It provides the business with the agreed service targets and the required management information to ensure that those targets have been met. Where targets are breached, SLM should provide feedback on the cause of the breach and details of the actions taken to prevent the breach from recurring. Thus SLM provides a reliable communication channel and a trusted relationship with the appropriate customers and business representatives.

4.2.4 Policies/principles/basic concepts

SLM is the name given to the processes of planning, coordinating, drafting, agreeing, monitoring and reporting of SLAs, and the ongoing review of service achievements to ensure that the required and cost-justifiable service quality is maintained and gradually improved. However, SLM is not only concerned with ensuring that current services and SLAs are managed, but it is also involved in ensuring that new requirements are captured and that new or changed services and SLAs are developed to match the business needs and expectations. SLAs provide the

basis for managing the relationship between the service provider and the customer, and SLM provides that central point of focus for a group of customers, business units or lines of business.

An SLA is a written agreement between an IT service provider and the IT customer(s), defining the key service targets and responsibilities of both parties. The emphasis must be on agreement, and SLAs should not be used as a way of holding one side or the other to ransom. A true partnership should be developed between the IT service provider and the customer, so that a mutually beneficial agreement is reached – otherwise the SLA could quickly fall into disrepute and a ‘blame culture’ could develop that would prevent any true service quality improvements from taking place.

SLM is also responsible for ensuring that all targets and measures agreed in SLAs with the business are supported by appropriate underpinning OLAs or contracts, with internal support units and external partners and suppliers. This is illustrated in Figure 4.5.

Figure 4.5 shows the relationship between the business and its processes and the services, and the associated technology, supporting services, teams and suppliers required to meet their needs. It demonstrates how important the SLAs, OLAs and contracts are in defining and achieving the level of service required by the business.

An OLA is an agreement between an IT service provider and another part of the same organization that assists with the provision of services – for instance, a facilities department that maintains the air conditioning, or network support team that supports the network service. An OLA should contain targets that underpin those within an SLA to ensure that targets will not be breached by failure of the supporting activity.

4.2.5 Process activities, methods and techniques

The key activities within the SLM process should include:

- Determine, negotiate, document and agree requirements for new or changed services in SLRs, and manage and review them through the Service Lifecycle into SLAs for operational services
- Monitor and measure service performance achievements of all operational services against targets within SLAs
- Collate, measure and improve customer satisfaction
- Produce service reports

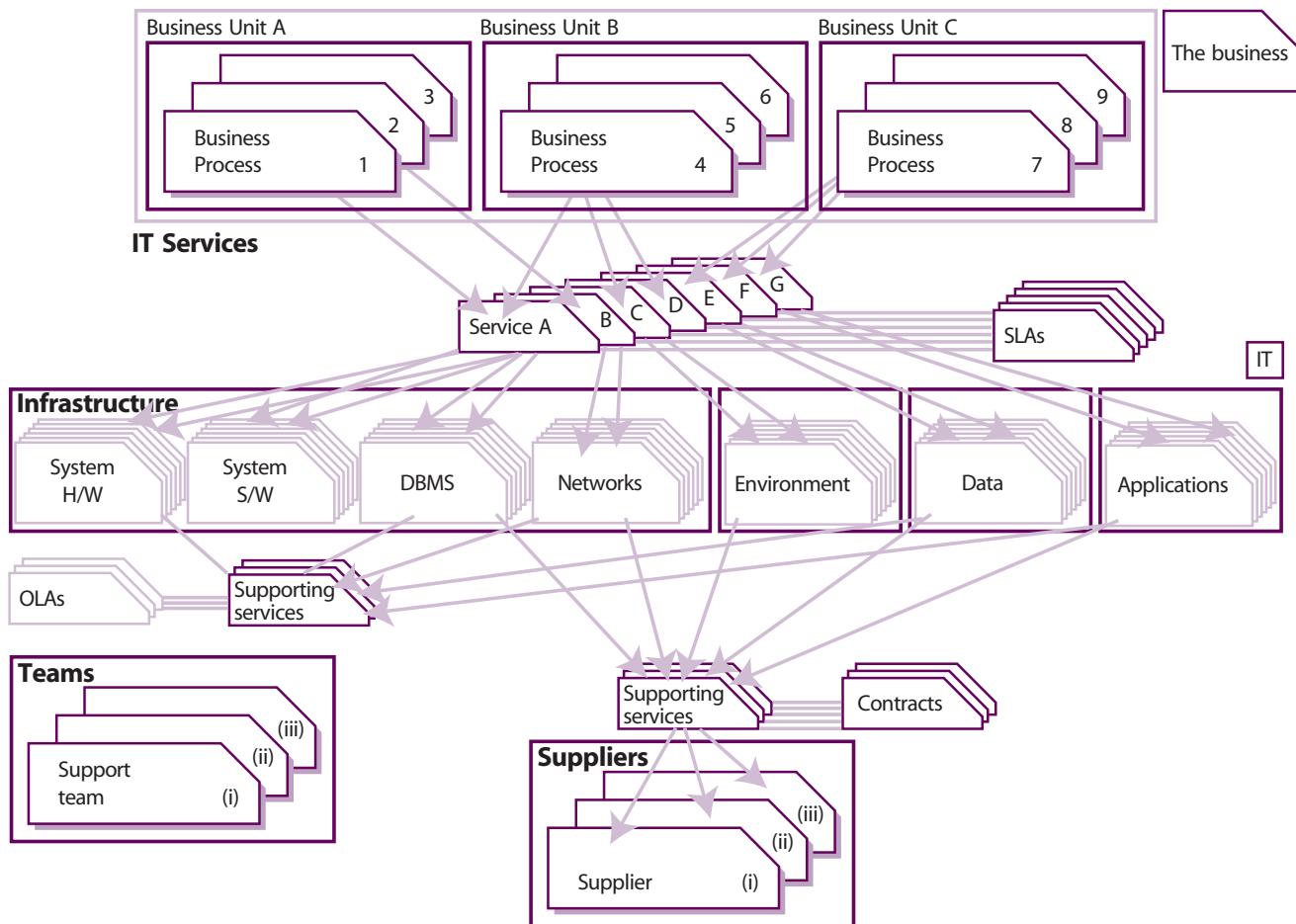


Figure 4.5 Service Level Management

- Conduct service review and instigate improvements within an overall Service Improvement Plan (SIP)
- Review and revise SLAs, service scope OLAs, contracts, and any other underpinning agreements
- Develop and document contacts and relationships with the business, customers and stakeholders
- Develop, maintain and operate procedures for logging, actioning and resolving all complaints, and for logging and distributing compliments
- Log and manage all complaints and compliments
- Provide the appropriate management information to aid performance management and demonstrate service achievement
- Make available and maintain up-to-date SLM document templates and standards.

The interfaces between the main activities are illustrated in Figure 4.6.

Although Figure 4.6 illustrates all the main activities of SLM as separate activities, they should be implemented as one integrated SLM process that can be consistently

applied to all areas of the businesses and to all customers. These activities are described in the following sections.

4.2.5.1 Designing SLA frameworks

Using the Service Catalogue as an aid, SLM must design the most appropriate SLA structure to ensure that all services and all customers are covered in a manner best suited to the organization's needs. There are a number of potential options, including the following.

Service-based SLA

This is where an SLA covers one service, for all the customers of that service – for example, an SLA may be established for an organization's e-mail service – covering all the customers of that service. This may appear fairly straightforward. However, difficulties may arise if the specific requirements of different customers vary for the same service, or if characteristics of the infrastructure mean that different service levels are inevitable (e.g. head office staff may be connected via a high-speed LAN, while local offices may have to use a lower-speed WAN line). In such cases, separate targets may be needed within the

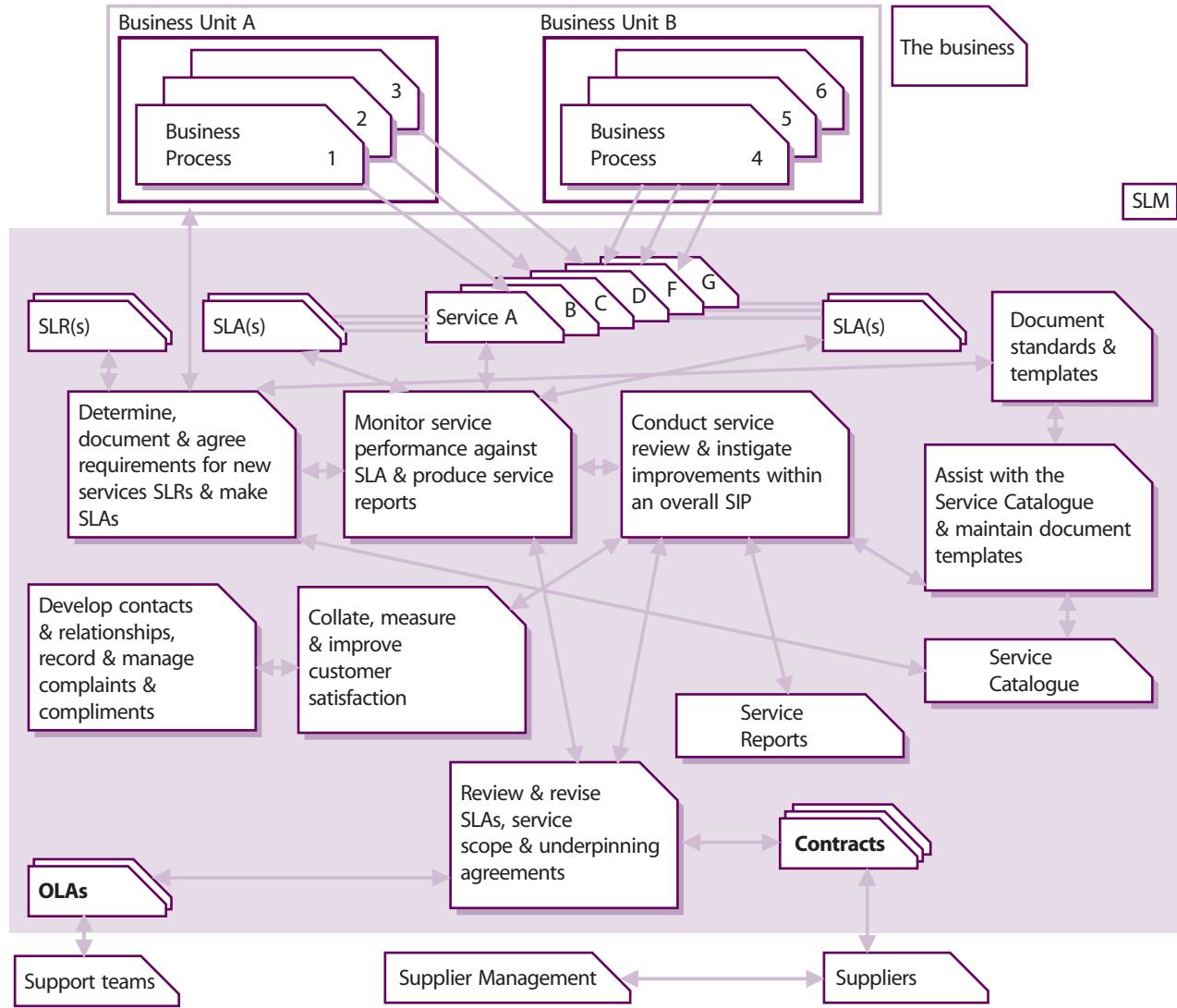


Figure 4.6 The Service Level Management process

one agreement. Difficulties may also arise in determining who should be the signatories to such an agreement. However, where common levels of service are provided across all areas of the business, e.g. e-mail or telephony, the service-based SLA can be an efficient approach to use. Multiple classes of service, e.g. gold, silver and bronze, can also be used to increase the effectiveness of service-based SLAs.

Customer-based SLA

This is an agreement with an individual customer group, covering all the services they use. For example, agreements may be reached with an organization's finance department covering, say, the finance system, the accounting system, the payroll system, the billing system, the procurement system, and any other IT systems that they use. Customers often prefer such an agreement, as all of their requirements are covered in a single document.

Only one signatory is normally required, which simplifies this issue.

Hints and tips

A combination of either of these structures might be appropriate, providing all services and customers are covered, with no overlap or duplication.

Multi-level SLAs

Some organizations have chosen to adopt a multi-level SLA structure. For example, a three-layer structure as follows:

- **Corporate level:** covering all the generic SLM issues appropriate to every customer throughout the organization. These issues are likely to be less volatile, so updates are less frequently required

- **Customer level:** covering all SLM issues relevant to the particular customer group or business unit, regardless of the service being used
- **Service level:** covering all SLM issues relevant to the specific service, in relation to a specific customer group (one for each service covered by the SLA).

As shown in Figure 4.7, such a structure allows SLAs to be kept to a manageable size, avoids unnecessary duplication, and reduces the need for frequent updates. However, it does mean that extra effort is required to maintain the necessary relationships and links within the Service Catalogue and the CMS.

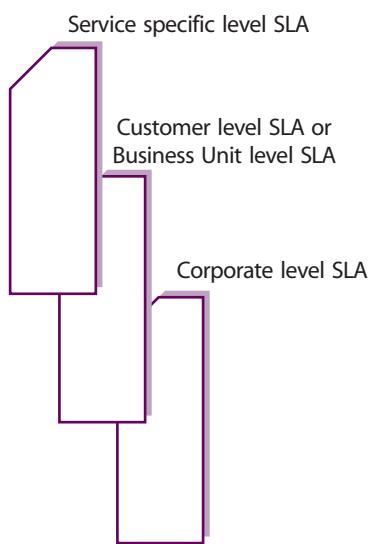


Figure 4.7 Multi-level SLAs

Many organizations have found it valuable to produce standards and a set of proformas or templates that can be used as a starting point for all SLAs, SLRs and OLAs. The proforma can often be developed alongside the draft SLA. Guidance on the items to be included in an SLA is given in Appendix F. Developing standards and templates will ensure that all agreements are developed in a consistent manner, and this will ease their subsequent use, operation and management.

Hints and tips

Make roles and responsibilities a part of the SLA. Consider three perspectives – the IT provider, the IT customer and the actual users.

The wording of SLAs should be clear and concise and leave no room for ambiguity. There is normally no need for agreements to be written in legal terminology, and plain language aids a common understanding. It is often helpful to have an independent person, who has not been

involved with the drafting, to do a final read-through. This often throws up potential ambiguities and difficulties that can then be addressed and clarified. For this reason alone, it is recommended that all SLAs contain a glossary, defining any terms and providing clarity for any areas of ambiguity.

It is also worth remembering that SLAs may have to cover services offered internationally. In such cases the SLA may have to be translated into several languages. Remember also that an SLA drafted in a single language may have to be reviewed for suitability in several different parts of the world (i.e. a version drafted in Australia may have to be reviewed for suitability in the USA or the UK – and differences in terminology, style and culture must be taken into account).

Where the IT services are provided to another organization by an external service provider, sometimes the service targets are contained within a contract and at other times they are contained within an SLA or schedule attached to the contract. Whatever document is used, it is essential that the targets documented and agreed are clear, specific and unambiguous, as they will provide the basis of the relationship and the quality of service delivered.

4.2.5.2 Determine, document and agree requirements for new services and produce SLRs

This is one of the earliest activities within the Service Design stage of the Service Lifecycle. Once the Service Catalogue has been produced and the SLA structure has been agreed, a first SLR must be drafted. It is advisable to involve customers from the outset, but rather than going along with a blank sheet to start with, it may be better to produce a first outline draft of the performance targets and the management and operational requirements, as a starting point for more detailed and in-depth discussion. Be careful, though, not to go too far and appear to be presenting the customer with a ‘fait accompli’.

It cannot be over-stressed how difficult this activity of determining the initial targets for inclusion with an SLR or SLA is. All of the other processes need to be consulted for their opinion on what are realistic targets that can be achieved, such as Incident Management on incident targets. The Capacity and Availability Management processes will be of particular value in determining appropriate service availability and performance targets. If there is any doubt, provisional targets should be included within a pilot SLA that is monitored and adjusted through a service warranty period, as illustrated in Figure 3.5.

While many organizations have to give initial priority to introducing SLAs for existing services, it is also important

to establish procedures for agreeing Service Level Requirements (SLRs) for new services being developed or procured.

The SLRs should be an integral part of the Service Design criteria, of which the functional specification is a part. They should, from the very start, form part of the testing/trialling criteria as the service progresses through the stages of design and development or procurement. This SLR will gradually be refined as the service progresses through the stages of its lifecycle, until it eventually becomes a pilot SLA during the early life support period. This pilot or draft SLA should be developed alongside the service itself, and should be signed and formalized before the service is introduced into live use.

It can be difficult to draw out requirements, as the business may not know what they want – especially if not asked previously – and they may need help in understanding and defining their needs, particularly in terms of capacity, security, availability and IT service continuity. Be aware that the requirements initially expressed may not be those ultimately agreed. Several iterations of negotiations may be required before an affordable balance is struck between what is sought and what is achievable and affordable. This process may involve a redesign of the service solution each time.

If new services are to be introduced in a seamless way into the live environment, another area that requires attention is the planning and formalization of the support arrangements for the service and its components. Advice should be sought from Change Management and Configuration Management to ensure the planning is comprehensive and covers the implementation, deployment and support of the service and its components. Specific responsibilities need to be defined and added to existing contracts/OLAs, or new ones need to be agreed. The support arrangements and all escalation routes also need adding to the CMS, including the Service Catalogue where appropriate, so that the Service Desk and other support staff are aware of them. Where appropriate, initial training and familiarization for the Service Desk and other support groups and knowledge transfer should be completed before live support is needed.

It should be noted that additional support resources (i.e. more staff) may be needed to support new services. There is often an expectation that an already overworked support group can magically cope with the additional effort imposed by a new service.

Using the draft agreement as a basis, negotiations must be held with the customer(s), or customer representatives to finalize the contents of the SLA and the initial service level

targets, and with the service providers to ensure that these are achievable.

4.2.5.3 Monitor service performance against SLA

Nothing should be included in an SLA unless it can be effectively monitored and measured at a commonly agreed point. The importance of this cannot be overstressed, as inclusion of items that cannot be effectively monitored almost always results in disputes and eventual loss of faith in the SLM process. A lot of organizations have discovered this the hard way and as a result have absorbed heavy costs, both in a financial sense as well as in terms of negative impacts on their credibility.

Anecdote

A global network provider agreed availability targets for the provision of a managed network service. These availability targets were agreed at the point where the service entered the customer's premises. However, the global network provider could only monitor and measure availability at the point the connection left its premises. The network links were provided by a number of different national telecommunications service providers, with widely varying availability levels. The result was a complete mismatch between the availability figures produced by the network provider and the customer, with correspondingly prolonged and heated debate and argument.

Existing monitoring capabilities should be reviewed and upgraded as necessary. Ideally this should be done ahead of, or in parallel with, the drafting of SLAs, so that monitoring can be in place to assist with the validation of proposed targets.

It is essential that monitoring matches the customer's true perception of the service. Unfortunately this is often very difficult to achieve. For example, monitoring of individual components, such as the network or server, does not guarantee that the service will be available so far as the customer is concerned. Customer perception is often that although a failure might affect more than one service, all they are bothered about is the service they cannot access at the time of the reported incident – though this is not always true, so caution is needed. Without monitoring all components in the end-to-end service (which may be very difficult and costly to achieve) a true picture cannot be gained. Similarly, users must be aware that they should report incidents immediately to aid diagnostics, especially if they are performance-related, so that the service provider is aware that service targets are being breached.

A considerable number of organizations use their Service Desk, linked to a comprehensive CMS, to monitor the customer's perception of availability. This may involve making specific changes to incident/problem logging screens and may require stringent compliance with incident logging procedures. All of this needs discussion and agreement with the Availability Management process.

The Service Desk is also used to monitor incident response times and resolution times, but once again the logging screen may need amendment to accommodate data capture, and call-logging procedures may need tightening and must be strictly followed. If support is being provided by a third party, this monitoring may also underpin Supplier Management.

It is essential to ensure that any incident/problem-handling targets included in SLAs are the same as those included in Service Desk tools and used for escalation and monitoring purposes. Where organizations have failed to recognize this, and perhaps used defaults provided by the tool supplier, they have ended up in a situation where they are monitoring something different from that which has been agreed in the SLAs, and are therefore unable to say whether SLA targets have been met, without considerable effort to manipulate the data. Some amendments may be needed to support tools, to include the necessary fields so that relevant data can be captured.

Another notoriously difficult area to monitor is transaction response times (the time between sending a screen and receiving a response). Often end-to-end response times are technically very difficult to monitor. In such cases it may be appropriate to deal with this as follows:

- Include a statement in the SLA along the following lines: 'The services covered by the SLA are designed for high-speed response and no significant delays should be encountered. If a response time delay of more than x seconds is experienced for more than y minutes, this should be reported immediately to the Service Desk'.
- Agree and include in the SLA an acceptable target for the number of such incidents that can be tolerated in the reporting period.
- Create an incident category of 'poor response' (or similar) and ensure that any such incidents are logged accurately and that they are related to the appropriate service.
- Produce regular reports of occasions where SLA transaction response time targets have been breached, and instigate investigations via Problem Management to correct the situation.

This approach not only overcomes the technical difficulties of monitoring, but also ensures that incidents of poor response are reported at the time they occur. This is very important, as poor response is often caused by a number of transient interacting events that can only be detected if they are investigated immediately.

The preferred method, however, is to implement some form of automated client/server response time monitoring in close consultation with the Service Operation. Wherever possible, implement sampling or 'robot' tools and techniques to give indications of slow or poor performance. These tools provide the ability to measure or sample actual or very similar response times to those being experienced by a variety of users, and are becoming increasingly available and increasingly more cost-effective to use.

Hints and tips

Some organizations have found that, in reality, 'poor response' is sometimes a problem of user perception. The user, having become used to a particular level of response over a period of time, starts complaining as soon as this is slower. Take the view that 'if the user thinks the service is slow, then it is'.

If the SLA includes targets for assessing and implementing Requests for Change (RFCs), the monitoring of targets relating to Change Management should ideally be carried out using whatever Change Management tool is in use (preferably part of an integrated Service Management support tool) and change logging screens and escalation processes should support this.

4.2.5.4 Collate, measure and improve customer satisfaction

There are a number of important 'soft' issues that cannot be monitored by mechanistic or procedural means, such as customers' overall feelings (these need not necessarily match the 'hard' monitoring). For example, even when there have been a number of reported service failures, the customers may still feel positive about things, because they may feel satisfied that appropriate actions are being taken to improve things. Of course, the opposite may apply, and customers may feel dissatisfied with some issues (e.g. the manner of some staff on the Service Desk) when few or no SLA targets have been broken.

From the outset, it is wise to try and manage customers' expectations. This means setting proper expectations and appropriate targets in the first place, and putting a systematic process in place to manage expectations going forward, as satisfaction = perception – expectation (where a zero or positive score indicates a satisfied customer).

SLAs are just documents, and in themselves do not materially alter the quality of service being provided (though they may affect behaviour and help engender an appropriate service culture, which can have an immediate beneficial effect, and make longer-term improvements possible). A degree of patience is therefore needed and should be built into expectations.

Where charges are being made for the services provided, this should modify customer demands. (Customers can have whatever they can cost-justify – providing it fits within agreed corporate strategy – and have authorized budget for, but no more.) Where direct charges are not made, the support of senior business managers should be enlisted to ensure that excessive or unrealistic demands are not placed on the IT provider by any individual customer group.

It is therefore recommended that attempts be made to monitor customer perception on these soft issues.

Methods of doing this include:

- Periodic questionnaires and customer surveys
- Customer feedback from service review meetings
- Feedback from Post Implementation Reviews (PIRs) conducted as part of the Change Management process on major changes, releases, new or changed services, etc.
- Telephone perception surveys (perhaps at random on the Service Desk, or using regular customer liaison representatives)
- Satisfaction survey handouts (left with customers following installations, service visits, etc.)
- User group or forum meetings
- Analysis of complaints and compliments.

Where possible, targets should be set for these and monitored as part of the SLA (e.g. an average score of 3.5 should be achieved by the service provider on results given, based on a scoring system of 1 to 5, where 1 is poor performance and 5 is excellent). Ensure that if users provide feedback they receive some return, and demonstrate to them that their comments have been incorporated in an action plan, perhaps a SIP. All customer satisfaction measurements should be reviewed, and where variations are identified, they should be analysed with action taken to rectify the variation.

4.2.5.5 Review and revise underpinning agreements and service scope

IT service providers are dependent to some extent on their own internal technical support teams or on external partners or suppliers. They cannot commit to meeting SLA

targets unless their own support team's and suppliers' performances underpin these targets. Contracts with external suppliers are mandatory, but many organizations have also identified the benefits of having simple agreements with internal support groups, usually referred to as OLAs. 'Underpinning agreements' is a term used to refer to all underpinning OLAs, SLAs and contracts.

Often these agreements are referred to as 'back-to-back' agreements. This is to reflect the need to ensure that all targets within underpinning or 'back-to-back' agreements are aligned with, and support, targets agreed with the business in SLAs or OLAs. There may be several layers of these underpinning or 'back-to-back' agreements with aligned targets. It is essential that the targets at each layer are aligned with, and support, the targets contained within the higher levels (i.e. those closest to the business targets).

OLAs need not be very complicated, but should set out specific back-to-back targets for support groups that underpin the targets included in SLAs. For example, if the SLA includes overall time to respond and fix targets for incidents (varying on the priority levels), then the OLAs should include targets for each of the elements in the support chain. It must be understood, however, that the incident resolution targets included in SLAs should not normally match the same targets included in contracts or OLAs with suppliers. This is because the SLA targets must include an element for all stages in the support cycle (e.g. detection time, Service Desk logging time, escalation time, referral time between groups etc, Service Desk review and closure time – as well as the actual time fixing the failure).

The SLA target should cover the time taken to answer calls, escalate incidents to technical support staff, and the time taken to start to investigate and to resolve incidents assigned to them. In addition, overall support hours should be stipulated for all groups that underpin the required service availability times in the SLA. If special procedures exist for contacted staff (e.g. out-of-hours telephone support) these must also be documented.

OLAs should be monitored against OLA and SLA targets, and reports on achievements provided as feedback to the appropriate managers of each support team. This highlights potential problem areas, which may need to be addressed internally or by a further review of the SLA or OLA. Serious consideration should be given to introducing formal OLAs for all internal support teams, which contribute to the support of operational services.

Before committing to new or revised SLAs, it is therefore important that existing contractual arrangements are investigated and, where necessary, upgraded. This is likely to incur additional costs, which must either be absorbed

by IT or passed on to the customer. In the latter case, the customer must agree to this, or the more relaxed targets in existing contracts should be agreed for inclusion in SLAs. This activity needs to be completed in close consultation with the Supplier Management process, to ensure not only that SLM requirements are met, but also that all other process requirements are considered, particularly supplier and contractual policies and standards.

4.2.5.6 Produce service reports

Immediately after the SLA is agreed and accepted, monitoring must be instigated, and service achievement reports must be produced. Operational reports must be produced frequently (weekly – perhaps even more frequently) and, where possible, exception reports should be produced whenever an SLA has been broken (or threatened, if appropriate thresholds have been set to give an ‘early warning’). Sometimes difficulties are encountered in meeting the targets of new services during the early life support period because of the high volume of RFCs. Limiting the number of RFCs processed during the early life support period can limit the impact of changes.

The SLA reporting mechanisms, intervals and report formats must be defined and agreed with the customers. The frequency and format of Service Review Meetings must also be agreed with the customers. Regular intervals are recommended, with periodic reports synchronized with the reviewing cycle.

Periodic reports must be produced and circulated to customers (or their representatives) and appropriate IT managers a few days in advance of service level reviews, so that any queries or disagreements can be resolved ahead of the review meeting. The meeting is not then diverted by such issues.

The periodic reports should incorporate details of performance against all SLA targets, together with details of any trends or specific actions being undertaken to improve service quality. A useful technique is to include a SLA Monitoring (SLAM) chart at the front of a service report to give an ‘at-a-glance’ overview of how achievements have measured up against targets. These are most effective if colour coded (Red, Amber, Green, and sometimes referred to as RAG charts as a result). Other interim reports may be required by IT management for OLA or internal performance reviews and/or supplier or contract management. This is likely to be an evolving process – a first effort is unlikely to be the final outcome.

The resources required to produce and verify reports should not be underestimated. It can be extremely time-

consuming, and if reports do not reflect the customer’s own perception of service quality accurately, they can make the situation worse. It is essential that accurate information from all areas and all processes (e.g. Incident Management, Problem Management, Availability Management, Capacity Management, Change and Configuration Management) is analysed and collated into a concise and comprehensive report on service performance, as measured against agreed business targets.

SLM should identify the specific reporting needs and automate production of these reports, as far as possible. The extent, accuracy and ease with which automated reports can be produced should form part of the selection criteria for integrated support tools. These service reports should not only include details of current performance against targets, but should also provide historic information on past performance and trends, so that the impact of improvement actions can be measured and predicted.

4.2.5.7 Conduct service reviews and instigate improvements within an overall SIP

Periodic review meetings must be held on a regular basis with customers (or their representatives) to review the service achievement in the last period and to preview any issues for the coming period. It is normal to hold such meetings monthly or, as a minimum, quarterly.

Actions must be placed on the customer and provider as appropriate to improve weak areas where targets are not being met. All actions must be minuted, and progress should be reviewed at the next meeting to ensure that action items are being followed up and properly implemented.

Particular attention should be focused on each breach of service level to determine exactly what caused the loss of service and what can be done to prevent any recurrence. If it is decided that the service level was, or has become, unachievable, it may be necessary to review, renegotiate, review-agree different service targets. If the service break has been caused by a failure of a third-party or internal support group, it may also be necessary to review the underpinning agreement or OLA. Analysis of the cost and impact of service breaches provides valuable input and justification of SIP activities and actions. The constant need for improvement needs to be balanced and focused on those areas most likely to give the greatest business benefit.

Reports should also be produced on the progress and success of the SIP, such as the number of SIP actions that were completed and the number of actions that delivered their expected benefit.

Hints and tips

'A spy in both camps' – Service Level Managers can be viewed with a certain amount of suspicion by both the IT service provider staff and the customer representatives. This is due to the dual nature of the job, where they are acting as an unofficial customer representative when talking to IT staff, and as an IT provider representative when talking to the customers. This is usually aggravated when having to represent the 'opposition's' point of view in any meeting etc. To avoid this the Service Level Manager should be as open and helpful as possible (within the bounds of any commercial propriety) when dealing with both sides, although colleagues should never be openly criticized.

4.2.5.8 Review and revise SLAs, service scope and underpinning agreements

All agreements and underpinning agreements, including SLAs, underpinning contracts and OLAs, must be kept up-to-date. They should be brought under Change and Configuration Management control and reviewed periodically, at least annually, to ensure that they are still current and comprehensive, and are still aligned to business needs and strategy.

These reviews should ensure that the services covered and the targets for each are still relevant – and that nothing significant has changed that invalidates the agreement in any way (this should include infrastructure changes, business changes, supplier changes, etc.). Where changes are made, the agreements must be updated under Change Management control to reflect the new situation. If all agreements are recorded as CIs within the CMS, it is easier to assess the impact and implement the changes in a controlled manner.

These reviews should also include the overall strategy documents, to ensure that all services and service agreements are kept in line with business and IT strategies and policies.

4.2.5.9 Develop contacts and relationships

It is very important that SLM develops trust and respect with the business, especially with the key business contacts. Using the Service Catalogue, especially the Business Service Catalogue element of it, enables SLM to be much more proactive. The Service Catalogue provides the information that enables SLM to understand the relationships between the services and the business units and business process that depend on those services. It should also provide the information on all the key

business and IT contacts relating to the services, their use and their importance. In order to ensure that this is done in a consistent manner, SLM should perform the following activities:

- Confirm stakeholders, customers and key business managers and service users.
- Assist with maintaining accurate information within the Service Portfolio and Service Catalogue.
- Be flexible and responsive to the needs of the business, customers and users, and understand current and planned new business processes and their requirements for new or changed services, documenting and communicating these requirements to all other processes as well as facilitating and innovating change wherever there is business benefit.
- Develop a full understanding of business, customer and user strategies, plans, business needs and objectives, ensuring that IT are working in partnership with the business, customers and users, developing long-term relationships.
- Regularly take the customer journey and sample the customer experience, providing feedback on customer issues to IT. (This applies to both IT customers and also the external business customers in their use of IT services).
- Ensure that the correct relationship processes are in place to achieve objectives and that they are subjected to continuous improvement.
- Conduct and complete customer surveys, assist with the analysis of the completed surveys and ensure that actions are taken on the results.
- Act as an IT representative on organizing and attending user groups.
- Proactively market and exploit the Service Portfolio and Service Catalogue and the use of the services within all areas of the business.
- Work with the business, customers and users to ensure that IT provides the most appropriate levels of service to meet business needs currently and in the future.
- Promote service awareness and understanding.
- Raise the awareness of the business benefits to be gained from the exploitation of new technology.
- Facilitate the development and negotiation of appropriate, achievable and realistic SLRs and SLAs between the business and IT.
- Ensure the business, customers and users understand their responsibilities/commitments to IT (i.e. IT dependencies).
- Assist with the maintenance of a register of all outstanding improvements and enhancements.

4.2.5.10 Complaints and compliments

The SLM process should also include activities and procedures for the logging and management of all complaints and compliments. The logging procedures are often performed by the Service Desk as they are similar to those of Incident Management and Request Fulfilment. The definition of a complaint and compliment should be agreed with the customers, together with agreed contact points and procedures for their management and analysis. All complaints and compliments should be recorded and communicated to the relevant parties. All complaints should also be actioned and resolved to the satisfaction of the originator. If not, there should be an escalation contact and procedure for all complaints that are not actioned and resolved within an appropriate timescale. All outstanding complaints should be reviewed and escalated to senior management where appropriate. Reports should also be produced on the numbers and types of complaints, the trends identified and actions taken to reduce the numbers received. Similar reports should also be produced for compliments.

4.2.6 Triggers, inputs, outputs and interfaces

There are many triggers that instigate SLM activity. These include:

- Changes in the Service Portfolio, such as new or changed business requirements or new or changed services
- New or changed agreements, SLRs, SLAs, OLAs or contracts
- Service review meetings and actions
- Service breaches or threatened breaches
- Compliments and complaints
- Periodic activities such as reviewing, reporting and customer satisfaction surveys
- Changes in strategy or policy.

4.2.6.1 SLM process inputs

There are a number of sources of information that are relevant to the Service Level Management process. These should include:

- Business information: from the organization's business strategy, plans, and financial plans and information on their current and future requirements
- Business Impact Analysis: providing information on the impact, priority, risk and number of users associated with each service
- Business requirements: details of any agreed, new or

changed business requirements

- The strategies, policies and constraints from Service Strategy
- The Service Portfolio and Service Catalogue
- Change information: from the Change Management process with a forward schedule of changes and a need to assess all changes for their impact on all services
- CMS: containing information on the relationships between the business services, the supporting services and the technology
- Customer and user feedback, complaints and compliments
- Other inputs: including advice, information and input from any of the other processes (e.g. Incident Management, Capacity Management and Availability Management), together with the existing SLAs, SLRs, and OLAs and past service reports on the quality of service delivered.

4.2.6.2 SLM process outputs

The outputs of Service Level Management should include:

- Service reports: providing details of the service levels achieved in relation to the targets contained within SLAs. These reports should contain details of all aspects of the service and its delivery, including current and historical performance, breaches and weaknesses, major events, changes planned, current and predicted workloads, customer feedback, and improvement plans and activities
- Service Improvement Plan (SIP): an overall programme or plan of prioritized improvement actions, encompassing all services and all processes, together with associated impacts and risks
- The Service Quality Plan: documenting and planning the overall improvement of service quality
- Document templates: standard document templates, format and content for SLAs, SLRs and OLAs, aligned with corporate standards
- Service Level Agreements (SLAs): a set of targets and responsibilities should be documented and agreed within an SLA for each operational service
- Service Level Requirements (SLRs): a set of targets and responsibilities should be documented and agreed within an SLR for each proposed new or changed service
- Operational Level Agreements (OLAs): a set of targets and responsibilities should be documented and agreed within an OLA for each internal support team
- Reports on OLAs and underpinning contracts

- Service review meeting minutes and actions: all meetings should be scheduled on a regular basis, with planned agendas and their discussions and actions recorded and progressed
- SLA review and service scope review meeting minutes: summarizing agreed actions and revisions to SLAs and service scope
- Revised contracts: changes to SLAs or new SLRs may require existing underpinning contracts to be changed, or new contracts to be negotiated and agreed.

4.2.7 Key Performance Indicators

Key Performance Indicators (KPIs) and metrics can be used to judge the efficiency and effectiveness of the SLM activities and the progress of the SIP. These metrics should be developed from the service, customer and business perspective and should cover both subjective and objective measurements such as the following.

Objective:

- Number or percentage of service targets being met
- Number and severity of service breaches
- Number of services with up-to-date SLAs
- Number of services with timely reports and active service reviews.

Subjective:

- Improvements in customer satisfaction.

More information on KPIs, measurements and improvements can be found in the following section and in the Continuous Service Improvement publication.

Hints and tips

Don't fall into the trap of using percentages as the only metric. It is easy to get caught out when there is a small system with limited measurement points (i.e. a single failure in a population of 100 is only 1%; a single failure in a population of 50 is 2% – if the target is 98.5%, then the SLA is already breached). Always go for number of incidents rather than a percentage on populations of less than 100, and be careful when targets are accepted. This is something organizations have learned the hard way.

The SLM process often generates a good starting point for a SIP – and the service review process may drive this, but all processes and all areas of the service provider organization should be involved in the SIP.

Where an underlying difficulty has been identified that is adversely impacting on service quality, SLM must, in conjunction with Problem Management and Availability

Management, instigate a SIP to identify and implement whatever actions are necessary to overcome the difficulties and restore service quality. SIP initiatives may also focus on such issues as user training, service and system testing and documentation. In these cases, the relevant people need to be involved and adequate feedback given to make improvements for the future. At any time, a number of separate initiatives that form part of the SIP may be running in parallel to address difficulties with a number of services.

Some organizations have established an up-front annual budget held by SLM from which SIP initiatives can be funded. This means that action can be undertaken quickly and that SLM is demonstrably effective. This practice should be encouraged and expanded to enable SLM to become increasingly proactive and predictive. The SIP needs to be owned and managed, with all improvement actions being assessed for risk and impact on services, customers and the business, and then prioritized, scheduled and implemented.

If an organization is outsourcing its Service Delivery to a third party, the issue of service improvement should be discussed at the outset and covered (and budgeted for) in the contract, otherwise there is no incentive during the lifetime of the contract for the supplier to improve service targets if they are already meeting contractual obligations and additional expenditure is needed to make the improvements.

4.2.7.1 KPIs

Manage the overall quality of IT service needed, both in the number and level of services provided and managed:

- Percentage reduction in SLA targets missed
- Percentage reduction in SLA targets threatened
- Percentage increase in customer perception and satisfaction of SLA achievements, via service reviews and Customer Satisfaction Survey responses
- Percentage reduction in SLA breaches caused because of third-party support contracts (underpinning contracts)
- Percentage reduction in SLA breaches caused because of internal Operational Level Agreements (OLAs).

Deliver service as previously agreed at affordable costs:

- Total number and percentage increase in fully documented SLAs in place
- Percentage increase in SLAs agreed against operational services being run
- Percentage reduction in the costs associated with service provision

- Percentage reduction in the cost of monitoring and reporting of SLAs
- Percentage increase in the speed and of developing and agreeing appropriate SLAs
- Frequency of service review meetings.

Manage business interface:

- Increased percentage of services covered by SLAs
- Documented and agreed SLM processes and procedures are in place
- Reduction in the time taken to respond to and implement SLA requests
- Increased percentage of SLA reviews completed on time
- Reduction in the percentage of outstanding SLAs for annual renegotiation
- Reduction in the percentage of SLAs requiring corrective changes (for example, targets not attainable; changes in usage levels). Care needs to be taken when using this KPI
- Percentage increase in the coverage of OLAs and third-party contracts in place, whilst possibly reducing the actual number of agreements (consolidation and centralization)
- Documentary evidence that issues raised at service and SLA reviews are being followed up and resolved
- Reduction in the number and severity of SLA breaches
- Effective review and follow-up of all SLA, OLA and underpinning contract breaches.

4.2.8 Information Management

SLM provides key information on all operational services, their expected targets and the service achievements and breaches for all operational services. It assists Service Catalogue Management with the management of the Service Catalogue and also provides the information and trends on customer satisfaction, including complaints and compliments.

SLM is crucial in providing information on the quality of IT service provided to the customer, and information on the customer's expectation and perception of that quality of service. This information should be widely available to all areas of the service provider organization.

4.2.9 Challenges, Critical Success Factors and risks

One challenge faced by SLM is that of identifying suitable customer representatives with whom to negotiate. Who 'owns' the service? In some cases, this may be obvious, and a single customer manager is willing to act as the

signatory to the agreement. In other cases, it may take quite a bit of negotiating or cajoling to find a representative 'volunteer' (beware that volunteers often want to express their own personal view rather than represent a general consensus), or it may be necessary to get all customers to sign.

If customer representatives exist who are able genuinely to represent the views of the customer community, because they frequently meet with a wide selection of customers, this is ideal. Unfortunately, all too often representatives are head-office based and seldom come into contact with genuine service customers. In the worst case, SLM may have to perform his/her own programme of discussions and meetings with customers to ensure true requirements are identified.

Anecdote

On negotiating the current and support hours for a large service, an organization found a discrepancy in the required time of usage between Head Office and the field office's customers. Head Office (with a limited user population) wanted service hours covering 8.00 to 18.00, whereas the field office (with at least 20 times the user population) stated that starting an hour earlier would be better – but all offices closed to the public by 16.00 at the latest, and so wouldn't require a service much beyond this. Head Office won the 'political' argument, and so the 8.00 to 18.00 band was set. When the service came to be used (and hence monitored) it was found that service extensions were usually asked for by the field office to cover the extra hour in the morning, and actual usage figures showed that the service had not been accessed after 17.00, except on very rare occasions. The Service Level Manager was blamed by the IT staff for having to cover a late shift, and by the customer representative for charging for a service that was not used (i.e. staff and running costs).

Hints and tips

Care should be taken when opening discussions on service levels for the first time, as it is likely that 'current issues' (the failure that occurred yesterday) or long-standing grievances (that old printer that we have been trying to get replaced for ages) are likely to be aired at the outset. Important though these may be, they must not be allowed to get in the way of establishing the longer-term requirements. Be aware, however, that it may be necessary to address any issues raised at the outset before gaining any credibility to progress further.

If there has been no previous experience of SLM, then it is advisable to start with a draft SLA. A decision should be made on which service or customers are to be used for the draft. It is helpful if the selected customer is enthusiastic and wishes to participate – perhaps because they are anxious to see improvements in service quality. The results of an initial customer perception survey may give pointers to a suitable initial draft SLA.

Hints and tips

Don't pick an area where large problems exist as the first SLA. Try to pick an area that is likely to show some quick benefits and develop the SLM process. Nothing encourages acceptance of a new idea quicker than success.

One difficulty sometimes encountered is that staff at different levels within the customer community may have different objectives and perceptions. For example, a senior manager may rarely use a service and may be more interested in issues such as value for money and output, whereas a junior member of staff may use the service throughout the day, and may be more interested in issues such as responsiveness, usability and reliability. It is important that all of the appropriate and relevant customer requirements, at all levels, are identified and incorporated in SLAs.

Some organizations have formed focus groups from different levels from within the customer community to help ensure that all issues have been correctly addressed. This takes additional resources, but can be well worth the effort.

The other group of people that has to be consulted during the whole of this process is the appropriate representatives from within the IT provider side (whether internal or from an external supplier or partner). They need to agree that targets are realistic, achievable and affordable. If they are not, further negotiations are needed until a compromise acceptable to all parties is agreed. The views of suppliers should also be sought, and any contractual implications should be taken into account during the negotiation stages.

Where no past monitored data is available, it is advisable to leave the agreement in draft format for an initial period, until monitoring can confirm that initial targets are achievable. Targets may have to be re-negotiated in some cases. Many organizations negotiate an agreed timeframe for IT to negotiate and create a baseline for establishing realistic service targets. When targets and timeframes have been confirmed, the SLAs must be signed.

Once the initial SLA has been completed, and any early difficulties overcome, then move on and gradually introduce SLAs for other services/customers. If it is decided from the outset to go for a multi-level structure, it is likely that the corporate-level issues have to be covered for all customers at the time of the initial SLA. It is also worth trialling the corporate issues during this initial phase.

Hints and tips

Don't go for easy targets at the corporate level. They may be easy to achieve, but have no value in improving service quality or credibility. Also, if the targets are set at a sufficiently high level, the corporate SLA can be used as the standard that all new services should reach.

One point to ensure is that at the end of the drafting and negotiating process, the SLA is actually signed by the appropriate managers on the customer and IT service provider sides to the agreement. This gives a firm commitment by both parties that every attempt will be made to meet the agreement. Generally speaking, the more senior the signatories are within their respective organizations, the stronger the message of commitment. Once an SLA is agreed, wide publicity needs to be used to ensure that customers, users and IT staff alike are aware of its existence and of the key targets.

Steps must be taken to advertise the existence of the new SLAs and OLAs amongst the Service Desk and other support groups, with details of when they become operational. It may be helpful to extract key targets from these agreements into tables that can be on display in support areas, so that staff are always aware of the targets to which they are working. If support tools allow, these targets should be recorded within the tools, such as within a Service Catalogue or CMS, so that their content can be made widely available to all personnel. They should also be included as thresholds, and automatically alerted against when a target is threatened or actually breached. SLAs, OLAs and the targets they contain must also be publicized amongst the user community, so that users are aware of what they can expect from the services they use, and know at what point to start expressing dissatisfaction.

It is important that the Service Desk staff are committed to the SLM process, and become proactive ambassadors for SLAs, embracing the necessary service culture, as they are the first contact point for customers' incidents, complaints and queries. If the Service Desk staff are not fully aware of SLAs in place, and do not act on their contents, customers very quickly lose faith in SLAs.

4.2.9.1 Critical Success Factors

The main Critical Success Factors for the Service Catalogue Management process are:

- Manage the overall quality of IT services required
- Deliver the service as previously agreed at affordable costs
- Manage the interface with the business and users.

The risks associated with regard to the provision of an accurate Service Catalogue are:

- A lack of accurate input, involvement and commitment from the business and customers
- The tools and resources required to agree, document, monitor, report and review agreements and service levels
- The process becomes a bureaucratic, administrative process rather than an active and proactive process delivering measurable benefit to the business
- Access to and support of appropriate and up-to-date CMS and SKMS
- Bypassing the use of the SLM processes
- Business and customer measurements are too difficult to measure and improve, so are not recorded
- Inappropriate business and customer contacts and relationships are developed
- High customer expectations and low perception
- Poor and inappropriate communication is achieved with the business and customers.

4.3 CAPACITY MANAGEMENT

Capacity Management is a process that extends across the Service Lifecycle. A key success factor in managing capacity is ensuring it is considered during the design stage. It is for this reason that the Capacity Management process is included in this publication. Capacity Management is supported initially in Service Strategy where the decisions and analysis of business requirements and customer outcomes influence the development of patterns of business activity (PBA), levels of service (LOS) and service level packages (SLPs). This provides the predictive and ongoing capacity indicators needed to align capacity to demand.

4.3.1 Purpose/goal/objective

'The goal of the Capacity Management process is to ensure that cost-justifiable IT capacity in all areas of IT always exists and is matched to the current and future agreed needs of the business, in a timely manner'.

The purpose of Capacity Management is to provide a point of focus and management for all capacity- and performance-related issues, relating to both services and resources.

The objectives of Capacity Management are to:

- Produce and maintain an appropriate and up-to-date Capacity Plan, which reflects the current and future needs of the business
- Provide advice and guidance to all other areas of the business and IT on all capacity- and performance-related issues
- Ensure that service performance achievements meet or exceed all of their agreed performance targets, by managing the performance and capacity of both services and resources
- Assist with the diagnosis and resolution of performance- and capacity-related incidents and problems
- Assess the impact of all changes on the Capacity Plan, and the performance and capacity of all services and resources
- Ensure that proactive measures to improve the performance of services are implemented wherever it is cost-justifiable to do so.

4.3.2 Scope

The Capacity Management process should be the focal point for all IT performance and capacity issues.

Technology management functions such as Network Support, Server Support or Operation Management may carry out the bulk of the day-to-day operational duties, but will provide performance information to the Capacity Management process. The process should encompass all areas of technology, both hardware and software, for all IT technology components and environments. Capacity Management should also consider space planning and environmental systems capacity as well as certain aspects of human resources, but only where a lack of human resources could result in a breach of SLA or OLA targets, a delay in the end-to-end performance or service response time, or an inability to meet future commitments and plans (e.g. overnight data backups not completed in time because no operators were present to load tapes).

In general, human resource management is a line management responsibility, though the staffing of a Service Desk should use identical Capacity Management techniques. The scheduling of human resources, staffing levels, skill levels and capability levels should therefore be included within the scope of Capacity Management. The driving force for Capacity Management should be the

business requirements of the organization and to plan the resources needed to provide service levels in line with SLAs and OLAs. Capacity Management needs to understand the total IT and business environments, including:

- The current business operation and its requirements, through the patterns of business activity
- The future business plans and requirements via the Service Portfolio
- The service targets and the current IT service operation through SLAs and Standard Operating Procedures
- All areas of IT technology and its capacity and performance, including infrastructure, data, environment and applications.

Understanding all of this will enable Capacity Management to ensure that all the current and future capacity and performance aspects of services are provided cost-effectively.

Capacity Management is also about understanding the potential for the delivery of new services. New technology needs to be understood and, if appropriate, used to innovate and deliver the services required by the customer. Capacity Management needs to recognize that the rate of technological change will probably increase and that new technology should be harnessed to ensure that the IT services continue to satisfy changing business expectations. A direct link to the Service Strategy and Service Portfolio is needed to ensure that emerging technologies are considered in future service planning.

The Capacity Management process should include:

- Monitoring patterns of business activity and service-level plans through performance, utilization and throughput of IT services and the supporting infrastructure, environmental, data and applications components and the production of regular and ad hoc reports on service and component capacity and performance
- Undertaking tuning activities to make the most efficient use of existing IT resources
- Understanding the agreed current and future demands being made by the customer for IT resources, and producing forecasts for future requirements
- Influencing demand management, perhaps in conjunction with Financial Management
- Producing a Capacity Plan that enables the service provider to continue to provide services of the quality defined in SLAs and that covers a sufficient planning timeframe to meet future service levels required as defined in the Service Portfolio and SLRs

- Assistance with the identification and resolution of any incidents and problems associated with service or component performance
- The proactive improvement of service or component performance wherever it is cost-justifiable and meets the needs of the business.

Managing the capacity of large distributed IT infrastructures is a complex and demanding task, especially when the IT capacity and the financial investment required is ever-increasing. Therefore it makes even more sense to plan for growth. While the cost of the upgrade to an individual component in a distributed environment is usually less than the upgrade to a component in a mainframe environment, there are often many more components in the distributed environment that need to be upgraded. Also there could now be economies of scale, because the cost per individual component could be reduced when many components need to be purchased. Capacity Management should have input to the Service Portfolio and procurement process to ensure that the best deals with suppliers are negotiated.

Capacity Management provides the necessary information on current and planned resource utilization of individual components to enable organizations to decide, with confidence:

- Which components to upgrade (i.e. more memory, faster storage devices, faster processors, greater bandwidth)
- When to upgrade – ideally this is not too early, resulting in expensive over-capacity, nor too late, failing to take advantage of advances in new technology, resulting in bottle-necks, inconsistent performance and, ultimately, customer dissatisfaction and lost business opportunities
- How much the upgrade will cost – the forecasting and planning elements of Capacity Management feed into budgetary lifecycles, ensuring planned investment.

Many of the other processes are less effective if there is no input to them from the Capacity Management process. For example:

- Can the Change Management process properly assess the effect of any change on the available capacity?
- When a new service is implemented, can the SLM process be assured that the SLRs of the new service are achievable, and that the SLAs of existing services will not be affected?
- Can the Problem Management process properly diagnose the underlying cause of incidents caused by poor performance?

- Can the IT Service Continuity process accurately determine the capacity requirements of the key business processes?

Capacity Management is one of the forward-looking processes that, when properly carried out, can forecast business events and impacts often before they happen. Good Capacity Management ensures that there are no surprises with regard to service and component design and performance.

Capacity Management has a close, two-way relationship with the Service Strategy and planning processes within an organization. On a regular basis, the long-term strategy of an organization is encapsulated in an update of the business plans. The Service Strategy will reflect the business plans and strategy, which are developed from the organization's understanding of the external factors such as the competitive marketplace, economic outlook and legislation, and its internal capability in terms of manpower, delivery capability, etc. Often a shorter-term tactical plan, or business change plan is developed to implement the changes necessary in the short to medium term to progress the overall business plan and Service Strategy. Capacity Management needs to understand the short-, medium- and long-term plans of the business while providing information on the latest ideas, trends and technologies being developed by the suppliers of computing hardware and software.

The organization's business plans drive the specific IT Service Strategy, the contents of which Capacity Management needs to be familiar with, and to which Capacity Management needs to have had significant and ongoing input. The right level of capacity at the right time is critical. Service Strategy plans will be helpful to capacity planning by identifying the timing for acquiring and implementing new technologies, hardware and software.

4.3.3 Value to the business

Capacity Management is responsible for ensuring that IT resources are planned and scheduled to provide a consistent level of service that is matched to the current and future needs of the business, as agreed and documented within SLAs and OLAs. In conjunction with the business and their plans, Capacity Management provides a Capacity Plan that outlines the IT resources and funding needed to support the business plan, together with a cost justification of that expenditure.

4.3.4 Policies/principles/basic concepts

Capacity Management ensures that the capacity and performance of the IT services and systems matches the

evolving agreed demands of the business in the most cost-effective and timely manner. Capacity Management is essentially a balancing act:

- **Balancing costs against resources needed:** the need to ensure that processing capacity that is purchased is cost-justifiable in terms of business need, and the need to make the most efficient use of those resources.
- **Balancing supply against demand:** the need to ensure that the available supply of IT processing power matches the demands made on it by the business, both now and in the future. It may also be necessary to manage or influence the demand for a particular resource.

Capacity Management processes and planning must be involved in all stages of the Service Lifecycle from Strategy and Design, through Transition and Operation to Improvement. From a strategic perspective, the Service Portfolio contains the IT resources and capabilities. The advent of Service Oriented Architecture, virtualization and the use of value networks in IT service provision are important factors in the management of capacity. The appropriate capacity and performance should be designed into services and components from the initial design stages. This will ensure not only that the performance of any new or changed service meets its expected targets, but also that all existing services continue to meet all of their targets. This is the basis of stable service provision.

The overall Capacity Management process is continually trying cost-effectively to match IT resources and capacity to the ever-changing needs and requirements of the business. This requires the tuning and optimization of the current resources and the effective estimation and planning of the future resources, as illustrated in Figure 4.8.

Capacity Management is an extremely technical, complex and demanding process, and in order to achieve results, it requires three supporting sub-processes.

One of the key activities of Capacity Management is to produce a plan that documents the current levels of resource utilization and service performance and, after consideration of the Service Strategy and plans, forecasts the future requirements for new IT resources to support the IT services that underpin the business activities. The plan should indicate clearly any assumptions made. It should also include any recommendations quantified in terms of resource required, cost, benefits, impact, etc.

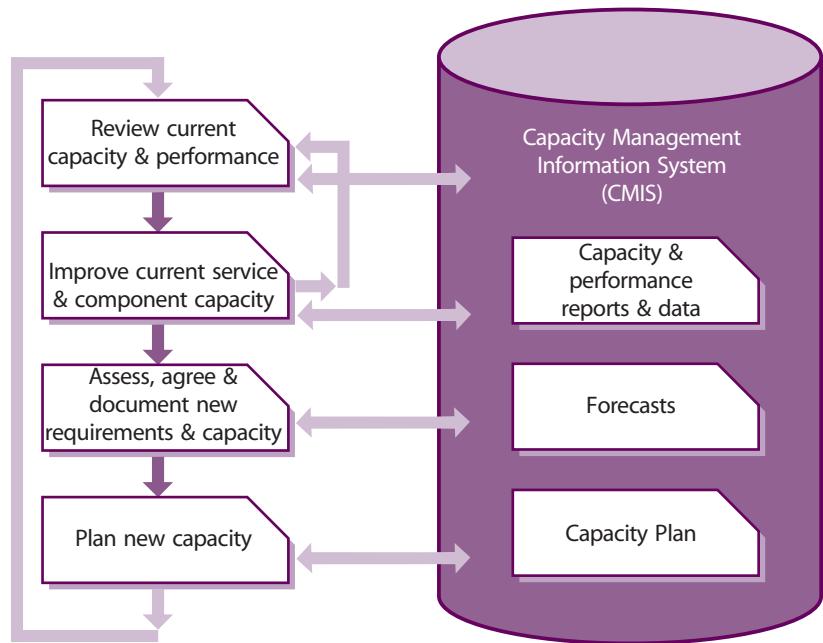


Figure 4.8 The Capacity Management process

The production and maintenance of a Capacity Plan should occur at pre-defined intervals. It is, essentially, an investment plan and should therefore be published annually, in line with the business or budget lifecycle, and completed before the start of negotiations on future budgets. A quarterly re-issue of the updated plan may be necessary to take into account changes in service plans, to report on the accuracy of forecasts and to make or refine recommendations. This takes extra effort but, if it is regularly updated, the Capacity Plan is more likely to be accurate and to reflect the changing business need.

The typical contents of a Capacity Plan are described in Appendix J.

4.3.4.1 Business Capacity Management

This sub-process translates business needs and plans into requirements for service and IT infrastructure, ensuring that the future business requirements for IT services are quantified, designed, planned and implemented in a timely fashion. This can be achieved by using the existing data on the current resource utilization by the various services and resources to trend, forecast, model or predict future requirements. These future requirements come from the Service Strategy and Service Portfolio detailing new processes and service requirements, changes, improvements, and also the growth in the existing services.

4.3.4.2 Service Capacity Management

The focus of this sub-process is the management, control and prediction of the end-to-end performance and capacity of the live, operational IT services usage and workloads. It ensures that the performance of all services, as detailed in service targets within SLAs and SLRs, is monitored and measured, and that the collected data is recorded, analysed and reported. Wherever necessary, proactive and reactive action should be instigated, to ensure that the performance of all services meets their agreed business targets. This is performed by staff with knowledge of all the areas of technology used in the delivery of end-to-end service, and often involves seeking advice from the specialists involved in Component Capacity Management. Wherever possible, automated thresholds should be used to manage all operational services, to ensure that situations where service targets are breached or threatened are rapidly identified and cost-effective actions to reduce or avoid their potential impact implemented.

4.3.4.3 Component Capacity Management

The focus in this sub-process is the management, control and prediction of the performance, utilization and capacity of individual IT technology components. It ensures that all components within the IT infrastructure that have finite resource are monitored and measured, and that the collected data is recorded, analysed and reported. Again, wherever possible, automated thresholds should be implemented to manage all components, to ensure that situations where service targets are breached or threatened by component usage or performance are rapidly identified, and cost-effective actions to reduce or avoid their potential impact are implemented.

There are many similar activities that are performed by each of the above sub-processes, but each sub-process has a very different focus. Business Capacity Management is focused on the current and future business requirements, while Service Capacity Management is focused on the delivery of the existing services that support the business, and Component Capacity Management is focused on the IT infrastructure that underpins service provision. The role that each of these sub-processes plays in the overall process and the use of management tools is illustrated in Figure 4.9.

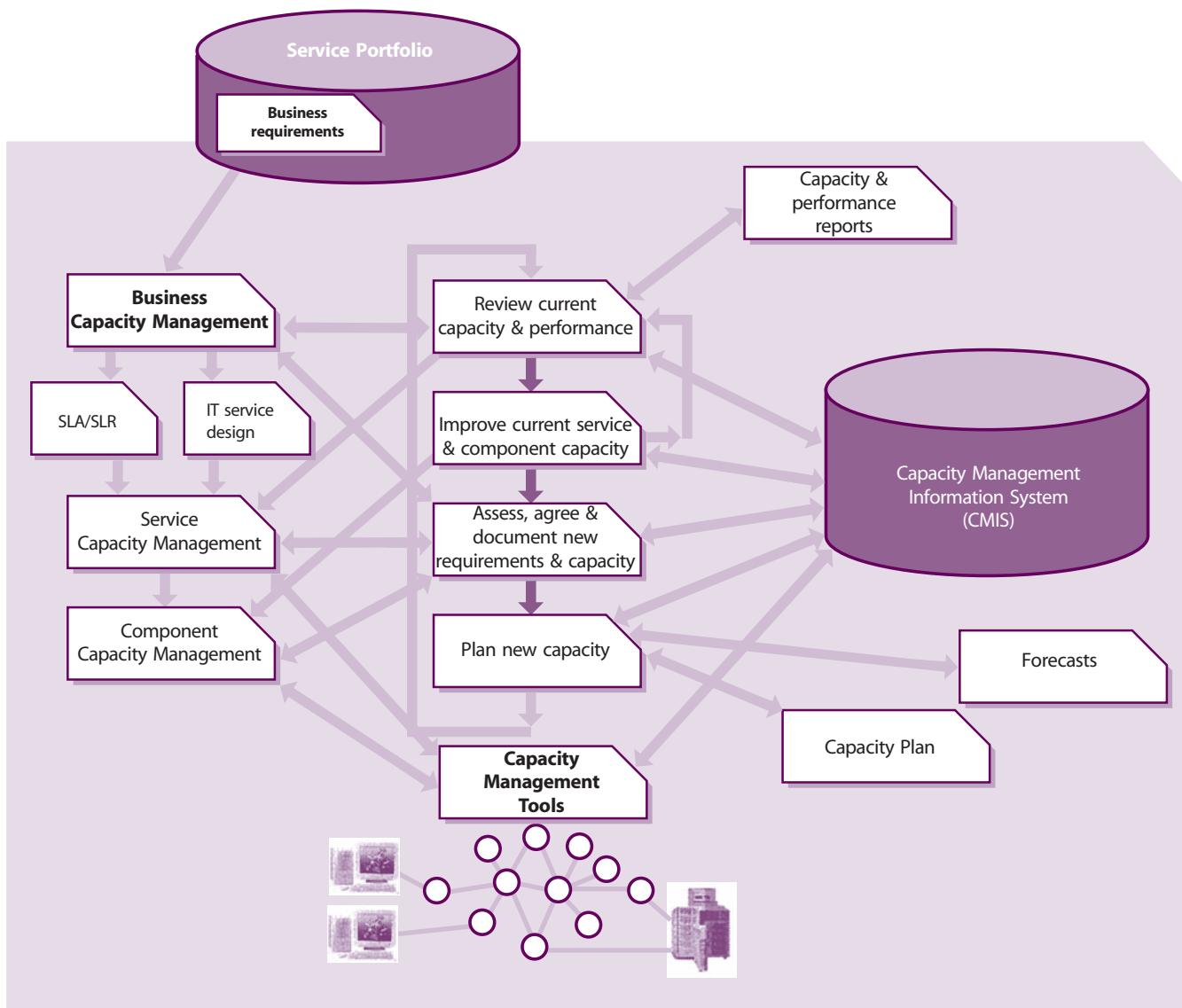


Figure 4.9 Capacity Management sub-processes

The tools used by Capacity Management need to conform to the organization's management architecture and integrate with other tools used for the management of IT systems and automating IT processes. The monitoring and control activities within Service Operation will provide a good basis for the tools to support and analyse information for Capacity Management.

4.3.5 Process activities, methods and techniques

Some activities in the Capacity Management process are reactive, while others are proactive. The proactive activities of Capacity Management should include:

- Pre-empting performance issues by taking the necessary actions before they occur
- Producing trends of the current component utilization and estimating the future requirements, using trends and thresholds for planning upgrades and enhancements
- Modelling and trending the predicted changes in IT services, and identifying the changes that need to be made to services and components of the IT infrastructure and applications to ensure that appropriate resource is available
- Ensuring that upgrades are budgeted, planned and implemented before SLAs and service targets are breached or performance issues occur
- Actively seeking to improve service performance wherever it is cost-justifiable
- Tuning and optimizing the performance of services and components.

The reactive activities of Capacity Management should include:

- Monitoring, measuring, reporting and reviewing the current performance of both services and components
- Responding to all capacity-related 'threshold' events and instigating corrective action
- Reacting to and assisting with specific performance issues. For example, the Service Desk may refer incidents of poor performance to Technology Management, which will employ Capacity Management techniques to resolve them.

Key message

The more successful the proactive and predictive activities of Capacity Management, the less need there will be for the reactive activities of Capacity Management.

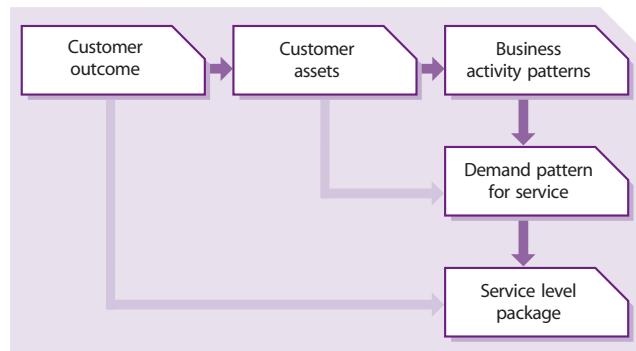


Figure 4.10 Capacity must support business requirements

4.3.5.1 Business Capacity Management

The main objective of the Business Capacity Management sub-process is to ensure that the future business requirements (customer outcomes) for IT services are considered and understood, and that sufficient IT capacity to support any new or changed services is planned and implemented within an appropriate timescale. Figure 4.10 illustrates that BCM is influenced by the business patterns of activity and how services are used.

The Capacity Management process must be responsive to changing requirements for capacity demand. New services or changed services will be required to underpin the changing business. Existing services will require modification to provide extra functionality. Old services will become obsolete, freeing up spare capacity. As a result, the ability to satisfy the customers' SLRs and SLAs will be affected. It is the responsibility of Capacity Management to predict the demand for capacity for such changes and manage the demand.

These new requirements may come to the attention of Capacity Management from many different sources and for many different reasons, but the principal sources of supply should be the Pattern of Business Activity from Demand Management and the Service Level Packages produced for the Service Portfolio. These indicate a window of future predictors for capacity. Such examples could be a recommendation to upgrade to take advantage of new technology, or the implementation of a tuning activity to resolve a performance problem. Figure 4.11 shows the cycle of demand management.

Capacity Management needs to be included in all strategic, planning and design activities, being involved as early as possible within each process, such as:

- Assisting and supporting the development of Service Strategy

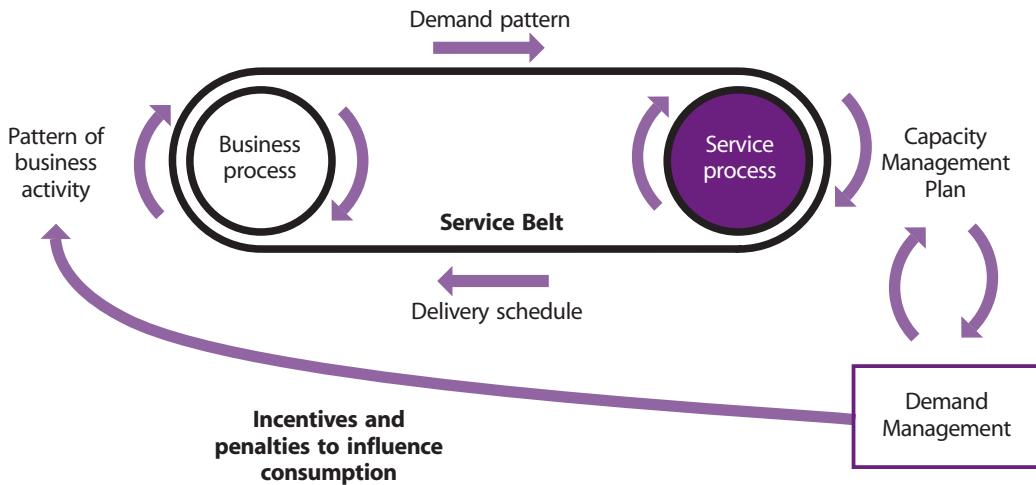


Figure 4.11 Capacity Management takes particular note of demand pattern

- Involvement in the review and improvement of IT strategies and policies
- Involvement in the review and improvement of technology architectures.

Key message

Capacity Management should not be a last-minute 'tick in the box' just prior to customer acceptance and operational acceptance.

If early involvement can be achieved from Capacity Management within these processes, then the planning and design of IT capacity can be closely aligned with business requirements and can ensure that service targets can be achieved and maintained.

Assist with agreeing Service Level Requirements

Capacity Management should assist SLM in understanding the customers' capacity and performance requirements, in terms of required service/system response times, expected throughput, patterns of usage and volume of users. Capacity Management should help in the negotiation process by providing possible solutions to a number of scenarios. For example, if the volume of users is less than 2,000, then response times can be guaranteed to be less than two seconds. If more than 2,000 users connect concurrently, then extra network bandwidth is needed to guarantee the required response time, or a slower response time will have to be accepted. Modelling, trending or application sizing techniques are often employed here to ensure that predictions accurately reflect the real situation.

Design, procure or amend service configuration

Capacity Management should be involved in the design of new or changing services and make recommendations for the procurement of hardware and software, where

performance and/or capacity are factors. In some instances Capacity Management instigates the implementation of the new requirement through Change Management, where it is also involved as a member of the Change Advisory Board. In the interest of balancing cost and capacity, the Capacity Management process obtains the costs of alternative proposed solutions and recommends the most appropriate cost-effective solution.

Verify SLA

The SLA should include details of the anticipated service throughputs and the performance requirements. Capacity Management advises SLM on achievable targets that can be monitored and on which the Service Design has been based. Confidence that the Service Design will meet the SLRs and provide the ability for future growth can be gained by using modelling, trending or sizing techniques.

Support SLA negotiation

The results of the predictive techniques provide the verification of service performance capabilities. There may be a need for SLM to renegotiate SLAs based on these findings. Capacity Management provides support to SLM should renegotiations be necessary, by recommending potential solutions and associated cost information. Once assured that the requirements are achievable, it is the responsibility of SLM to agree the service levels and sign the SLA.

Control and implementation

All changes to service and resource capacity must follow all IT processes such as Change, Release, Configuration and Project Management to ensure that the right degree of control and coordination is in place on all changes and that any new or change components are recorded and tracked through their lifecycle.

4.3.5.2 Service Capacity Management

The main objective of the Service Capacity Management sub-process is to identify and understand the IT services, their use of resource, working patterns, peaks and troughs, and to ensure that the services meet their SLA targets, i.e. to ensure that the IT services perform as required. In this sub-process, the focus is on managing service performance, as determined by the targets contained in the agreed SLAs or SLRs.

The Service Capacity Management sub-process ensures that the services meet the agreed capacity service targets. The monitored service provides data that can identify trends from which normal service levels can be established. By regular monitoring and comparison with these levels, exception conditions can be defined, identified and reported on. Therefore Capacity Management informs SLM of any service breaches or near misses.

There will be occasions when incidents and problems are referred to Capacity Management from other processes, or it is identified that a service could fail to meet its SLA targets. On some of these occasions, the cause of the potential failure may not be resolved by Component Capacity Management. For example, when the failure is analysed it may be found that there is no lack of capacity, or no individual component is over-utilized. However, if the design or coding of an application is inefficient, then the service performance may need to be managed, as well as individual hardware or software resources. Service Capacity Management should also be monitoring service workloads and transactions to ensure that they remain within agreed limitations and thresholds.

The key to successful Service Capacity Management is to forecast issues, wherever possible, by monitoring changes in performance and monitoring the impact of changes. So this is another sub-process that has to be proactive and predictive, even pre-emptive, rather than reactive. However, there are times when it has to react to specific performance problems. From a knowledge and understanding of the performance requirements of each of the services being used, the effects of changes in the use of services can be estimated, and actions taken to ensure that the required service performance can be achieved.

4.3.5.3 Component Capacity Management

The main objective of Component Capacity Management (CCM) is to identify and understand the performance, capacity and utilization of each of the individual components within the technology used to support the IT

services, including the infrastructure, environment, data and applications. This ensures the optimum use of the current hardware and software resources in order to achieve and maintain the agreed service levels. All hardware components and many software components in the IT infrastructure have a finite capacity that, when approached or exceeded, has the potential to cause performance problems.

This sub-process is concerned with components such as processors, memory, disks, network bandwidth, network connections etc. So information on resource utilization needs to be collected on a continuous basis. Monitors should be installed on the individual hardware and software components, and then configured to collect the necessary data, which is accumulated and stored over a period of time. This is an activity generally carried out through monitoring and control within Service Operation. A direct feedback to CCM should be applied within this sub-process.

As in Service Capacity Management, the key to successful CCM is to forecast issues, wherever possible, and it therefore has to be proactive and predictive as well. However, there are times when CCM has to react to specific problems that are caused by a lack of capacity, or the inefficient use of the component. From a knowledge and understanding of the use of resource by each of the services being run, the effects of changes in the use of services can be estimated and hardware or software upgrades can be budgeted and planned. Alternatively, services can be balanced across the existing resources to make most effective use of the current resources.

4.3.5.4 The underpinning activities of Capacity Management

The activities described in this section are necessary to support the sub-processes of Capacity Management, and these activities can be done both reactively or proactively, or even pre-emptively.

The major difference between the sub-processes is in the data that is being monitored and collected, and the perspective from which it is analysed. For example, the level of utilization of individual components in the infrastructure – such as processors, disks, and network links – is of interest in Component Capacity Management, while the transaction throughput rates and response times are of interest in Service Capacity Management. For Business Capacity Management, the transaction

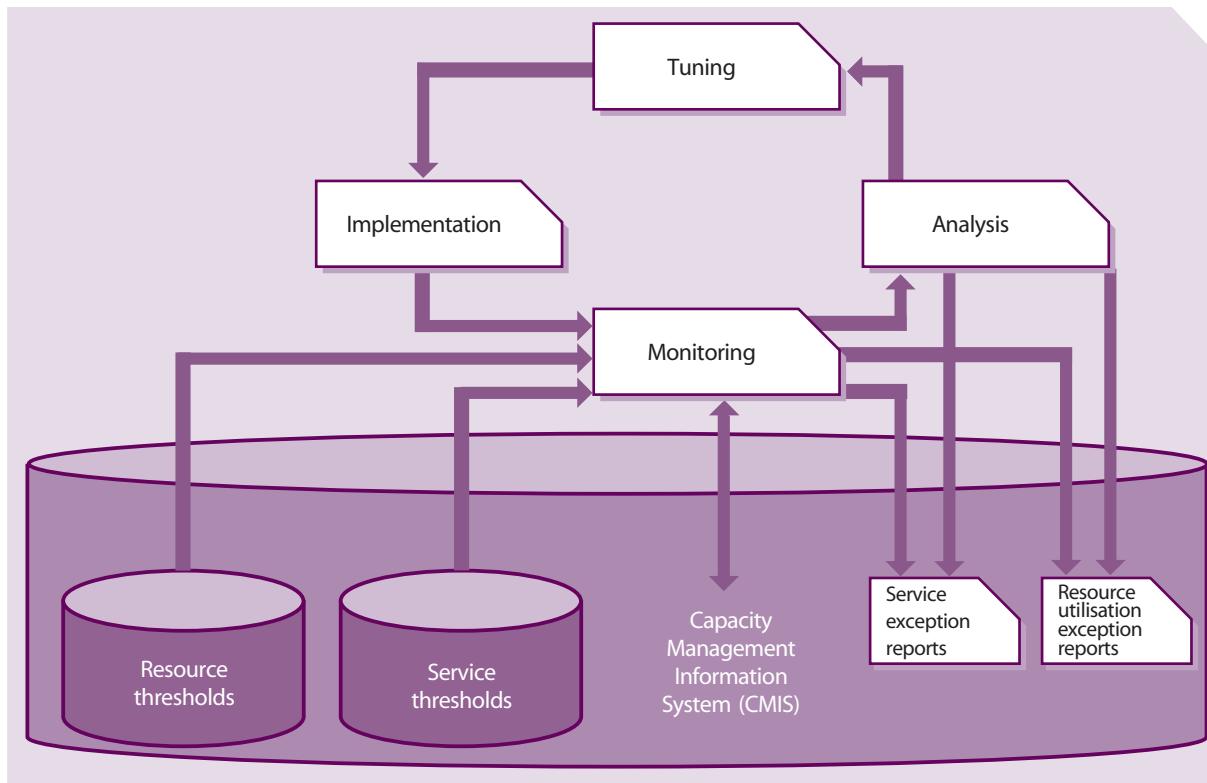


Figure 4.12 Iterative ongoing activities of Capacity Management

throughput rates for the online service need to be translated into business volumes – for example, in terms of sales invoices raised or orders taken. The biggest challenge facing Capacity Management is to understand the relationship between the demands and requirements of the business and the business workload, and to be able to translate these in terms of the impact and effect of these on the service and resource workloads and utilizations, so that appropriate thresholds can be set at each level.

Tuning and optimization activities

A number of the activities need to be carried out iteratively and form a natural cycle, as illustrated in Figure 4.12.

These activities provide the basic historical information and triggers necessary for all of the other activities and processes within Capacity Management. Monitors should be established on all the components and for each of the services. The data should be analysed using, wherever possible, expert systems to compare usage levels against thresholds. The results of the analysis should be included in reports, and recommendations made as appropriate. Some form of control mechanism may then be put in place to act on the recommendations. This may take the

form of balancing services, balancing workloads, changing concurrency levels and adding or removing resources. All of the information accumulated during these activities should be stored in the Capacity Management Information System (CMIS) and the cycle then begins again, monitoring any changes made to ensure they have had a beneficial effect and collecting more data for future actions.

Utilization monitoring

The monitors should be specific to particular operating systems, hardware configurations, applications, etc. It is important that the monitors can collect all the data required by the Capacity Management process, for a specific component or service. Typical monitored data includes:

- Processor utilization
- Memory utilization
- Per cent processor per transaction type
- IO rates (physical and buffer) and device utilization
- Queue lengths
- Disk utilization
- Transaction rates
- Response times

- Batch duration
- Database usage
- Index usage
- Hit rates
- Concurrent user numbers
- Network traffic rates.

In considering the data that needs to be included, a distinction needs to be drawn between the data collected to monitor capacity (e.g. throughput) and the data to monitor performance (e.g. response times). Data of both types is required by the Service and Component Capacity Management sub-processes. This monitoring and collection needs to incorporate all components in the service, thus monitoring the 'end-to-end' customer experience. The data should be gathered at total resource utilization level and at a more detailed profile for the load that each service places on each particular component. This needs to be carried out across the whole technology, host or server, the network, local server and client or workstation. Similarly the data needs to be collected for each service.

Part of the monitoring activity should be of thresholds and baselines or profiles of the normal operating levels. If these are exceeded, alarms should be raised and exception reports produced. These thresholds and baselines should have been determined from the analysis of previously recorded data, and can be set at both the component and service level. All thresholds should be set below the level at which the component or service is over-utilized, or below the targets in the SLAs. When the threshold is reached or threatened, there is still an opportunity to take corrective action before the SLA has been breached, or the resource has become over-utilised and there has been a period of poor performance. The monitoring and management of these events, thresholds and alarms is covered in detail in the Service Operation publication.

Often it is more difficult to get the data on the current business volumes as required by the Business Capacity Management sub-process. These statistics may need to be derived from the data available to the Service and Component Capacity Management sub-processes.

Response time monitoring

Many SLAs have user response times as one of the targets to be measured, but equally many organizations have great difficulty in supporting this requirement. User response times of IT and network services can be monitored and measured by the following:

- **Incorporating specific code within client and server applications software.** This can be used to provide complete 'end-to-end' service response times or intermediate timing points to break down the overall response into its constituent components. The figures obtained from these tools give the actual response times as perceived by the users of a service.
- **Using 'robotic scripted systems' with terminal emulation software.** These systems consist of client systems with terminal emulation software (e.g. browser or Telnet systems) and specialized scripted software for generating and measuring transactions and responses. These systems generally provide sample 'end-to-end' service response times and are useful for providing representative response times, particularly for multi-phase transactions or complex interactions. These only give sample response times, not the actual response times as perceived by the real users of the service.
- **Using distributed agent monitoring software.** Useful information on service response times can be obtained by distributing agent systems with monitoring software at different points of a network (e.g. within different countries on the internet). These systems can then be used to generate transactions from a number of locations and give periodic measurements of an internet site as perceived by international users of an internet website. However, again the times received are only indications of the response times and are not the real user response times.
- **Using specific passive monitoring systems.** Tracking a representative sample number of client systems. This method relies on the connection of specific network monitoring systems, often referred to as 'sniffers' being inserted at appropriate points within the network. These can then monitor, record and time all traffic passing a particular point within the network. Once recorded, this traffic can then be analysed to give detailed information on the service response times. Once again, however, these can only be used to give an approximation to the actual user response times, although these are often very close to the real-world situation, but this depends on the position of the monitor itself within the IT infrastructure.

In some cases, a combination of a number of systems may be used. The monitoring of response times is a complex process even if it is an in-house service running on a private network. If this is an external internet service, the process is much more complex because of the sheer number of different organizations and technologies involved.

Anecdote

A private company with a major website implemented a website monitoring service from an external supplier that would provide automatic alarms on the availability and responsiveness of their website. The availability and speed of the monitoring points were lower than those of the website being monitored. Therefore the figures produced by the service were of the availability and responsiveness of the monitoring service itself, rather than those of the monitored website.

Hints and tips

When implementing external monitoring services, ensure that the service levels and performance commitments of the monitoring service are in excess of those of the service(s) being monitored.

Analysis

The data collected from the monitoring should be analysed to identify trends from which the normal utilization and service levels, or baselines, can be established. By regular monitoring and comparison with this baseline, exception conditions in the utilization of individual components or service thresholds can be defined, and breaches or near misses in the SLAs can be reported and actioned. Also the data can be used to predict future resource usage, or to monitor actual business growth against predicted growth.

Analysis of the data may identify issues such as:

- ‘Bottlenecks’ or ‘hot spots’ within the infrastructure
- Inappropriate distribution of workload across available resources
- Inappropriate database indexing
- Inefficiencies in the application design
- Unexpected increase in workloads or transaction rates
- Inefficient scheduling or memory usage.

The use of each component and service needs to be considered over the short, medium and long term, and the minimum, maximum and average utilization for these periods recorded. Typically, the short-term pattern covers the utilization over a 24-hour period, while the medium term may cover a one- to four-week period, and the long term a year-long period. Over time, the trend in the use of the resource by the various IT services will become apparent. The usefulness of this information is further enhanced by recording any observed contributing factors to peaks or valleys in utilization – for example, if a change of business process or staffing coincides with any deviations from the normal utilization.

It is important to understand the utilization in each of these periods, so that changes in the use of any service can be related to predicted changes in the level of utilization of individual components. The ability to identify the specific hardware or software components on which a particular IT service depends is improved greatly by an accurate, up-to-date and comprehensive CMS.

When the utilization of a particular resource is considered, it is important to understand both the total level of utilization and the utilization by individual services of the resource.

Example

If a processor that is 75% loaded during the peak hour is being used by two different services, A and B, it is important to know how much of the total 75% is being used by each service. Assuming the system overhead on the processor is 5%, the remaining 70% load could be split evenly between the two services. If a change in either Service A or Service B is estimated to double its loading on the processor, then the processor would be overloaded.

However, if service A uses 60% and Service B uses 10% of the processor, then the processor would be overloaded if service A doubled its loading on the processor. But if service B doubled its loading on the processor, then the processor would not necessarily be overloaded.

Tuning

The analysis of the monitored data may identify areas of the configuration that could be tuned to better utilize the service, system and component resources or improve the performance of the particular service.

Tuning techniques that are of assistance include:

- Balancing workloads and traffic – transactions may arrive at the host or server at a particular gateway, depending on where the transaction was initiated; balancing the ratio of initiation points to gateways can provide tuning benefits
- Balancing disk traffic – storing data on disk efficiently and strategically, e.g. striping data across many spindles may reduce data contention
- Definition of an accepted locking strategy that specifies when locks are necessary and the appropriate level, e.g. database, page, file, record and row – delaying the lock until an update is necessary may provide benefits
- Efficient use of memory – may include looking to utilize more or less memory, depending on the circumstances.

Before implementing any of the recommendations arising from the tuning techniques, it may be appropriate to consider testing the validity of the recommendation. For example, 'Can Demand Management be used to avoid the need to carry out any tuning?' or 'Can the proposed change be modelled to show its effectiveness before it is implemented?'

Implementation

The objective of this activity is to introduce to the live operation services any changes that have been identified by the monitoring, analysis and tuning activities. The implementation of any changes arising from these activities must be undertaken through a strict, formal Change Management process. The impact of system tuning changes can have major implications on the customers of the service. The impact and risk associated with these types of changes are likely to be greater than that of other different type of changes.

It is important that further monitoring takes place, so that the effects of the change can be assessed. It may be necessary to make further changes or to regress some of the original changes.

Exploitation of new technology

This involves understanding new techniques and new technology and how they can be used to support the business and innovate improvements. It may be appropriate to introduce new technology to improve the provision and support of the IT services on which the organization is dependent. This information can be gathered by studying professional literature (magazine and press articles) and by attending:

- Promotional seminars by hardware and software suppliers
- User group meetings of suppliers of potential hardware and software
- User group meetings for other IT professionals involved in Capacity Management.

Each of these provides sources of information relating to potential techniques, technology, hardware and software, which might be advantageous for IT to implement to realize business benefits. However, at all times Capacity Management should recognize that the introduction and use of this new technology must be cost-justified and deliver real benefit to the business. It is not just the new technology itself that is important, but Capacity Management should also keep aware of the advantages to be obtained from the use of new technologies, using techniques such as 'grid computing', 'virtualization' and 'on-demand computing'.

Designing resilience

Capacity Management assists with the identification and improvement of the resilience within the IT infrastructure or any subset of it, wherever it is cost-justified. In conjunction with Availability Management, Capacity Management should use techniques such as Component Failure Impact Analysis (CFIA, as described in section 4.4 on Availability Management) to identify how susceptible the current configuration is to the failure or overload of individual components and make recommendations on any cost-effective solutions.

Capacity Management should be able to identify the impact on the available resources of particular failures, and the potential for running the most important services on the remaining resources. So the provision of spare capacity can act as resilience or fail-over in failure situations.

The requirements for resilience in the IT infrastructure should always be considered at the time of the service or system design. However, for many services, the resilience of the service is only considered after it is in live operational use. Incorporating resilience into Service Design is much more effective and efficient than trying to add it at a later date, once a service has become operational.

4.3.5.5 Threshold management and control

The technical limits and constraints on the individual services and components can be used by the monitoring activities to set the thresholds at which warnings and alarms are raised and exception reports are produced. However, care must be exercised when setting thresholds,

because many thresholds are dependent on the work being run on the particular component.

The management and control of service and component thresholds is fundamental to the effective delivery of services to meet their agreed service levels. It ensures that all service and component thresholds are maintained at the appropriate levels and are continuously, automatically monitored, and alerts and warnings generated when breaches occur. Whenever monitored thresholds are breached or threatened, then alarms are raised and breaches, warnings and exception reports are produced. Analysis of the situation should then be completed and remedial action taken whenever justified, ensuring that the situation does not recur. The same data items can be used to identify when SLAs are breached or likely to be breached or when component performance degrades or is likely to be degraded. By setting thresholds below or above the actual targets, action can be taken and a breach of the SLA targets avoided. Threshold monitoring should not only alarm on exceeding a threshold, but should also monitor the rate of change and predict when the threshold will be reached. For example, a disk-space monitor should monitor the rate of growth and raise an alarm when the current rate will cause the disk to be full within the next N days. If a 1GB disk has reached 90% capacity, and is growing at 100KB per day, it will be 1,000 days before it is full. If it is growing at 10MB per day, it will only be 10 days before it is full. The monitoring and management of these events and alarms is covered in detail in the Service Operations publication.

There may be occasions when optimization of infrastructure components and resources is needed to maintain or improve performance or throughput. This can often be done through Workload Management, which is a generic term to cover such actions as:

- Rescheduling a particular service or workload to run at a different time of day or day of the week, etc. (usually away from peak times to off-peak windows) – which will often mean having to make adjustments to job-scheduling software
- Moving a service or workload from one location or set of CIs to another – often to balance utilization or traffic
- Technical ‘virtualization’: setting up and using virtualization techniques and systems to allow the movement of processing around the infrastructure to give better performance/resilience in a dynamic fashion

- Limiting or moving demand for components or resources through Demand Management techniques, in conjunction with Financial Management (see section 4.3.5.6).

It will only be possible to manage workloads effectively if a good understanding exists of which workloads will run at what time and how much resource utilization each workload places on the IT infrastructure. Diligent monitoring and analysis of workloads, together with a comprehensive CMIS, are therefore needed on an ongoing operational basis.

4.3.5.6 Demand Management

The prime objective of Demand Management is to influence user and customer demand for IT services and manage the impact on IT resources.

This activity can be carried out as a short-term requirement because there is insufficient current capacity to support the work being run, or, as a deliberate policy of IT management, to limit the required capacity in the long term.

Short-term Demand Management may occur when there has been a partial failure of a critical resource in the IT infrastructure. For example, if there has been a failure of a processor within a multi-processor server, it may not be possible to run the full range of services. However, a limited subset of the services could be run. Capacity Management should be aware of the business priority of each of the services, know the resource requirements of each service (in this case, the amount of processor power required to run the service) and then be able to identify which services can be run while there is a limited amount of processor power available.

Long-term Demand Management may be required when it is difficult to cost-justify an expensive upgrade. For example, many processors are heavily utilized for only a few hours each day, typically 10.00-12.00 and 14.00-16.00. Within these periods, the processor may be overloaded for only one or two hours. For the hours between 18.00-08.00, these processors are only very lightly loaded and the components are under-utilized. Is it possible to justify the cost of an upgrade to provide additional capacity for only a few hours in 24 hours? Or is it possible to influence the demand and spread the requirement for resource across 24 hours, thereby delaying or avoiding altogether the need for a costly upgrade?

Demand Management needs to understand which services are utilizing the resource and to what level, and the schedule of when they must be run. Then a decision can

be made on whether it will be possible to influence the use of resource and, if so, which option is appropriate.

The influence on the services that are running could be exercised by:

- **Physical constraints:** for example, it may be possible to stop some services from being available at certain times, or to limit the number of customers who can use a particular service – for example, by limiting the number of concurrent users; the constraint could be implemented on a specific resource or component – for example, by limiting the number of physical connections to a network router or switch
- **Financial constraints:** if charging for IT services is in place, reduced rates could be offered for running work at times of the day when there is currently less demand for the resource. This is known as differential charging.

4.3.5.7 Modelling and trending

A prime objective of Capacity Management is to predict the behaviour of IT services under a given volume and variety of work. Modelling is an activity that can be used to beneficial effect in any of the sub-processes of Capacity Management.

The different types of modelling range from making estimates based on experience and current resource utilization information, to pilot studies, prototypes and full-scale benchmarks. The former is a cheap and reasonable approach for day-to-day small decisions, while the latter is expensive, but may be advisable when implementing a large new project or service. With all types of modelling, similar levels of accuracy can be obtained, but all are totally dependent on the skill of the person constructing the model and the information used to create it.

Baselining

The first stage in modelling is to create a baseline model that reflects accurately the performance that is being achieved. When this baseline model has been created, predictive modelling can be done, i.e. ask the 'What if?' questions that reflect failures, planned changes to the hardware and/or the volume/variety of workloads. If the baseline model is accurate, then the accuracy of the result of the potential failures and changes can be trusted.

Effective Capacity Management, together with modelling techniques, enables Capacity Management to answer the 'What if?' questions. What if the throughput of Service A doubles? What if Service B is moved from the current server onto a new server – what will be the effect on the response times of the two services?

Trend analysis

Trend analysis can be done on the resource utilization and service performance information that has been collected by the Capacity Management process. The data can be analysed in a spreadsheet, and the graphical and trending and forecasting facilities used to show the utilization of a particular resource over a previous period of time, and how it can be expected to change in the future.

Typically, trend analysis only provides estimates of future resource utilization information. Trend analysis is less effective in producing an accurate estimate of response times, in which case either analytical or simulation modelling should be used. Trend analysis is most effective when there is a linear relationship between a small number of variables, and less effective when there are non-linear relationships between variables or when there are many variables.

Analytical modelling

Analytical models are representations of the behaviour of computer systems using mathematical techniques, e.g. multi-class network queuing theory. Typically, a model is built using a software package on a PC, by specifying within the package the components and structure of the configuration that needs to be modelled, and the utilization of the components, e.g. processor, memory and disks, by the various workloads or applications. When the model is run, the queuing theory is used to calculate the response times in the computer system. If the response times predicted by the model are sufficiently close to the response times recorded in real life, the model can be regarded as an accurate representation of the computer system.

The technique of analytical modelling requires less time and effort than simulation modelling, but typically it gives less accurate results. Also, the model must be kept up-to-date. However, if the results are within 5% accuracy for utilization, and 15–20% for online application response times, the results are usually satisfactory.

Simulation modelling

Simulation involves the modelling of discrete events, e.g. transaction arrival rates, against a given hardware configuration. This type of modelling can be very accurate in sizing new applications or predicting the effects of changes on existing applications, but can also be very time-consuming and therefore costly.

When simulating transaction arrival rates, have a number of staff enter a series of transactions from prepared scripts, or use software to input the same scripted transactions with a random arrival rate. Either of these approaches

takes time and effort to prepare and run. However, it can be cost-justified for organizations with very large services and systems where the major cost and the associated performance implications assume great importance.

4.3.5.8 Application sizing

Application sizing has a finite lifespan. It is initiated at the design stage for a new service, or when there is a major change to an existing service, and is completed when the application is accepted into the live operational environment. Sizing activities should include all areas of technology related to the applications, and not just the applications themselves. This should include the infrastructure, environment and data, and will often use modelling and trending techniques.

The primary objective of application sizing is to estimate the resource requirements to support a proposed change to an existing service or the implementation of a new service, to ensure that it meets its required service levels. To achieve this, application sizing has to be an integral part of the Service Lifecycle.

During the initial requirements and design, the required service levels must be specified in an SLR. This enables the Service Design and development to employ the pertinent technologies and products to achieve a design that meets the desired levels of service. It is much easier and less expensive to achieve the required service levels if Service Design considers the required service levels at the very beginning of the Service Lifecycle, rather than at some later stage.

Other considerations in application sizing are the resilience aspects that it may be necessary to build into the design of new services. Capacity Management is able to provide advice and guidance to the Availability Management process on the resources required to provide the required level of performance and resilience.

The sizing of the application should be refined as the design and development process progresses. The use of modelling can be used within the application sizing process.

The SLRs of the planned application developments should not be considered in isolation. The resources to be utilized by the application are likely to be shared with other services, and potential threats to existing SLA targets must be recognized and managed.

When purchasing software packages from external suppliers, it is just as important to understand the resource requirements needed to support the service. Often it can be difficult to obtain this information from the suppliers

and it may vary, depending on throughput. Therefore, it is beneficial to identify similar customers of the product and to gain an understanding of the resource implications from them. It may be pertinent to benchmark, evaluate or trial the product prior to purchase.

Key message

Quality must be built in.

Some aspects of service quality can be improved after implementation (additional hardware can be added to improve performance, for example). Others – particularly aspects such as reliability and maintainability of applications software – rely on quality being ‘built in’, since to attempt to add it at a later stage is, in effect, redesign and redevelopment, normally at a much higher cost than the original development. Even in the hardware example quoted above, it is likely to cost more to add additional capacity after service implementation rather than as part of the original project.

4.3.6 Triggers, inputs, outputs and interfaces

There are many triggers that will initiate Capacity Management activities. These include:

- Service breaches, capacity or performance events and alerts, including threshold events
- Exception reports
- Periodic revision of current capacity and performance and the review of forecasts, reports and plans
- New and changed services requiring additional capacity
- Periodic trending and modelling
- Review and revision of business and IT plans and strategies
- Review and revision of designs and strategies
- Review and revision of SLAs, OLAs, contracts or any other agreements.

There are a number of sources of information that are relevant to the Capacity Management process. Some of these are as follows.

4.3.6.1 Inputs

- **Business information:** from the organization’s business strategy, plans and financial plans, and information on their current and future requirements.
- **Service and IT information:** from Service Strategy, the IT strategy and plans and current budgets, covering all areas of technology and technology plans,

including the infrastructure, environment, data and applications, and the way in which they relate to business strategy and plans.

- **Component performance and capacity information:** of both existing and new technology, from manufacturers and suppliers.
- **Service performance issues:** the Incident and Problem Management processes, with incidents and problems relating to poor performance.
- **Service information:** from the SLM process, with details of the services from the Service Portfolio and the Service Catalogue and service level targets within SLAs and SLRs, and possibly from the monitoring of SLAs, service reviews and breaches of the SLAs.
- **Financial information:** from Financial Management, the cost of service provision, the cost of resources, components and upgrades, the resultant business benefit and the financial plans and budgets, together with the costs associated with service and component failure. Some of the costs of components and upgrades to components will be obtained from procurement, suppliers and manufacturers.
- **Change information:** from the Change Management process, with a Change Schedule and a need to assess all changes for their impact on the capacity of the technology.
- **Performance information:** from the Capacity Management Information System (CMIS) on the current performance of both all existing services and IT infrastructure components.
- **CMS:** containing information on the relationships between the business, the services, the supporting services and the technology.
- **Workload information:** from the IT Operations team, with schedules of all the work that needs to be run, and information on the dependencies between different services and information, and the interdependencies within a service.

4.3.6.2 Outputs

The outputs of Capacity Management are used within all other parts of the process, by many other processes and by other parts of the organization. Often this information is supplied as electronic reports or displays on shared areas, or as pages on intranet servers, to ensure the most up-to-date information is always used. The information provided is as follows:

- **The Capacity Management Information System (CMIS):** holds the information needed by all subprocesses within Capacity Management. For example,

the data monitored and collected as part of Component and Service Capacity Management is used in Business Capacity Management to determine what infrastructure components or upgrades to components are needed, and when.

- **The Capacity Plan:** used by all areas of the business and IT management, and is acted on by the IT service provider and senior management of the organization to plan the capacity of the IT infrastructure. It also provides planning input to many other areas of IT and the business. It contains information on the current usage of service and components, and plans for the development of IT capacity to meet the needs in the growth of both existing service and any agreed new services. The Capacity Plan should be actively used as a basis for decision-making. Too often, Capacity Plans are created and never referred to or used.
- **Service performance information and reports:** used by many other processes. For example, the Capacity Management process assists Service Level Management with the reporting and reviewing of service performance and the development of new SLRs or changes to existing SLAs. It also assists the Financial Management process by identifying when money needs to be budgeted for IT infrastructure upgrades, or the purchase of new components.
- **Workload analysis and reports:** used by IT Operations to assess and implement changes in conjunction with Capacity Management to schedule or reschedule when services or workloads are run, to ensure that the most effective and efficient use is made of the available resources.
- **Ad hoc capacity and performance reports:** used by all areas of Capacity Management, IT and the business to analyse and resolve service and performance issues.
- **Forecasts and predictive reports:** used by all areas to analyse, predict and forecast particular business and IT scenarios and their potential solutions.
- **Thresholds, alerts and events.**

4.3.7 Key Performance Indicators

Some of the KPIs and metrics that can be used to judge the efficiency and effectiveness of the Capacity Management activities should include:

- Accurate business forecasts:
 - Production of workload forecasts on time
 - Percentage accuracy of forecasts of business trends
 - Timely incorporation of business plans into the Capacity Plan

- Reduction in the number of variances from the business plans and Capacity Plans.
- Knowledge of current and future technologies:
 - Increased ability to monitor performance and throughput of all services and components
 - Timely justification and implementation of new technology in line with business requirements (time, cost and functionality)
 - Reduction in the use of old technology, causing breached SLAs due to problems with support or performance.
- Ability to demonstrate cost-effectiveness:
 - Reduction in last-minute buying to address urgent performance issues
 - Reduction in the over-capacity of IT
 - Accurate forecasts of planned expenditure
 - Reduction in the business disruption caused by a lack of adequate IT capacity
 - Relative reduction in the cost of production of the Capacity Plan.
- Ability to plan and implement the appropriate IT capacity to match business needs:
 - Percentage reduction in the number of incidents due to poor performance
 - Percentage reduction in lost business due to inadequate capacity
 - All new services implemented match Service Level Requirements (SLRs)
 - Increased percentage of recommendations made by Capacity Management are acted on
 - Reduction in the number of SLA breaches due to either poor service performance or poor component performance.

4.3.8 Information Management

The aim of the CMIS is to provide the relevant capacity and performance information to produce reports and support the Capacity Management process. These reports provide valuable information to many IT and Service Management processes. These reports should include the following.

Component-based reports

For each component there should be a team of technical staff responsible for its control and management. Reports must be produced to illustrate how components are

performing and how much of their maximum capacity is being used.

Service-based reports

Reports and information must also be produced to illustrate how the service and its constituent components are performing with respect to their overall service targets and constraints. These reports will provide the basis of SLM and customer service reports.

Exception reports

Reports that show management and technical staff when the capacity and performance of a particular component or service becomes unacceptable are also a required from analysis of capacity data. Thresholds can be set for any component, service or measurement within the CMIS. An example threshold may be that processor percentage utilization for a particular server has breached 70% for three consecutive hours, or that the concurrent number of logged-in users exceeds the agreed limit.

In particular, exception reports are of interest to the SLM process in determining whether the targets in SLAs have been breached. Also the Incident and Problem Management processes may be able to use the exception reports in the resolution of incidents and problems.

Predictive and forecast reports

To ensure the IT service provider continues to provide the required service levels, the Capacity Management process must predict future workloads and growth. To do this, future component and service capacity and performance must be forecast. This can be done in a variety of ways, depending on the techniques and the technology used. Changes to workloads by the development and implementation of new functionality and services must be considered alongside growth in the current functionality and services driven by business growth. A simple example of a capacity forecast is a correlation between a business driver and a component utilization, e.g. processor utilization against the number of customer accounts. This data can be correlated to find the effect that an increase in the number of customer accounts will have on the processor utilization. If the forecasts on future capacity requirements identify a requirement for increased resource, this requirement needs to be input into the Capacity Plan and included within the IT budget cycle.

Often capacity reports are consolidated together and stored on an intranet site so that anyone can access and refer to them.

4.3.8.1 Capacity Management Information System

Often capacity data is stored in technology-specific tools and databases, and full value of the data, the information and its analysis is not obtained. The true value of the data can only be obtained when the data is combined into a single set of integrated, information repositories or set of databases.

The Capacity Management Information System (CMIS) is the cornerstone of a successful Capacity Management process. Information contained within the CMIS is stored and analysed by all the sub-processes of Capacity Management because it is a repository that holds a number of different types of data, including business, service, resource or utilization and financial data, from all areas of technology.

However, the CMIS is unlikely to be a single database, and probably exists in several physical locations. Data from all areas of technology, and all components that make up the IT services, can then be combined for analysis and provision of technical and management reporting. Only when all of the information is integrated can 'end-to-end' service reports be produced. The integrity and accuracy of the data within the CMIS needs to be carefully managed. If the CMIS is not part of an overall CMS or SKMS, then links between these systems need to be implemented to ensure consistency and accuracy of the information recorded within them.

The information in the CMIS is used to form the basis of performance and Capacity Management reports and views that are to be delivered to customers, IT management and technical personnel. Also, the data is utilized to generate future capacity forecasts and allow Capacity Management to plan for future capacity requirements. Often a web interface is provided to the CMIS to provide the different access and views required outside of the Capacity Management process itself.

The full range of data types stored within the CMIS is as follows.

Business data

It is essential to have quality information on the current and future needs of the business. The future business plans of the organization need to be considered and the effects on the IT services understood. The business data is used to forecast and validate how changes in business drivers affect the capacity and performance of the IT infrastructure. Business data should include business

transactions or measurements such as the number of accounts, the number of invoices generated, the number of product lines.

Service data

To achieve a service-orientated approach to Capacity Management, service data should be stored within the CMIS. Typical service data are transaction response times, transaction rates, workload volumes, etc. In general, the SLAs and SLRs provide the service targets for which the Capacity Management process needs to record and monitor data. To ensure that the targets in the SLAs are achieved, SLM thresholds should be included, so that the monitoring activity can measure against these service thresholds and raise exception warnings and reports before service targets are breached.

Component utilization data

The CMIS also needs to record resource data consisting of utilization, threshold and limit information on all of the technological components supporting the services. Most of the IT components have limitations on the level to which they should be utilized. Beyond this level of utilization, the resource will be over-utilized and the performance of the services using the resource will be impaired. For example, the maximum recommended level of utilization on a processor could be 80%, or the utilization of a shared Ethernet LAN segment should not exceed 40%.

Also, components have various physical limitations beyond which greater connectivity or use is impossible. For example, the maximum number of connections through an application or a network gateway is 100, or a particular type of disk has a physical capacity of 15Gb. The CMIS should therefore contain, for each component and the maximum performance and capacity limits, current and past utilization rates and the associated component thresholds. Over time this can require vast amounts of data to be accumulated, so there need to be good techniques for analysing, aggregating and archiving this data.

Financial data

The Capacity Management process requires financial data. For evaluating alternative upgrade options, when proposing various scenarios in the Capacity Plan, the financial cost of the upgrades to the components of the IT infrastructure, together with information about the current IT hardware budget, must be known and included in the considerations. Most of this data may be available from the Financial Management for IT services process, but

Capacity Management needs to consider this information when managing the future business requirements.

4.3.9 Challenges, Critical Success Factors and risks

One of the major challenges facing Capacity Management is persuading the business to provide information on its strategic business plans, to enable the IT service provider organization to provide effective Business Continuity Management (BCM). This is particularly true in outsourced situations where there may be commercial or confidential reasons why this data cannot be shared. Even if the data on the strategic business plan is available, there may be issues with regard to the quality or accuracy of the data contained within the business plans with regard to BCM.

Another challenge is the combination of all of the CCM data into an integrated set of information that can be analysed in a consistent manner to provide details of the usage of all components of the services. This is particularly challenging when the information from the different technologies is provided by different tools in differing formats. Often the quality of component information on the performance of the technology is variable in both its quality and accuracy.

The amounts of information produced by BCM, and especially SCM and CCM, are huge and the analysis of this information is difficult to achieve. The people and the processes need to focus on the key resources and their usage, whilst not ignoring other areas. In order to do this, appropriate thresholds must be used, and reliance placed on the tools and technology to automatically manage the technology and provide warnings and alerts when things deviate significantly from the 'norm'.

The main CSFs for the Capacity Management process are:

- Accurate business forecasts
- Knowledge of current and future technologies
- Ability to demonstrate cost-effectiveness
- Ability to plan and implement the appropriate IT capacity to match business need.

Some of the major risks associated with Capacity Management include:

- A lack of commitment from the business to the Capacity Management process
- A lack of appropriate information from the business on future plans and strategies

- A lack of senior management commitment or a lack of resources and/or budget for the Capacity Management process
- SCM and CCM performed in isolation because BCM is difficult, or there is a lack of appropriate and accurate business information
- The processes become too bureaucratic or manually intensive
- The processes focus too much on the technology (CCM) and not enough on the services (SCM) and the business (BCM)
- The reports and information provided are too bulky or too technical and do not give the information required or appropriate to the customers and the business.

4.4 AVAILABILITY MANAGEMENT

4.4.1 Purpose/goal/objective

The goal of the Availability Management process is to ensure that the level of service availability delivered in all services is matched to or exceeds the current and future agreed needs of the business, in a cost-effective manner.

The purpose of Availability Management is to provide a point of focus and management for all availability-related issues, relating to both services and resources, ensuring that availability targets in all areas are measured and achieved.

The objectives of Availability Management are to:

- Produce and maintain an appropriate and up-to-date Availability Plan that reflects the current and future needs of the business
- Provide advice and guidance to all other areas of the business and IT on all availability-related issues
- Ensure that service availability achievements meet or exceed all their agreed targets, by managing services and resources-related availability performance
- Assist with the diagnosis and resolution of availability-related incidents and problems
- Assess the impact of all changes on the Availability Plan and the performance and capacity of all services and resources
- Ensure that proactive measures to improve the availability of services are implemented wherever it is cost-justifiable to do so.

Availability Management should ensure the agreed level of availability is provided. The measurement and monitoring

of IT availability is a key activity to ensure availability levels are being met consistently. Availability Management should look to continually optimize and proactively improve the availability of the IT infrastructure, the services and the supporting organization, in order to provide cost-effective availability improvements that can deliver business and customer benefits.

4.4.2 Scope

The scope of the Availability Management process covers the design, implementation, measurement, management and improvement of IT service and component availability. Availability Management needs to understand the service and component availability requirements from the business perspective in terms of the:

- Current business processes, their operation and requirements
- Future business plans and requirements
- Service targets and the current IT service operation and delivery
- IT infrastructure, data, applications and environment and their performance
- Business impacts and priorities in relation to the services and their usage.

Understanding all of this will enable Availability Management to ensure that all the services and components are designed and delivered to meet their targets in terms of agreed business needs. The Availability Management process:

- Should be applied to all operational services and technology, particularly those covered by SLAs. It can also be applied to those IT services deemed to be business critical regardless of whether formal SLAs exist
- Should be applied to all new IT services and for existing services where Service Level Requirements (SLRs) or Service Level Agreements (SLAs) have been established
- Should be applied to all supporting services and the partners and suppliers (both internal and external) that form the IT support organization as a precursor to the creation of formal agreements
- Considers all aspects of the IT services and components and supporting organizations that may impact availability, including training, skills, process effectiveness, procedures and tools.

The Availability Management process does not include Business Continuity Management and the resumption of business processing after a major disaster. The support of BCM is included within IT Service Continuity Management (ITSCM). However, Availability Management does provide key inputs to ITSCM, and the two processes have a close relationship, particularly in the assessment and management of risks and in the implementation of risk reduction and resilience measures.

The Availability Management process should include:

- Monitoring of all aspects of availability, reliability and maintainability of IT services and the supporting components, with appropriate events, alarms and escalation, with automated scripts for recovery
- Maintenance of a set of methods, techniques and calculations for all availability measurements, metrics and reporting
- Assistance with risk assessment and management activities
- Collection of measurements, analysis and production of regular and ad hoc reports on service and component availability
- Understanding the agreed current and future demands of the business for IT services and their availability
- Influencing the design of services and components to align with business needs
- Producing an Availability Plan that enables the service provider to continue to provide and improve services in line with availability targets defined in Service Level Agreements (SLAs), and to plan and forecast future availability levels required, as defined in Service Level Requirements (SLRs)
- Maintaining a schedule of tests for all resilient and fail-over components and mechanisms
- Assistance with the identification and resolution of any incidents and problems associated with service or component unavailability
- Proactive improvement of service or component availability wherever it is cost-justifiable and meets the needs of the business.

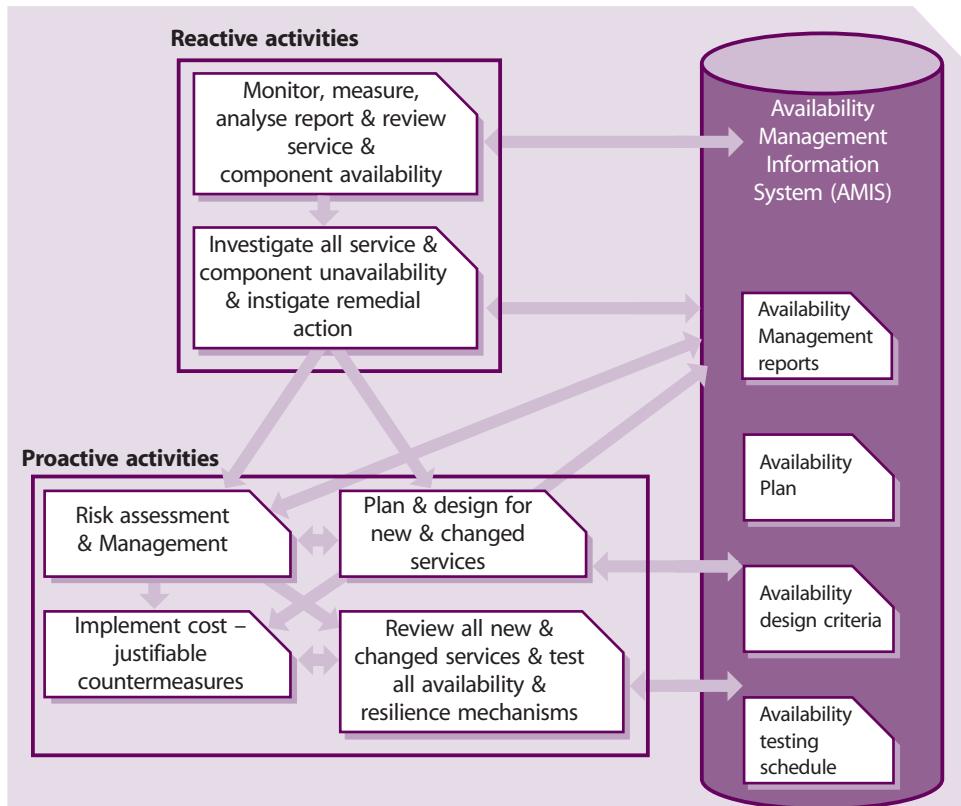


Figure 4.13 The Availability Management process

4.4.3 Value to the business

The Availability Management process ensures that the availability of systems and services matches the evolving agreed needs of the business. The role of IT within the business is now pivotal. The availability and reliability of IT services can directly influence customer satisfaction and the reputation of the business. This is why Availability Management is essential in ensuring IT delivers the right levels of service availability required by the business to satisfy its business objectives and deliver the quality of service demanded by its customers. In today's competitive marketplace, customer satisfaction with service(s) provided is paramount. Customer loyalty can no longer be relied on, and dissatisfaction with the availability and reliability of IT service can be a key factor in customers taking their business to a competitor.

The Availability Management process and planning, just like Capacity Management, must be involved in all stages of the Service Lifecycle, from Strategy and Design, through Transition and Operation to Improvement. The appropriate availability and resilience should be designed into services and components from the initial design stages. This will ensure not only that the availability of any new or changed service meets its expected targets, but also that

all existing services and components continue to meet all of their targets. This is the basis of stable service provision.

4.4.4 Policies/principles/basic concepts

The Availability Management process is continually trying to ensure that all operational services meet their agreed availability targets, and that new or changed services are designed appropriately to meet their intended targets, without compromising the performance of existing services. In order to achieve this, Availability Management should perform the reactive and proactive activities illustrated in Figure 4.13.

The reactive activities of Availability Management consist of monitoring, measuring, analysing, reporting and reviewing all aspects of component and service availability. This is to ensure that all agreed service targets are measured and achieved. Wherever deviations or breaches are detected, these are investigated and remedial action instigated. Most of these activities are conducted within the Operations stage of the lifecycle and are linked into the monitoring and control activities, Event and Incident Management processes. (See the Service Operation publication.)

The proactive activities consist of producing recommendations, plans and documents on design guidelines and criteria for new and changed services, and the continual improvement of service and reduction of risk in existing services wherever it can be cost-justified. These are key aspects to be considered within Service Design activities.

An effective Availability Management process, consisting of both the reactive and proactive activities, can 'make a big difference' and will be recognized as such by the business, if the deployment of Availability Management within an IT organization has a strong emphasis on the needs of the business and customers. To reinforce this emphasis, there are several guiding principles that should underpin the Availability Management process and its focus:

- Service availability is at the core of customer satisfaction and business success: there is a direct correlation in most organizations between the service availability and customer and user satisfaction, where poor service performance is defined as being unavailable.
- Recognizing that when services fail, it is still possible to achieve business, customer and user satisfaction and recognition: the way a service provider reacts in a failure situation has a major influence on customer and user perception and expectation.
- Improving availability can only begin after understanding how the IT services support the operation of the business.
- Service availability is only as good as the weakest link on the chain: it can be greatly increased by the elimination of Single Points of Failure (SPoFs) or an unreliable or weak component.
- Availability is not just a reactive process. The more proactive the process, the better service availability will be. Availability should not purely react to service and component failure. The more events and failures are predicted, pre-empted and prevented, the higher the level of service availability.
- It is cheaper to design the right level of service availability into a service from the start rather than try and 'bolt it on' subsequently. Adding resilience into a service or component is invariably more expensive than designing it in from the start. Also, once a service gets a bad name for unreliability, it becomes very difficult to change the image. Resilience is also a key consideration of ITSCM, and this should be considered at the same time.

The scope of Availability Management covers the design, implementation, measurement and management of IT

service and infrastructure availability. This is reflected in the process description shown in Figure 4.13 and described in the following paragraphs.

The Availability Management process has two key elements:

- Reactive activities: the reactive aspect of Availability Management involves the monitoring, measuring, analysis and management of all events, incidents and problems involving unavailability. These activities are principally involved within operational roles.
- Proactive activities: the proactive activities of Availability Management involve the proactive planning, design and improvement of availability. These activities are principally involved within design and planning roles.

Availability Management is completed at two interconnected levels:

- **Service availability:** involves all aspects of service availability and unavailability and the impact of component availability, or the potential impact of component unavailability on service availability
- **Component availability:** involves all aspects of component availability and unavailability.

Availability Management relies on the monitoring, measurement, analysis and reporting of the following aspects:

Availability: the ability of a service, component or CI to perform its agreed function when required. It is often measured and reported as a percentage:

$$\frac{(\text{Agreed Service Time (AST)} - \text{downtime})}{\text{Agreed Service Time (AST)}} \times 100 \%$$

$$\text{Availability} (\%) = \frac{\text{Actual Service Time}}{\text{Agreed Service Time (AST)}} \times 100 \%$$

Note: Downtime should only be included in the above calculation when it occurs within the Agreed Service Time (AST). However, total downtime should also be recorded and reported.

Reliability: a measure of how long a service, component or CI can perform its agreed function without interruption. The reliability of the service can be improved by increasing the reliability of individual components or by increasing the resilience of the service to individual component failure (i.e. increasing the component redundancy, e.g. by using load-balancing techniques). It is often measured and reported as Mean Time Between Service Incidents (MTBSI) or Mean Time Between Failures (MTBF):

$$\text{Reliability (MTBSI in hours)} = \frac{\text{Available time in hours}}{\text{Number of breaks}}$$

$$\text{Reliability (MTBF in hours)} = \frac{\text{Available time in hours} - \text{Total downtime in hours}}{\text{Number of breaks}}$$

Maintainability: a measure of how quickly and effectively a service, component or CI can be restored to normal working after a failure. It is measured and reported as Mean Time to Restore Service (MTRS) and should be calculated using the following formula:

$$\text{Maintainability (MTRS in hours)} = \frac{\text{Total downtime in hours}}{\text{Number of service breaks}}$$

MTRS should be used to avoid the ambiguity of the more common industry term Mean Time To Repair (MTTR), which in some definitions includes only repair time, but in others includes recovery time. The downtime in MTRS covers all the contributory factors that make the service, component or CI unavailable:

- Time to record
- Time to respond
- Time to resolve
- Time to physically repair or replace
- Time to recover.

Example: A situation where a 24 x 7 service has been running for a period of 5,020 hours with only two breaks, one of six hours and one of 14 hours, would give the following figures:

$$\text{Availability} = (5,020 - (6+14)) / 5,020 \times 100 = 99.60\%$$

$$\text{Reliability (MTBSI)} = 5,020 / 2 = 2,510 \text{ hours}$$

$$\text{Reliability (MTBF)} = 5,020 - (6+14) / 2 = 2,500 \text{ hours}$$

$$\text{Maintainability (MTRS)} = (6+14) / 2 = 10 \text{ hours}$$

Serviceability: the ability of a third-party supplier to meet the terms of their contract. Often this contract will include agreed levels of availability, reliability and/or maintainability for a supporting service or component.

These aspects and their inter-relationships are illustrated in Figure 4.14.

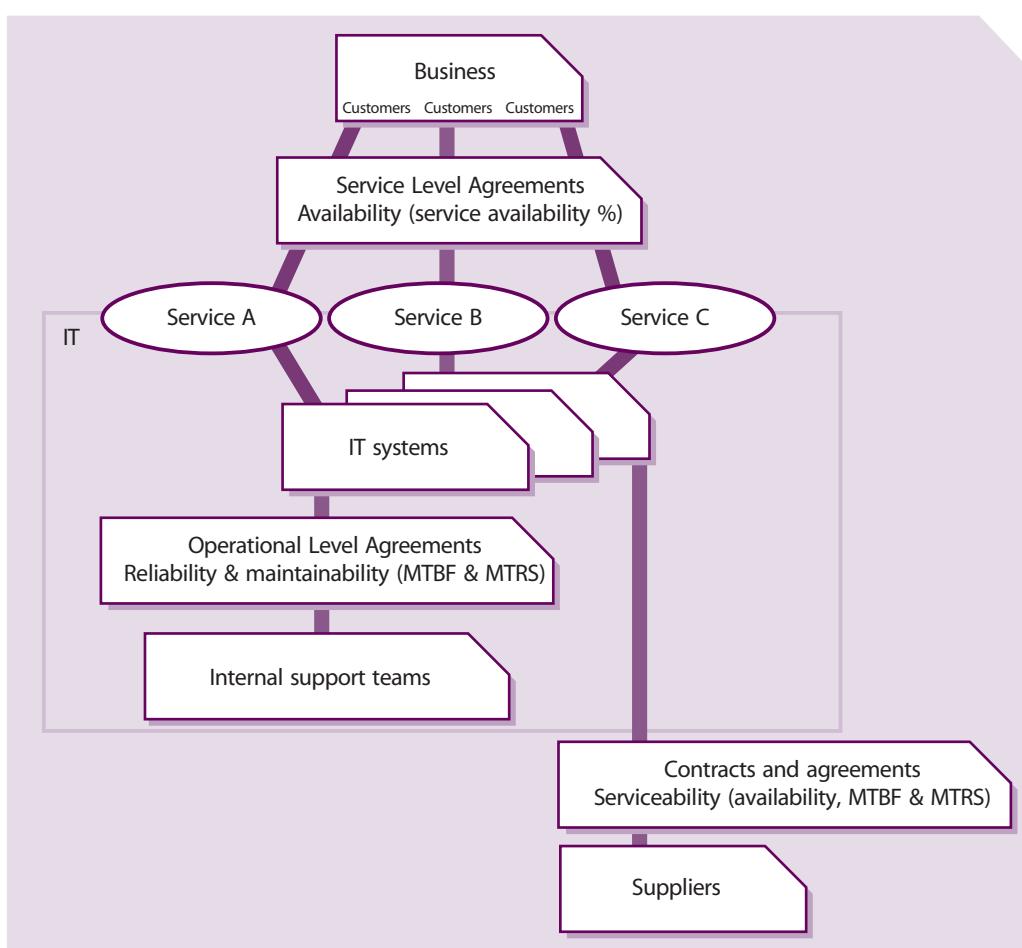


Figure 4.14 Availability terms and measurements

Although the principal service target contained within SLAs for the customers and business is availability, as illustrated in Figure 4.14, some customers also require reliability and maintainability targets to be included as well. Where these are included they should relate to service reliability and maintainability targets, whereas the reliability and maintainability targets contained in OLAs and contracts relate to component and supporting service targets and can often include availability targets relating to the relevant components or supporting services.

The term Vital Business Function (VBF) is used to reflect the business critical elements of the business process supported by an IT service. An IT service may support a number of business functions that are less critical. For example, an automated teller machine (ATM) or cash dispenser service VBF would be the dispensing of cash. However, the ability to obtain a statement from an ATM may not be considered as vital. This distinction is important and should influence availability design and associated costs. The more vital the business function generally, the greater the level of resilience and availability that needs to be incorporated into the design required in the supporting IT services. For all services, whether VBFs or not, the availability requirements should be determined by the business and not by IT. The initial availability targets are often set at too high a level, and this leads to either over-priced services or an iterative discussion between the service provider and the business to agree an appropriate compromise between the service availability and the cost of the service and its supporting technology.

Certain VBFs may need special designs, which are now being used as a matter of course within Service Design plans, incorporating:

- **High availability:** a characteristic of the IT service that minimizes or masks the effects of IT component failure to the users of a service.
- **Fault tolerance:** the ability of an IT service, component or CI to continue to operate correctly after failure of a component part.
- **Continuous operation:** an approach or design to eliminate planned downtime of an IT service. Note that individual components or CIs may be down even though the IT service remains available.
- **Continuous availability:** an approach or design to achieve 100% availability. A continuously Available IT service has no planned or unplanned downtime.

Industry view

Many suppliers commit to high availability or continuous availability solutions only if stringent environmental standards and resilient processes are used. They often agree to such contracts only after a site survey has been completed and additional, sometimes costly, improvements have been made.

Availability Management commences as soon as the availability requirements for an IT service are clear enough to be articulated. It is an ongoing process, finishing only when the IT service is decommissioned or retired. The key activities of the Availability Management process are:

- Determining the availability requirements from the business for a new or enhanced IT service and formulating the availability and recovery design criteria for the supporting IT components
- Determining the VBFs, in conjunction with the business and ITSCM
- Determining the impact arising from IT service and component failure in conjunction with ITSCM and, where appropriate, reviewing the availability design criteria to provide additional resilience to prevent or minimize impact to the business
- Defining the targets for availability, reliability and maintainability for the IT infrastructure components that underpin the IT service to enable these to be documented and agreed within SLAs, OLAs and contracts
- Establishing measures and reporting of availability, reliability and maintainability that reflect the business, user and IT support organization perspectives
- Monitoring and trend analysis of the availability, reliability and maintainability of IT components
- Reviewing IT service and component availability and identifying unacceptable levels
- Investigating the underlying reasons for unacceptable availability
- Producing and maintaining an Availability Plan that prioritizes and plans IT availability improvements.

4.4.5 Process activities, methods and techniques

The Availability Management process depends heavily on the measurement of service and component achievements with regard to availability.

Key messages

- 'If you don't measure it, you can't manage it'
- 'If you don't measure it, you can't improve it'
- 'If you don't measure it, you probably don't care'
- 'If you can't influence or control it, then don't measure it'

'What to measure and how to report it' inevitably depends on which activity is being supported, who the recipients are and how the information is to be utilized. It is important to recognize the differing perspectives of availability to ensure measurement and reporting satisfies these varied needs:

- The business perspective considers IT service availability in terms of its contribution or impact on the VBFs that drive the business operation.
- The user perspective considers IT service availability as a combination of three factors, namely the frequency, the duration and the scope of impact, i.e. all users, some users, all business functions or certain business functions – the user also considers IT service availability in terms of response times. For many performance-centric applications, poor response times are considered equal in impact to failures of technology.
- The IT service provider perspective considers IT service and component availability with regard to availability, reliability and maintainability.

In order to satisfy the differing perspectives of availability, Availability Management needs to consider the spectrum of measures needed to report the 'same' level of availability in different ways. Measurements need to be meaningful and add value if availability measurement and reporting are ultimately to deliver benefit to the IT and business organizations. This is influenced strongly by the combination of 'what you measure' and 'how you report it'.

4.4.5.1 The reactive activities of Availability Management

Monitor, measure, analyse and report service and component availability

A key output from the Availability Management process is the measurement and reporting of IT availability. Availability measures should be incorporated into SLAs, OLAs and any underpinning contracts. These should be reviewed regularly at Service Level review meetings. Measurement and reporting provide the basis for:

- Monitoring the actual availability delivered versus agreed targets

- Establishing measures of availability and agreeing availability targets with the business
- Identifying unacceptable levels of availability that impact the business and users
- Reviewing availability with the IT support organization
- Continual improvement activities to optimize availability.

The IT service provider organizations have, for many years, measured and reported on their perspective of availability. Traditionally these measures have concentrated on component availability and have been somewhat divorced from the business and user views. Typically these traditional measures are based on a combination of an availability percentage (%), time lost and the frequency of failure. Some examples of these traditional measures are as follows:

- **Per cent available** – the truly 'traditional' measure that represents availability as a percentage and, as such, much more useful as a component availability measure than a service availability measure. It is typically used to track and report achievement against a service level target. It tends to emphasize the 'big number' such that if the service level target was 98.5% and the achievement was 98.3%, then it does not seem that bad. This can encourage a complacent behaviour within the IT support organization.
- **Per cent unavailable** – the inverse of the above. This representation, however, has the benefit of focusing on non-availability. Based on the above example, if the target for non-availability is 1.5% and the achievement was 1.7%, then this is a much larger relative difference. This method of reporting is more likely to create awareness of the shortfall in delivering the level of availability required.
- **Duration** – achieved by converting the percentage unavailable into hours and minutes. This provides a more 'human' measure that people can relate to. If the weekly downtime target is two hours, but one week the actual downtime was four hours; this would represent a trend leading to an additional four days of non-availability to the business over a full year. This type of measure and reporting is more likely to encourage focus on service improvement.
- **Frequency of failure** – used to record the number of interruptions to the IT service. It helps provide a good indication of reliability from a user perspective. It is best used in combination with 'duration' to take a balanced view of the level of service interruptions and the duration of time lost to the business.
- **Impact of failure** – this is the true measure of service unavailability. It depends on mature incident recording

where the inability of users to perform their business tasks is the most important piece of information captured. All other measures suffer from a potential to mask the real effects of service failure and are often converted to a financial impact.

The business may have, for many years, accepted that the IT availability that they experience is represented in terms of component availability rather than overall service or business availability. However, this is no longer being viewed as acceptable and the business is keen to better represent availability in measure(s) that demonstrate the positive and negative consequences of IT availability on their business and users.

Key messages

The most important availability measurements are those that reflect and measure availability from the business and user perspective.

Availability Management needs to consider availability from both a business/IT service provider perspective and from an IT component perspective. These are entirely different aspects, and while the underlying concept is similar, the measurement, focus and impact are entirely different.

The sole purpose of producing these availability measurements and reports, including those from the business perspective, is to improve the quality and availability of IT service provided to the business and users. All measures, reports and activities should reflect this purpose.

Availability, when measured and reported to reflect the experience of the user, provides a more representative view on overall IT service quality. The user view of availability is influenced by three factors:

- Frequency of downtime
- Duration of downtime
- Scope of impact.

Measurements and reporting of user availability should therefore embrace these factors. The methodology employed to reflect user availability could consider two approaches:

- **Impact by user minutes lost:** this is to base calculations on the duration of downtime multiplied by the number of users impacted. This can be the basis to report availability as lost user productivity, or to calculate the availability percentage from a user perspective, and can also include the costs of recovery for lost productivity (e.g. increased overtime payments).

- **Impact by business transaction:** this is to base calculations on the number of business transactions that could not be processed during the period of downtime. This provides a better indication of business impact reflecting differing transaction processing profiles across the time of day, week etc. In many instances it may be the case that the user impact correlates to a VBF, e.g. if the user takes customer purchase orders and a VBF is customer sales. This single measure is the basis to reflect impact to the business operation and user.

The method employed should be influenced by the nature of the business operation. A business operation supporting data entry activity is well suited to reporting that reflects user productivity loss. Business operations that are more customer-facing, e.g. ATM services, benefit from reporting transaction impact. It should also be noted that not all business impact is user-related. With increasing automation and electronic processing, the ability to process automated transactions or meet market cut-off times can also have a large financial impact that may be greater than the ability of users to work.

The IT support organization needs to have a keen awareness of the user experience of availability. However, the real benefits come from aggregating the user view into the overall business view. A guiding principle of the Availability Management process is that '**Improving availability can only begin when the way technology supports the business is understood**'. Therefore Availability Management isn't just about understanding the availability of each IT component, but is all about understanding the impact of component failure on service and user availability. From the business perspective, an IT service can only be considered available when the business is able to perform all vital business functions required to drive the business operation. For the IT service to be available, it therefore relies on all components on which the service depends being available, i.e. systems, key components, network, data and applications.

The traditional IT approach would be to measure individually the availability of each of these components. However, the true measure of availability has to be based on the positive and negative impacts on the VBFs on which the business operation is dependent. This approach ensures that SLAs and IT availability reporting are based on measures that are understood by both the business and IT. By measuring the VBFs that rely on IT services, measurement and reporting becomes business-driven, with the impact of failure reflecting the consequences to the business. It is also important that the availability of the services is defined and agreed with the business and

reflected within SLAs. This definition of availability should include:

- What is the minimum available level of functionality of the service?
- At what level of service response is the service considered unavailable?
- Where will this level of functionality and response be measured?
- What are the relative weightings for partial service unavailability?
- If one location or office is impacted, is the whole service considered unavailable, or is this considered to be 'partial unavailability'? This needs to be agreed with the customers.

Reporting and analysis tools are required for the manipulation of data stored in the various databases utilized by Availability Management. These tools can either be platform- or PC-based and are often a combination of the two. This will be influenced by the database repository technologies selected and the complexity of data processing and reporting required. Availability Management, once implemented and deployed, will be required to produce regular reports on an agreed basis, e.g. monthly availability reports, Availability Plan, Service Failure Analysis (SFA) status reports, etc. The activities involved within these reporting activities can require much manual effort and the only solution is to automate as much of the report generation activity as possible. For reporting purposes, organizational reporting standards should be used wherever possible. If these don't exist, IT standards should be developed so that IT reports can be developed using standard tools and techniques. This means that the integration and consolidation of reports will subsequently be much easier to achieve.

Unavailability analysis

All events and incidents causing unavailability of services and components should be investigated, with remedial actions being implemented within either the Availability Plan or the overall SIP. Trends should be produced from this analysis to direct and focus activities such as Service Failure Analysis (SFA) to those areas causing the most impact or disruption to the business and the users.

The overall costs of an IT service are influenced by the levels of availability required and the investments required in technology and services provided by the IT support organization to meet this requirement. Availability certainly does not come for free. However, it is important to reflect that the unavailability of IT also has a cost, therefore

unavailability isn't free either. For highly critical business processes and VBFs, it is necessary to consider not only the cost of providing the service, but also the costs that are incurred from failure. The optimum balance to strike is the cost of the availability solution weighed against the costs of unavailability.

Before any SLR is accepted, and ultimately the SLR or SLA is negotiated and agreed between the business and the IT organization, it is essential that the availability requirements of the business are analysed to assess if/how the IT service can deliver the required levels of availability. This applies not only to new IT services that are being introduced, but also to any requested changes to the availability requirements of existing IT services.

The cost of an IT failure could simply be expressed as the number of business or IT transactions impacted, either as an actual figure (derived from instrumentation) or based on an estimation. When measured against the VBFs that support the business operation, this can provide an obvious indication of the consequence of failure. The advantage of this approach is the relative ease of obtaining the impact data and the lack of any complex calculations. It also becomes a 'value' that is understood by both the business and IT organization. This can be the stimulus for identifying improvement opportunities and can become a key metric in monitoring the availability of IT services.

The major disadvantage of this approach is that it offers no obvious monetary value that would be needed to justify any significant financial investment decisions for improving availability. Where significant financial investment decisions are required, it is better to express the cost of failure arising from service, system, application or function loss to the business as a monetary 'value'.

The monetary value can be calculated as a combination of the tangible costs associated with failure, but can also include a number of intangible costs. The monetary value should also reflect the cost impact to the whole organization, i.e. the business and IT organization.

Tangible costs can include:

- Lost user productivity
- Lost IT staff productivity
- Lost revenue
- Overtime payments
- Wasted goods and material
- Imposed fines or penalty payments.

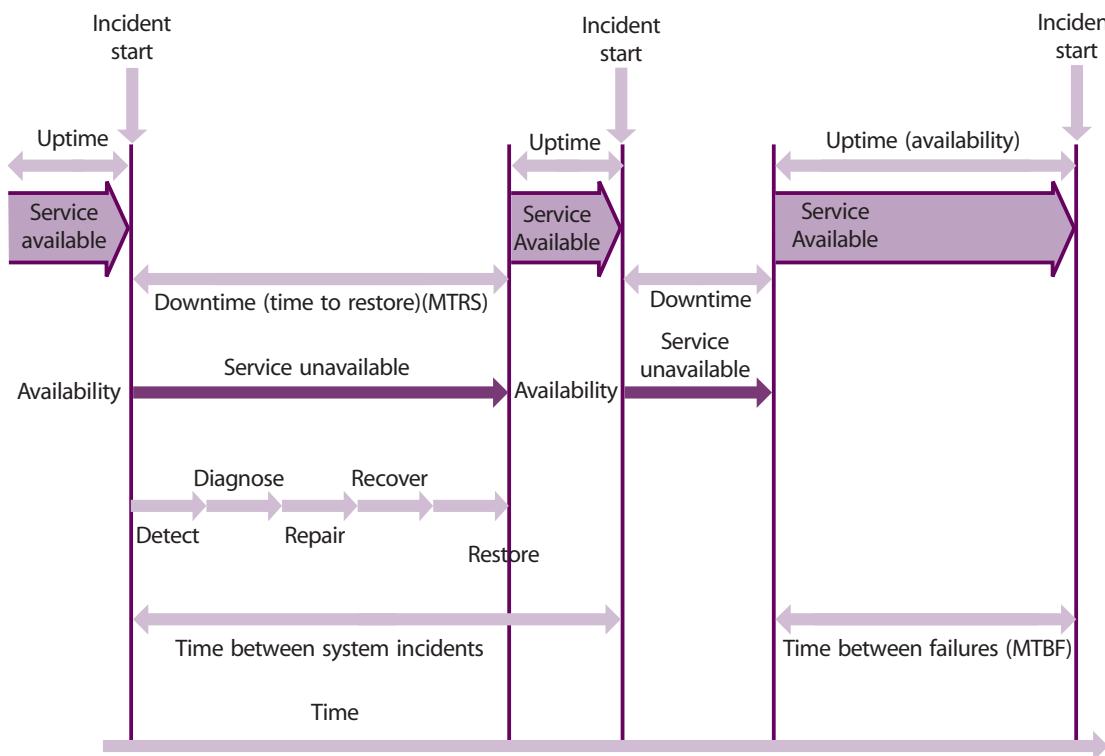


Figure 4.15 The expanded incident lifecycle

These costs are often well understood by the finance area of the business and IT organization, and in relative terms are easier to obtain and aggregate than the intangible costs associated with an IT failure.

Intangible costs can include:

- Loss of customers
- Loss of customer goodwill (customer dissatisfaction)
- Loss of business opportunity (to sell, gain new customers or revenue, etc.)
- Damage to business reputation
- Loss of confidence in IT service provider
- Damage to staff morale.

It is important not simply to dismiss the intangible costs (and the potential consequences) on the grounds that they may be difficult to measure. The overall unavailability of service, the total tangible cost and the total intangible costs arising from service unavailability are all key metrics in the measurement of the effectiveness of the Availability Management process.

The expanded incident lifecycle

A guiding principle of Availability Management is to recognize that it is still possible to gain customer satisfaction even when things go wrong. One approach to help achieve this requires Availability Management to ensure that the duration of any incident is minimized to

enable normal business operations to resume as quickly as possible. An aim of Availability Management is to ensure the duration and impact from incidents impacting IT services are minimized, to enable business operations to resume as quickly as is possible. The analysis of the 'expanded incident lifecycle' enables the total IT service downtime for any given incident to be broken down and mapped against the major stages through which all incidents progress (the lifecycle). Availability Management should work closely with Incident Management and Problem Management in the analysis of all incidents causing unavailability.

A good technique to help with the technical analysis of incidents affecting the availability of components and IT services is to take an incident 'lifecycle' view. Every incident passes through several major stages. The time elapsed in these stages may vary considerably. For Availability Management purposes, the standard incident 'lifecycle', as described within Incident Management, has been expanded to provide additional help and guidance particularly in the area of 'designing for recovery'. Figure 4.15 illustrates the expanded incident lifecycle.

From the above it can be seen that an incident can be broken down into individual stages within a lifecycle that can be timed and measured. This lifecycle view provides

an important framework in determining, amongst others, systems management requirements for event and incident detection, diagnostic data capture requirements and tools for diagnosis, recovery plans to aid speedy recovery and how to verify that IT service has been restored. The individual stages of the lifecycle are considered in more detail as follows.

- **Incident detection:** the time at which the IT service provider organization is made aware of an incident. Systems management tools positively influence the ability to detect events and incidents and therefore to improve levels of availability that can be delivered. Implementation and exploitation should have a strong focus on achieving high availability and enhanced recovery objectives. In the context of recovery, such tools should be exploited to provide automated failure detection, assist failure diagnosis and support automated error recovery, with scripted responses. Tools are very important in reducing all stages of the incident lifecycle, but principally the detection of events and incidents. Ideally the event is automatically detected and resolved, before the users have noticed it or have been impacted in any way.
- **Incident diagnosis:** the time at which diagnosis to determine the underlying cause has been completed. When IT components fail, it is important that the required level of diagnostics is captured, to enable problem determination to identify the root cause and resolve the issue. The use and capability of diagnostic tools and skills is critical to the speedy resolution of service issues. For certain failures, the capture of diagnostics may extend service downtime. However, the non-capture of the appropriate diagnostics creates and exposes the service to repeat failures. Where the time required to take diagnostics is considered excessive, or varies from the target, a review should be instigated to identify if techniques and/or procedures can be streamlined to reduce the time required. Equally the scope of the diagnostic data available for capture can be assessed to ensure only the diagnostic data considered essential is taken. The additional downtime required to capture diagnostics should be included in the recovery metrics documented for each IT component.
- **Incident repair:** the time at which the failure has been repaired/fixed. Repair times for incidents should be continuously monitored and compared against the targets agreed within OLAs, underpinning contracts and other agreements. This is particularly important with respect to externally provided services and supplier performance. Wherever breaches are observed,

techniques should be used to reduce or remove the breaches from similar incidents in the future.

- **Incident recovery:** the time at which component recovery has been completed. The backup and recovery requirements for the components underpinning a new IT service should be identified as early as possible within the design cycle. These requirements should cover hardware, software and data and recovery targets. The outcome from this activity should be a documented set of recovery requirements that enables the development of appropriate recovery plans. To anticipate and prepare for performing recovery such that reinstatement of service is effective and efficient requires the development and testing of appropriate recovery plans based on the documented recovery requirements. Wherever possible, the operational activities within the recovery plan should be automated. The testing of the recovery plans also delivers approximate timings for recovery. These recovery metrics can be used to support the communication of estimated recovery of service and validate or enhance the Component Failure Impact Analysis documentation. Availability Management must continuously seek and promote faster methods of recovery for all potential Incidents. This can be achieved via a range of methods, including automated failure detection, automated recovery, more stringent escalation procedures, exploitation of new and faster recovery tools and techniques. Availability requirements should also contribute to determining what spare parts are kept within the Definitive Spares to facilitate quick and effective repairs, as described within the Service Transition publication.
- **Incident restoration:** the time at which normal business service is resumed. An incident can only be considered 'closed' once service has been restored and normal business operation has resumed. It is important that the restored IT service is verified as working correctly as soon as service restoration is completed and before any technical staff involved in the incident are stood down. In the majority of cases, this is simply a case of getting confirmation from the affected users. However, the users for some services may be customers of the business, i.e. ATM services, internet-based services. For these types of services, it is recommended that IT service verification procedures are developed to enable the IT service provider organization to verify that a restored IT service is now working as expected. These could simply be visual checks of transaction throughput or user simulation scripts that validate the end-to-end service.

Each stage, and the associated time taken, influences the total downtime perceived by the user. By taking this approach it is possible to see where time is being 'lost' for the duration of an incident. For example, the service was unavailable to the business for 60 minutes, yet it only took five minutes to apply a fix – where did the other 55 minutes go?

Using this approach identifies possible areas of inefficiency that combine to make the loss of service experienced by the business greater than it need be. These could cover areas such as poor automation (alerts, automated recovery etc.), poor diagnostic tools and scripts, unclear escalation procedures (which delay the escalation to the appropriate technical support group or supplier), or lack of comprehensive operational documentation. Availability Management needs to work in close association with Incident and Problem Management to ensure repeat occurrences are eliminated. It is recommended that these measures are established and captured for all availability incidents. This provides Availability Management with metrics for both specific incidents and trending information. This information can be used as input to SFA assignments, SIP activities and regular Availability Management reporting and to provide an impetus for continual improvement activity to pursue cost-effective improvements. It can also enable targets to be set for specific stages of the incident lifecycle. While accepting that each incident may have a wide range of technical complexity, the targets can be used to reflect the consistency of how the IT service provider organization responds to incidents.

An output from the Availability Management process is the real-time monitoring requirements for IT services and components. To achieve the levels of availability required and/or ensure the rapid restoration of service following an IT failure requires investment and exploitation of a systems management toolset. Systems management tools are an essential building block for IT services that require a high level of availability and can provide an invaluable role in reducing the amount of downtime incurred. Availability Management requirements cover the detection and alerting of IT service and component exceptions, automated escalation and notification of IT failures and the automated recovery and restoration of components from known IT failure situations. This makes it possible to identify where 'time is being lost' and provides the basis for the identification of factors that can improve recovery and restoration times. These activities are performed on a regular basis within Service Operation.

Service Failure Analysis

Service Failure Analysis (SFA) is a technique designed to provide a structured approach to identifying the underlying causes of service interruptions to the user. SFA utilizes a range of data sources to assess where and why shortfalls in availability are occurring. SFA enables a holistic view to be taken to drive not just technology improvements, but also improvements to the IT support organization, processes, procedures and tools. SFA is run as an assignment or project, and may utilize other Availability Management methods and techniques to formulate the recommendations for improvement. The detailed analysis of service interruptions can identify opportunities to enhance levels of availability. SFA is a structured technique to identify improvement opportunities in end-to-end service availability that can deliver benefits to the user. Many of the activities involved in SFA are closely aligned with those of Problem Management, and in a number of organizations these activities are performed jointly by Problem and Availability Management.

The high-level objectives of SFA are:

- To improve the overall availability of IT services by producing a set of improvements for implementation or input to the Availability Plan
- To identify the underlying causes of service interruption to users
- To assess the effectiveness of the IT support organization and key processes
- To produce reports detailing the major findings and recommendations
- That availability improvements derived from SFA-driven activities are measured.

SFA initiatives should use input from all areas and all processes including, most importantly, the business and users. Each SFA assignment should have a recognized sponsor(s) (ideally, joint sponsorship from the IT and business) and involve resources from many technical and process areas. The use of the SFA approach:

- Provides the ability to deliver enhanced levels of availability without major cost
- Provides the business with visible commitment from the IT support organization
- Develops in-house skills and competencies to avoid expensive consultancy assignments related to availability improvement
- Encourages cross-functional team working and breaks barriers between teams, and is an enabler to lateral

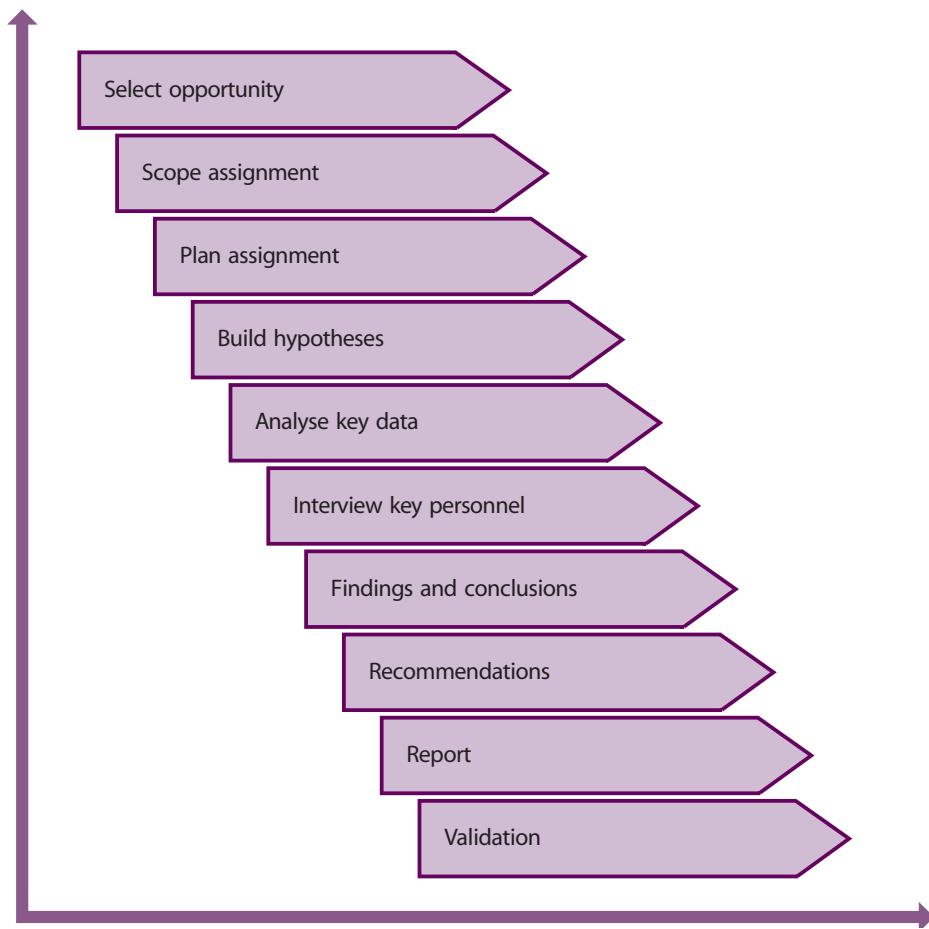


Figure 4.16 The structured approach to Service Failure Analysis (SFA)

thinking, challenging traditional thoughts and providing innovative, and often inexpensive, solutions

- Provides a programme of improvement opportunities that can make a real difference to service quality and user perception
- Provides opportunities that are focused on delivering benefit to the user
- Provides an independent 'health check' of IT Service Management processes and is the stimulus for process improvements.

To maximize both the time of individuals allocated to the SFA assignment and the quality of the delivered report, a structured approach is required. This structure is illustrated in Figure 4.16. This approach is similar to many consultancy models utilized within the industry, and in many ways Availability Management can be considered as providing via SFA a form of internal consultancy.

The above high-level structure is described briefly as follows.

- **Select opportunity:** prior to scheduling an SFA assignment, there needs to be agreement as to which IT service or technology is to be selected. It is

recommended that an agreed number of assignments are scheduled per year within the Availability Plan and, if possible, the IT services are selected in advance as part of the proactive approach to Availability Management. Before commencing with the SFA, it is important that the assignment has a recognized sponsor from within the IT organization and/or the business and that they are involved and regularly updated with progress of the SFA activity. This ensures organizational visibility to the SFA and ensures recommendations are endorsed at a senior level within the organization.

- **Scope assignment:** this is to state explicitly what areas are and are not covered within the assignment. This is normally documented in Terms of Reference issued prior to the assignment.
- **Plan assignment:** the SFA assignment needs to be planned a number of weeks in advance of the assignment commencing, with an agreed project plan and a committed set of resources. The project should look at identifying improvement opportunities that benefit the user. It is therefore important that an end-to-end view of the data and Management Information

System (MIS) requirements is taken. The data and documentation should be collected from all areas and analysed from the user and business perspective. A 'virtual' SFA team should be formed from all relevant areas to ensure that all aspects and perspectives are considered. The size of the team should reflect the scope and complexity of the SFA assignment.

- **Build hypothesis:** this is a useful method of building likely scenarios, which can help the study team draw early conclusions within the analysis period. These scenarios can be built from discussing the forthcoming assignment with key roles, e.g. senior management and users, or by using the planning session to brainstorm the list from the assembled team. The completed hypotheses list should be documented and input to the analysis period to provide some early focus on the data and Management Information System (MIS) that match the individual scenarios. It should be noted that this approach also eliminates perceived issues, i.e. no data or MIS substantiates what is perceived to be a service issue.
- **Analyse data:** the number of individuals that form the SFA team dictates how to allocate specific analysis responsibilities. During this analysis period the hypotheses list should be used to help draw some early conclusions.
- **Interview key personnel:** it is essential that key business representatives and users are interviewed to ensure the business and user perspectives are captured. It is surprising how this dialogue can identify quick win opportunities, as often what the business views as a big issue can be addressed by a simple IT solution. Therefore these interviews should be initiated as soon as possible within the SFA assignment. The study team should also seek input from key individuals within the IT service provider organization to identify additional problem areas and possible solutions that can be fed back to the study team. The dialogue also helps capture those issues that are not easily visible from the assembled data and MIS reports.
- **Findings and conclusions:** after analysis of the data and MIS provided, interviews and continual revision of the hypothesis list, the study team should be in a position to start documenting initial findings and conclusions. It is recommended that the team meet immediately after the analysis period to share their individual findings and then take an aggregate view to form the draft findings and conclusions. It is important

that all findings can be evidenced by facts gathered during the analysis. During this phase of the assignment, it may be necessary to validate finding(s) by additional analysis to ensure the SFA team can back up all findings with clear documented evidence.

- **Recommendations:** after all findings and conclusions have been validated, the SFA team should be in a position to formulate recommendations. In many cases, the recommendations to support a particular finding are straightforward and obvious. However, the benefit of bringing a cross-functional team together for the SFA assignment is to create an environment for innovative lateral-thinking approaches. The SFA assignment leader should facilitate this session with the aim of identifying recommendations that are practical and sustainable once implemented.
- **Report:** the final report should be issued to the sponsor with a management summary. Reporting styles are normally determined by the individual organizations. It is important that the report clearly shows where loss of availability is being incurred and how the recommendations address this. If the report contains many recommendations, an attempt should be made to quantify the availability benefit of each recommendation, together with the estimated effort to implement. This enables informed choices to be made on how to take the recommendations forward and how these should be prioritized and resourced.
- **Validation:** it is recommended that for each SFA, key measures that reflect the business and user perspectives prior to the assignment are captured and recorded as the 'before' view. As SFA recommendations are progressed, the positive impacts on availability should be captured to provide the 'after' view for comparative purposes. Where anticipated benefits have not been delivered, this should be investigated and remedial action taken. Having invested time and effort in completing the SFA assignment, it is important that the recommendations, once agreed by the sponsor, are then taken forward for implementation. The best mechanism for achieving this is by incorporating the recommendations as activities to be completed within the Availability Plan or the overall SIP. The success of the SFA assignment as a whole should be monitored and measured to ensure its continued effectiveness.

Hints and tips

Consider categorizing the recommendations under the following headings:

DETECTION: Recommendations that, if implemented, will provide enhanced reporting of key indicators to ensure underlying IT service issues are detected early to enable a proactive response.

REDUCTION: Recommendations that, if implemented, will reduce or minimize the user impact from IT service interruption, e.g. recovery and/or restoration can be enhanced to reduce impact duration.

AVOIDANCE: Recommendations that, if implemented, will eliminate this particular cause of IT service interruption.

Designing for availability

The level of availability required by the business influences the overall cost of the IT service provided. In general, the higher the level of availability required by the business, the higher the cost. These costs are not just the procurement of the base IT technology and services required to underpin the IT infrastructure. Additional costs are incurred in providing the appropriate Service Management processes, systems management tools and high-availability solutions required to meet the more stringent availability requirements. The greatest level of availability should be included in the design of those services supporting the most critical of the VBFs.

When considering how the availability requirements of the business are to be met, it is important to ensure that the level of availability to be provided for an IT service is at the level actually required, and is affordable and cost-justifiable to the business. Figure 4.17 indicates the products and processes required to provide varying levels of availability and the cost implications.

Base product and components

The procurement or development of the base products, technology and components should be based on their capability to meet stringent availability and reliability requirements. These should be considered as the cornerstone of the availability design. The additional investment required to achieve even higher levels of availability will be wasted and availability levels not met if these base products and components are unreliable and prone to failure.

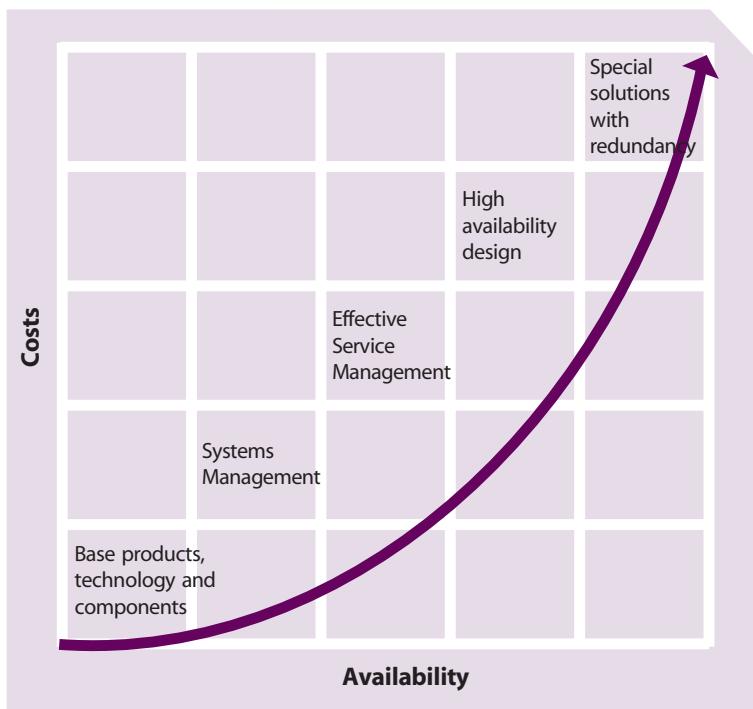


Figure 4.17 Relationship between levels of availability and overall costs

Systems management

Systems management should provide the monitoring, diagnostic and automated error recovery to enable fast detection and speedy resolution of potential and actual IT failure.

Service Management processes

Effective Service Management processes contribute to higher levels of availability. Processes such as Availability Management, Incident Management, Problem Management, Change Management, Configuration Management, etc. play a crucial role in the overall management of the IT service.

High-availability design

The design for high availability needs to consider the elimination of SPoFs and/or the provision of alternative components to provide minimal disruption to the business operation should an IT component failure occur. The design also needs to eliminate or minimize the effects of planned downtime to the business operation normally required to accommodate maintenance activity, the implementation of changes to the IT infrastructure or business application. Recovery criteria should define rapid recovery and IT service reinstatement as a key objective within the designing for recovery phase of design.

Special solutions with full redundancy

To approach continuous availability in the range of 100% requires expensive solutions that incorporate full mirroring or redundancy. Redundancy is the technique of improving availability by using duplicate components. For stringent availability requirements to be met, these need to be working autonomously in parallel. These solutions are not just restricted to the IT components, but also to the IT environments, i.e. data centres, power supplies, air conditioning and telecommunications.

Where new IT services are being developed, it is essential that Availability Management takes an early and participating design role in determining the availability requirements. This enables Availability Management to influence positively the IT infrastructure design to ensure that it can deliver the level of availability required. The importance of this participation early in the design of the IT infrastructure cannot be underestimated. There needs to be a dialogue between IT and the business to determine the balance between the business perception of the cost of unavailability and the exponential cost of delivering higher levels of availability.

As illustrated in Figure 4.17, there is a significant increase in costs when the business requirement is higher than the

optimum level of availability that the IT infrastructure can deliver. These increased costs are driven by major redesign of the technology and the changing of requirements for the IT support organization.

It is important that the level of availability designed into the service is appropriate to the business needs, the criticality of the business processes being supported and the available budget. The business should be consulted early in the Service Design lifecycle so that the business availability needs of a new or enhanced IT service can be costed and agreed. This is particularly important where stringent availability requirements may require additional investment in Service Management processes, IT service and System Management tools, high-availability design and special solutions with full redundancy.

It is likely that the business need for IT availability cannot be expressed in technical terms. Availability Management therefore provides an important role in being able to translate the business and user requirements into quantifiable availability targets and conditions. This is an important input into the IT Service Design and provides the basis for assessing the capability of the IT design and IT support organization in meeting the availability requirements of the business.

The business requirements for IT availability should contain at least:

- A definition of the VBFs supported by the IT service
- A definition of IT service downtime, i.e. the conditions under which the business considers the IT service to be unavailable
- The business impact caused by loss of service, together with the associated risk
- Quantitative availability requirements, i.e. the extent to which the business tolerates IT service downtime or degraded service
- The required service hours, i.e. when the service is to be provided
- An assessment of the relative importance of different working periods
- Specific security requirements
- The service backup and recovery capability.

Once the IT technology design and IT support organization are determined, the service provider organization is then in a position to confirm if the availability requirements can be met. Where shortfalls are identified, dialogue with the business is required to present the cost options that exist to enhance the proposed design to meet the availability requirements. This enables the business to reassess if lower or higher

levels of availability are required, and to understand the appropriate impact and costs associated with their decision.

Determining the availability requirements is likely to be an iterative process, particularly where there is a need to balance the business availability requirement against the associated costs. The necessary steps are:

- Determine the business impact caused by loss of service
- From the business requirements, specify the availability, reliability and maintainability requirements for the IT service and components supported by the IT support organization
- For IT services and components provided externally, identify the serviceability requirements
- Estimate the costs involved in meeting the availability, reliability, maintainability and serviceability requirements
- Determine, with the business, if the costs identified in meeting the availability requirements are justified
- Determine, from the business, the costs likely to be incurred from loss or degradation of service
- Where these are seen as cost-justified, define the availability, reliability, maintainability and serviceability requirements in agreements and negotiate into contracts.

Hints and tips

If costs are seen as prohibitive, either:

- Reassess the IT infrastructure design and provide options for reducing costs and assess the consequences on availability; or
- Reassess the business use and reliance on the IT service and renegotiate the availability targets within the SLA.

The SLM process is normally responsible for communicating with the business on how its availability requirements for IT services are to be met and negotiating the SLR/SLA for the IT Service Design process. Availability Management therefore provides important support and input to the both SLM and design processes during this period. While higher levels of availability can often be provided by investment in tools and technology, there is no justification for providing a higher level of availability than that needed and afforded by the business. The reality is that satisfying availability requirements is always a balance between cost and quality. This is where Availability Management can play a key role in optimizing

availability of the IT Service Design to meet increasing availability demands while deferring an increase in costs.

Designing service for availability is a key activity driven by Availability Management. This ensures that the required level of availability for an IT service can be met. Availability Management needs to ensure that the design activity for availability looks at the task from two related, but distinct, perspectives:

- **Designing for availability:** this activity relates to the technical design of the IT service and the alignment of the internal and external suppliers required to meet the availability requirements of the business. It needs to cover all aspects of technology, including infrastructure, environment, data and applications.
- **Designing for recovery:** this activity relates to the design points required to ensure that in the event of an IT service failure, the service and its supporting components can be reinstated to enable normal business operations to resume as quickly as is possible. This again needs to cover all aspects of technology.

Additionally, the ability to recover quickly may be a crucial factor. In simple terms, it may not be possible or cost-justified to build a design that is highly resilient to failure(s). The ability to meet the availability requirements within the cost parameters may rely on the ability consistently to recover in a timely and effective manner. All aspects of availability should be considered in the Service Design process and should consider all stages within the Service Lifecycle.

The contribution of Availability Management within the design activities is to provide:

- The specification of the availability requirements for all components of the service
- The requirements for availability measurement points (instrumentation)
- The requirements for new/enhanced systems and Service Management
- Assistance with the IT infrastructure design
- The specification of the reliability, maintainability and serviceability requirements for components supplied by internal and external suppliers
- Validation of the final design to meet the minimum levels of availability required by the business for the IT service.

If the availability requirements cannot be met, the next task is to re-evaluate the Service Design and identify cost-justified design changes. Improvements in design to meet the availability requirements can be achieved by reviewing

the capability of the technology to be deployed in the proposed IT design. For example:

- The exploitation of fault-tolerant technology to mask the impact of planned or unplanned component downtime
- Duplexing, or the provision of alternative IT infrastructure components to allow one component to take over the work of another component
- Improving component reliability by enhancing testing regimes
- Improved software design and development
- Improved processes and procedures
- Systems management enhancements/exploitation
- Improved externally supplied services, contracts or agreements
- Developing the capability of the people with more training.

Hints and tips

Consider documenting the availability design requirements and considerations for new IT services and making them available to the design and implementation functions. Longer term seek to mandate these requirements and integrate within the appropriate governance mechanisms that cover the introduction of new IT services.

Part of the activity of designing for availability must ensure that all business, data and information security requirements are incorporated within the Service Design. The overall aim of IT security is ‘balanced security in depth’, with justifiable controls implemented to ensure that the Information Security Policy is enforced and that continued IT services within secure parameters (i.e. confidentiality, integrity and availability) continue to operate. During the gathering of availability requirements for new IT services, it is important that requirements that cover IT security are defined. These requirements need to be applied within the design phase for the supporting technology. For many organizations, the approach taken to IT security is covered by an Information Security Policy owned and maintained by Information Security Management. In the execution of the security policy, Availability Management plays an important role in its operation for new IT services.

Where the business operation has a high dependency on IT service availability, and the cost of failure or loss of business reputation is considered not acceptable, the business may define stringent availability requirements. These factors may be sufficient for the business to justify the additional costs required to meet these more demanding levels of availability. Achieving agreed levels of availability begins with the design, procurement and/or development of good-quality products and components. However, these in isolation are unlikely to deliver the sustained levels of availability required. To achieve a consistent and sustained level of availability requires investment in and deployment of effective Service Management processes, systems management tools, high-availability design and ultimately special solutions with full mirroring or redundancy.

Designing for availability is a key activity, driven by Availability Management, which ensures that the stated availability requirements for an IT service can be met. However, Availability Management should also ensure that within this design activity there is focus on the design elements required to ensure that when IT services fail, the service can be reinstated to enable normal business operations to resume as quickly as is possible. ‘Designing for recovery’ may at first sound negative. Clearly good availability design is about avoiding failures and delivering, where possible, a fault-tolerant IT infrastructure. However, with this focus is too much reliance placed on technology, and has as much emphasis been placed on the fault tolerance aspects of the IT infrastructure? The reality is that failures will occur. The way the IT organization manages failure situations can have a positive effect on the perception of the business, customers and users of the IT services.

Key message

Every failure is an important ‘moment of truth’ – an opportunity to make or break your reputation with the business.

By providing focus on the ‘designing for recovery’ aspects of the overall availability, design can ensure that every failure is an opportunity to maintain and even enhance business and user satisfaction. To provide an effective ‘design for recovery’, it is important to recognize that both the business and the IT organization have needs that must be satisfied to enable an effective recovery from IT failure.

These are informational needs that the business requires to help them manage the impact of failure on their business and set expectation within the business, user community and their business customers. These are the skills, knowledge, processes, procedures and tools required to enable the technical recovery to be completed in an optimal time.

Hints and tips

Consider documenting the recovery design requirements and considerations for new IT services and make them available to the areas responsible for design and implementation. In the longer term, seek to mandate these requirements and integrate them within the appropriate governance mechanisms that cover the introduction of new IT services.

A key aim is to prevent minor incidents from becoming major incidents by ensuring the right people are involved early enough to avoid mistakes being made and to ensure the appropriate business and technical recovery procedures are invoked at the earliest opportunity. The instigation of these activities is the responsibility of the Incident Management process and a role of the Service Desk. To ensure business needs are met during major IT service failures, and to ensure the most optimal recovery, the Incident Management process and Service Desk need to have defined and to execute effective procedures for assessing and managing all incidents.

Key message

The above are not the responsibilities of Availability Management. However, the effectiveness of the Incident Management process and Service Desk can strongly influence the overall recovery period. The use of Availability Management methods and techniques to further optimize IT recovery may be the stimulus for subsequent continual improvement activities to the Incident Management process and the Service Desk.

In order to remain effective, the maintainability of IT services and components should be monitored, and their impact on the ‘expanded incident lifecycle’ understood, managed and improved.

Component Failure Impact Analysis

Component Failure Impact Analysis (CFIA) can be used to predict and evaluate the impact on IT service arising from component failures within the technology. The output from a CFIA can be used to identify where additional resilience should be considered to prevent or minimize the impact of component failure to the business operation

and users. This is particularly important during the Service Design stage, where it is necessary to predict and evaluate the impact on IT service availability arising from component failures within the proposed IT Service Design. However, the technique can also be applied to existing services and infrastructure.

CFIA is a relatively simple technique that can be used to provide this information. IBM devised CFIA in the early 1970s, with its origins based on hardware design and configuration. However, it is recommended that CFIA be used in a much wider context to reflect the full scope of the IT infrastructure, i.e. hardware, network, software, applications, data centres and support staff. Additionally the technique can also be applied to identify impact and dependencies on IT support organization skills and competencies amongst staff supporting the new IT service. This activity is often completed in conjunction with ITSCM and possibly Capacity Management.

The output from a CFIA provides vital information to ensure that the availability and recovery design criteria for the new IT service is influenced to prevent or minimize the impact of failure to the business operation and users. CFIA achieves this by providing and indicating:

- SPoFs that can impact availability
- The impact of component failure on the business operation and users
- Component and people dependencies
- Component recovery timings
- The need to identify and document recovery options
- The need to identify and implement risk reduction measures.

The above can also provide the stimulus for input to ITSCM to consider the balance between recovery options and risk reduction measures, i.e. where the potential business impact is high there is a need to concentrate on high-availability risk reduction measures, i.e. increased resilience or standby systems.

Having determined the IT infrastructure configuration to be assessed, the first step is to create a grid with CIs on one axis and the IT services that have a dependency on the CI on the other, as illustrated in Figure 4.18. This information should be available from the CMS, or alternatively it can be built using documented configuration charts and SLAs.

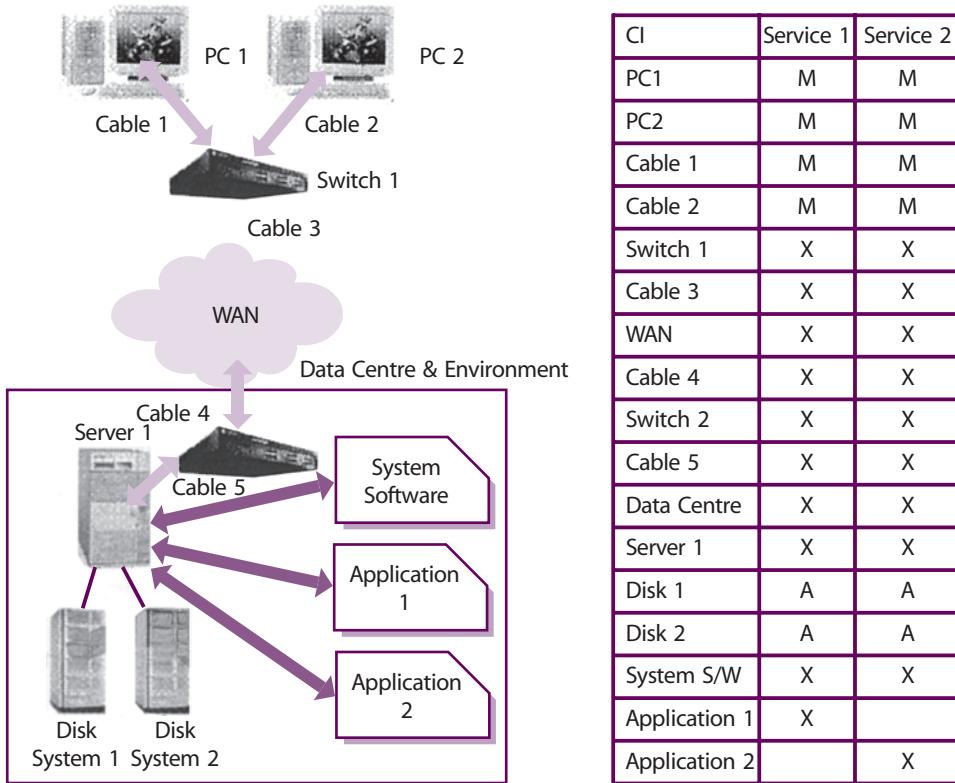


Figure 4.18 Component Failure Impact Analysis

The next step is to perform the CFIA and populate the grid as follows:

- Leave a blank when a failure of the CI does not impact the service in any way
- Insert an 'X' when the failure of the CI causes the IT service to be inoperative
- Insert an 'A' when there is an alternative CI to provide the service
- Insert an 'M' when there is an alternative CI, but the service requires manual intervention to be recovered.

Having built the grid, CIs that have a large number of Xs are critical to many services and can result in high impact should the CI fail. Equally, IT services having high counts of Xs are complex and are vulnerable to failure. This basic approach to CFIA can provide valuable information in quickly identifying SPoFs, IT services at risk from CI failure and what alternatives are available should CIs fail. It should also be used to assess the existence and validity of recovery procedures for the selected CIs. The above example assumes common infrastructure supporting multiple IT services. The same approach can be used for a single IT service by mapping the component CIs against the VBFs and users supported by each component, thus understanding the impact of a component failure on the business and user. The approach can also be further

refined and developed to include and develop 'component availability weighting' factors that can be used to assess and calculate the overall effect of the component failure on the total service availability.

To undertake an advanced CFIA requires the CFIA matrix to be expanded to provide additional fields required for the more detailed analysis. This could include fields such as:

- **Component availability weighting:** a weighting factor appropriate to the impact of failure of the component on the total service availability. For example, if the failure of a switch can cause 2,000 users to lose service out of a total service user base of 10,000, then the weighting factor should be 0.2, or 20%
- **Probability of failure:** this can be based on the reliability of the component as measured by the Mean Time Between Failures (MTBF) information if available or on the current trends. This can be expressed as a low/medium/high indicator or as a numeric representation
- **Recovery time:** this is the estimated recovery time to recover the CI. This can be based on recent recovery timings, recovery information from disaster recovery testing or a scheduled test recovery

- **Recovery procedures:** this is to verify that up-to-date recovery procedures are available for the CI
- **Device independence:** where software CIs have duplex files to provide resilience, this is to ensure that file placements have been verified as being on separate hardware disk configurations. This also applies to power supplies – it should be verified that alternate power supplies are connected correctly
- **Dependency:** this is to show any dependencies between CIs. If one CI failed, there could be an impact on other CIs – for example, if the security CI failed, the operating system might prevent tape processing.

Single Point of Failure analysis

A Single Point of Failure (SPoF) is any component within the IT infrastructure that has no backup or fail-over capability, and has the potential to cause disruption to the business, customers or users when it fails. It is important that no unrecognized SPoFs exist within the IT infrastructure design or the actual technology, and that they are avoided wherever possible.

The use of SPoF analysis or CFIA as techniques to identify SPoFs is recommended. SPoF and CFIA analysis exercises should be conducted on a regular basis, and wherever SPoFs are identified, CFIA can be used to identify the

potential business, customer or user impact and help determine what alternatives can or should be considered to cater for this weakness in the design or the actual infrastructure. Countermeasures should then be implemented wherever they are cost-justifiable. The impact and disruption caused by the potential failure of the SPoF should be used to cost-justify its implementation.

Fault Tree Analysis

Fault Tree Analysis (FTA) is a technique that can be used to determine the chain of events that causes a disruption to IT services. FTA, in conjunction with calculation methods, can offer detailed models of availability. This can be used to assess the availability improvement that can be achieved by individual technology component design options. Using FTA:

- Information can be provided that can be used for availability calculations
- Operations can be performed on the resulting fault tree; these operations correspond with design options
- The desired level of detail in the analysis can be chosen.

FTA makes a representation of a chain of events using Boolean notation. Figure 4.19 gives an example of a fault tree.

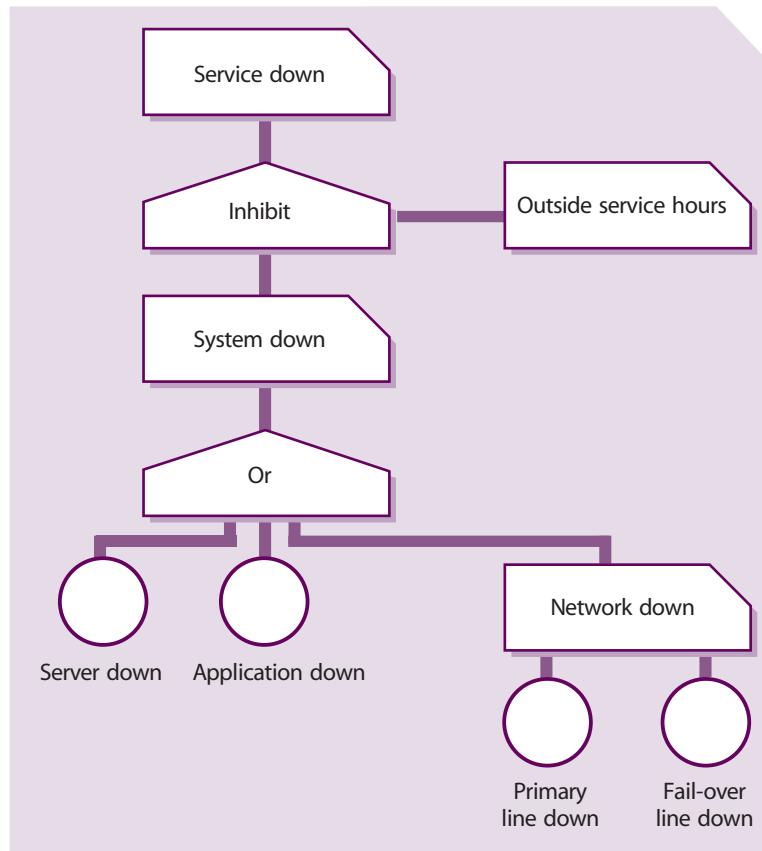


Figure 4.19 Example Fault Tree Analysis

Essentially FTA distinguishes the following events:

- **Basic events** – terminal points for the fault tree, e.g. power failure, operator error. Basic events are not investigated in great depth. If basic events are investigated in further depth, they automatically become resulting events.
- **Resulting events** – intermediate nodes in the fault tree, resulting from a combination of events. The highest point in the fault tree is usually a failure of the IT service.
- **Conditional events** – events that only occur under certain conditions, e.g. failure of the air-conditioning equipment only affects the IT service if equipment temperature exceeds the serviceable values.
- **Trigger events** – events that trigger other events, e.g. power failure detection equipment can trigger automatic shutdown of IT services.

These events can be combined using logic operators, i.e.:

- **AND-gate** – the resulting event only occurs when all input events occur simultaneously
- **OR-gate** – the resulting event occurs when one or more of the input events occurs
- **Exclusive OR-gate** – the resulting event occurs when one and only one of the input events occurs
- **Inhibit gate** – the resulting event only occurs when the input condition is not met.

This is the basic FTA technique. This technique can also be refined, but complex FTA and the mathematical evaluation of fault trees are beyond the scope of this publication.

Modelling

To assess if new components within a design can match the stated requirements, it is important that the testing regime instigated ensures that the availability expected can be delivered. Simulation, modelling or load testing tools to generate the expected user demand for the new IT service should be seriously considered to ensure components continue to operate under anticipated volume and stress conditions.

Modelling tools are also required to forecast availability and to assess the impact of changes to the IT infrastructure. Inputs to the modelling process include

descriptive data of the component reliability, maintainability and serviceability. A spreadsheet package to perform calculations is usually sufficient. If more detailed and accurate data is required, a more complex modelling tool may need to be developed or acquired. The lack of readily available availability modelling tools in the marketplace may require such a tool to be developed and maintained ‘in-house’, but this is a very expensive and time-consuming activity that should only be considered where the investment can be justified. Unless there is a clearly perceived benefit from such a development and the ongoing maintenance costs, the use of existing tools and spreadsheets should be sufficient. However, some System Management tools do provide modelling capability and can provide useful information on trending and forecasting availability needs.

Risk Analysis and Management

To assess the vulnerability of failure within the configuration and capability of the IT service and support organization it is recommended that existing or proposed IT infrastructure, service configurations, Service Design and supporting organization (internal and external suppliers) are subject to formal Risk Analysis and Management exercises. Risk Analysis and Management is a technique that can be used to identify and quantify risks and justifiable countermeasures that can be implemented to protect the availability of IT systems. The identification of risks and the provision of justified countermeasures to reduce or eliminate the threats posed by such risks can play an important role in achieving the required levels of availability for a new or enhanced IT service. Risk Analysis should be undertaken during the design phase for the IT technology and service to identify:

- Risks that may incur unavailability for IT components within the technology and Service Design
- Risks that may incur confidentiality and/or integrity exposures within the IT technology and Service Design.

Most risk assessment and management methodologies involve the use of a formal approach to the assessment of risk and the subsequent mitigation of risk with the implementation of subsequent cost-justifiable countermeasures, as illustrated in Figure 4.20.

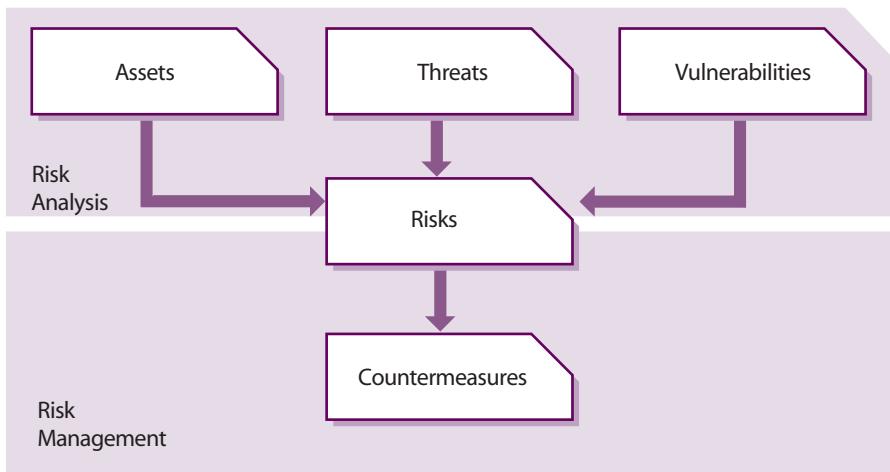


Figure 4.20 Risk Analysis and Management

Risk Analysis involves the identification and assessment of the level (measure) of the risks calculated from the assessed values of assets and the assessed levels of threats to, and vulnerabilities of, those assets. Risk is also determined to a certain extent by its acceptance. Some organizations and businesses may be more willing to accept risk whereas others cannot.

Risk management involves the identification, selection and adoption of countermeasures justified by the identified risks to assets in terms of their potential impact on services if failure occurs, and the reduction of those risks to an acceptable level. Risk management is an activity that is associated with many other activities, especially ITSCM, Security Management and Service Transition. All of these risk assessment exercises should be coordinated rather than being separate activities.

This approach, when applied via a formal method, ensures coverage is complete, together with sufficient confidence that:

- All possible risks and countermeasures have been identified
- All vulnerabilities have been identified and their levels accurately assessed
- All threats have been identified and their levels accurately assessed
- All results are consistent across the broad spectrum of the technology reviewed
- All expenditure on selected countermeasures can be justified.

Formal Risk Analysis and Management methods are now an important element in the overall design and provision of IT services. The assessment of risk is often based on the probability and potential impact of an event occurring. Counter-measures are implemented wherever they are cost-justifiable, to reduce the impact of an event, or the probability of an event occurring, or both.

Management of Risk (M_o_R) provides an alternative generic framework for the management of risk across all parts of an organization – strategic, programme, project and operational. It incorporates all the activities required to identify and control the exposure to any type of risk, positive or negative, that may have an impact on the achievement of your organization's business objectives.

M_o_R provides a framework that is tried, tested and effective to help you eliminate – or manage – the risks involved in reaching your goals. M_o_R adopts a systematic application of principles, approach and processes to the task of identifying, assessing and then planning and implementing risk responses. Guidance stresses a collaborative approach and focuses on the following key elements:

- Developing a framework that is transparent, repeatable and adaptable
- Clearly communicating the policy and its benefits to all staff
- Nominating key individuals in senior management to 'own' risk management initiatives and ensure they move forwards
- Ensuring the culture engages with and supports properly considered risk, including innovation
- Embedding risk management systems in management and applying them consistently
- Ensuring that risk management supports objectives – rather than vice versa
- Explicitly assessing the risks involved in working with other organizations
- Adopting a no-blame approach to monitoring and reviewing risk assessment activity.

Availability testing schedule

A key deliverable from the Availability Management process is the ‘availability testing schedule’. This is a schedule for the regular testing of all availability mechanisms. Some availability mechanisms, such as ‘load balancing’, ‘mirroring’ and ‘grid computing’, are used in the provision of normal service on a day-by-day basis; others are used on a fail-over or manual reconfiguration basis. It is essential, therefore, that all availability mechanisms are tested in a regular and scheduled manner to ensure that when they are actually needed for real they work. This schedule needs to be maintained and widely circulated so that all areas are aware of its content and so that all other proposed activities can be synchronized with its content, such as:

- The change schedule
- Release plans and the release schedule
- All transition plans, projects and programmes
- Planned and preventative maintenance schedules
- The schedule for testing IT service continuity and recovery plans
- Business plans and schedules.

Planned and preventative maintenance

All IT components should be subject to a planned maintenance strategy. The frequency and levels of maintenance required varies from component to component, taking into account the technologies involved, criticality and the potential business benefits that may be introduced. Planned maintenance activities enable the IT support organization to provide:

- Preventative maintenance to avoid failures
- Planned software or hardware upgrades to provide new functionality or additional capacity
- Business requested changes to the business applications
- Implementation of new technology and functionality for exploitation by the business.

The requirement for planned downtime clearly influences the level of availability that can be delivered for an IT service, particularly those that have stringent availability requirements. In determining the availability requirements for a new or enhanced IT service, the amount of downtime and the resultant loss of income required for planned maintenance may not be acceptable to the business. This is becoming a growing issue in the area of 24 x 7 service operation. In these instances, it is essential that continuous operation is a core design feature to enable maintenance activity to be performed without impacting the availability of IT services.

Where the required service hours for IT services are less than 24 hours per day and/or seven days per week, it is likely that the majority of planned maintenance can be accommodated without impacting IT service availability. However, where the business needs IT services available on a 24-hour and seven-day basis, Availability Management needs to determine the most effective approach in balancing the requirements for planned maintenance against the loss of service to the business. Unless mechanisms exist to allow continuous operation, scheduled downtime for planned maintenance is essential if high levels of availability are to be achieved and sustained. For all IT services, there should logically be a ‘low-impact’ period for the implementation of maintenance. Once the requirements for managing scheduled maintenance have been defined and agreed, these should be documented as a minimum in:

- SLAs
- OLAs
- Underpinning contracts
- Change Management schedules
- Release and Deployment Management schedules.

Hints and tips

Availability Management should ensure that building in preventative maintenance is one of the prime design considerations for a ‘24 x 7’ IT service.

The most appropriate time to schedule planned downtime is clearly when the impact on the business and its customers is least. This information should be provided initially by the business when determining the availability requirements. For an existing IT service, or once the new service has been established, monitoring of business and customer transactions helps establish the hours when IT service usage is at its lowest. This should determine the most appropriate time for the component(s) to be removed for planned maintenance activity.

To accommodate the individual component requirements for planned downtime while balancing the IT service availability requirements of the business provides an opportunity to consider scheduling planned maintenance to multiple components concurrently. The benefit of this approach is that the number of service disruptions required to meet the maintenance requirements is reduced. While this approach has benefits, there are potential risks that need to be assessed. For example:

- The capability of the IT support organization to coordinate the concurrent implementation of a high number of changes

- The ability to perform effective problem determination where the IT service is impacted after the completion of multiple changes
- The impact of change dependency across multiple components where back-out of a failed change requires multiple changes to be removed.

The effective management of planned downtime is an important contribution in meeting the required levels of availability for an IT service. Where planned downtime is required on a cyclic basis to an IT component(s), the time that the component is unavailable to enable the planned maintenance activity to be undertaken should be defined and agreed with the internal or external supplier. This becomes a stated objective that can be formalized, measured and reported. All planned maintenance should be scheduled, managed and controlled to ensure that the individual objectives and time slots are not exceeded and to ensure that activities are coordinated with all other schedules of activity to minimize clashes and conflict (e.g. change and release schedules, testing schedules.) In addition they provide an early warning during the maintenance activity of the time allocated to the planned outage duration being breached. This can enable an early decision to be made on whether the activity is allowed to complete with the potential to further impact service or to abort the activity and instigate the back-out plan. Planned downtime and performance against the stated objectives for each component should be recorded and used in service reporting.

Production of the Projected Service Outage (PSO) document

Availability Management should produce and maintain the PSO document. This document consists of any variations from the service availability agreed within SLAs. This should be produced based on input from:

- The change schedule
- The release schedules
- Planned and preventative maintenance schedules
- Availability testing schedules
- ITSCM and Business Continuity Management testing schedules.

The PSO contains details of all scheduled and planned service downtime within the agreed service hours for all services. These documents should be agreed with all the appropriate areas and representatives of both the business and IT. Once the PSO has been agreed, the Service Desk should ensure that it is communicated to all relevant parties so that everyone is made aware of any additional, planned service downtime.

Continual review and improvement

Changing business needs and customer demand may require the levels of availability provided for an IT service to be reviewed. Such reviews should form part of the regular service reviews with the business undertaken by SLM. Other input should also be considered on a regular basis from ITSCM, particularly from the updated Business Impact Analysis and Risk Analysis exercises. The criticality of services will often change and it is important that the design and the technology supporting such services is regularly reviewed and improved by Availability Management to ensure that the change of importance in the service is reflected within a revised design and supporting technology. Where the required levels of availability are already being delivered, it may take considerable effort and incur significant cost to achieve a small incremental improvement within the level of availability.

A key activity for Availability Management is continually to look at opportunities to optimize the availability of the IT infrastructure in conjunction with Continual Service Improvement activities. The benefits of this regular review approach are that, sometimes, enhanced levels of availability may be achievable, but with much lower costs. The optimization approach is a sensible first step to delivering better value for money. A number of Availability Management techniques can be applied to identify optimization opportunities. It is recommended that the scope should not be restricted to the technology, but also include a review of both the business process and other end-to-end business-owned responsibilities. To help achieve these aims, Availability Management needs to be recognized as a leading influence over the IT service provider organization to ensure continued focus on availability and stability of the technology.

Availability Management can provide the IT support organization with a real business and user perspective on how deficiencies within the technology and the underpinning process and procedure impact on the business operation and ultimately their customers. The use of business-driven metrics can demonstrate this impact in real terms and, importantly, also help quantify the benefits of improvement opportunities. Availability Management can play an important role in helping the IT service provider organization recognize where it can add value by exploiting its technical skills and competencies in an availability context. The continual improvement technique can be used by Availability Management to harness this technical capability. This can be used with either small groups of technical staff or a wider group within a workshop or SFA environment.

The impetus to improve availability comes from one or more of the following:

- The inability for existing or new IT services to meet SLA targets on a consistent basis
- Period(s) of IT service instability resulting in unacceptable levels of availability
- Availability measurement trends indicating a gradual deterioration in availability
- Unacceptable IT service recovery and restoration times
- Requests from the business to increase the level of availability provided
- Increasing impact on the business and its customers of IT service failures as a result of growth and/or increased business priorities or functionality
- A request from SLM to improve availability as part of an overall SIP
- Availability Management monitoring and trend analysis.

Availability Management should take a proactive role in identifying and progressing cost-justified availability improvement opportunities within the Availability Plan. The ability to do this places reliance on having appropriate and meaningful availability measurement and reporting. To ensure availability improvements deliver benefits to the business and users, it is important that measurement and reporting reflects not just IT component availability but also availability from a business operation and user perspective.

Where the business has a requirement to improve availability, the process and techniques to reassess the technology and IT service provider organization capability to meet these enhanced requirements should be followed. An output of this activity is enhanced availability and recovery design criteria. To satisfy the business requirement for increased levels of availability may require additional financial investment to enhance the underpinning technology and/or extend the services provided by the IT service provider organization. It is important that any additional investment to improve the levels of availability delivered can be cost-justified. Determining the cost of unavailability as a result of IT failure(s) can help support any financial investment decision in improving availability.

4.4.6 Triggers, inputs, outputs and interfaces

Many events may trigger Availability Management activity. These include:

- New or changed business needs or new or changed services

- New or changed targets within agreements, such as SLRs, SLAs, OLAs or contracts
- Service or component breaches, availability events and alerts, including threshold events, exception reports
- Periodic activities such as reviewing, revising or reporting
- Review of Availability Management forecasts, reports and plans
- Review and revision of business and IT plans and strategies
- Review and revision of designs and strategies
- Recognition or notification of a change of risk or impact of a business process or VBF, an IT service or component
- Request from SLM for assistance with availability targets and explanation of achievements.

The key interfaces that Availability Management has with other processes are:

- **Incident and Problem Management:** in providing assistance with the resolution and subsequent justification and correction of availability incidents and problems
- **Capacity Management:** with the provision of resilience and spare capacity
- **IT Service Continuity Management:** with the assessment of business impact and risk and the provision of resilience, fail-over and recovery mechanisms
- **Service Level Management:** assistance with the determining of availability targets and the investigation and resolution of service and component breaches.

4.4.6.1 Inputs

A number of sources of information are relevant to the Availability Management process. Some of these are as follows:

- **Business information:** from the organization's business strategy, plans and financial plans, and information on their current and future requirements, including the availability requirements for new or enhanced IT services
- **Business impact information:** from BIAs and assessment of VBFs underpinned by IT services
- **Previous Risk Analysis** and Assessment reports and a risk register
- **Service information:** from the Service Portfolio and the Service Catalogue,
- **Service information:** from the SLM process, with

details of the services from the Service Portfolio and the Service Catalogue, service level targets within SLAs and SLRs, and possibly from the monitoring of SLAs, service reviews and breaches of the SLAs

- **Financial information:** from Financial Management, the cost of service provision, the cost of resources and components
- **Change and release information:** from the Change Management process with a Change Schedule, the Release Schedule from Release Management and a need to assess all changes for their impact on service availability
- **Configuration Management:** containing information on the relationships between the business, the services, the supporting services and the technology
- **Service targets:** from SLAs, SLRs, OLAs and contracts
- **Component information:** on the availability, reliability and maintainability requirements for the technology components that underpin IT service(s)
- **Technology information:** from the CMS on the topology and the relationships between the components and the assessment of the capabilities of new technology
- **Past performance:** from previous measurements, achievements and reports and the Availability Management Information System (AMIS)
- **Unavailability and failure information:** from incidents and problems.

4.4.6.2 Outputs

The outputs produced by Availability Management should include:

- The Availability Management Information System (AMIS)
- The Availability Plan for the proactive improvement of IT services and technology
- Availability and recovery design criteria and proposed service targets for new or changed services
- Service availability, reliability and maintainability reports of achievements against targets, including input for all service reports
- Component availability, reliability and maintainability reports of achievements against targets
- Revised risk analysis reviews and reports and an updated risk register
- Monitoring, management and reporting requirements for IT services and components to ensure that deviations in availability, reliability and maintainability are detected, actioned, recorded and reported

- An Availability Management test schedule for testing all availability, resilience and recovery mechanisms
- The planned and preventative maintenance schedules
- The Projected Service Outage (PSO) in conjunction with Change and Release Management
- Details of the proactive availability techniques and measures that will be deployed to provide additional resilience to prevent or minimize the impact of component failures on the IT service availability
- Improvement actions for inclusion within the SIP.

4.4.7 Key Performance Indicators

Many KPIs can be used to measure the effectiveness and efficiency of Availability Management, including the following examples:

Manage availability and reliability of IT service:

- Percentage reduction in the unavailability of services and components
- Percentage increase in the reliability of services and components
- Effective review and follow-up of all SLA, OLA and underpinning contract breaches
- Percentage improvement in overall end-to-end availability of service
- Percentage reduction in the number and impact of service breaks
- Improvement in the MTBF (Mean Time Between Failures)
- Improvement in the MTBSI (Mean Time Between Systems Incidents)
- Reduction in the MTRS (Mean Time to Restore Service).

Satisfy business needs for access to IT services:

- Percentage reduction in the unavailability of services
- Percentage reduction of the cost of business overtime due to unavailable IT
- Percentage reduction in critical time failures, e.g. specific business peak and priority availability needs are planned for
- Percentage improvement in business and users satisfied with service (by CSS results).

Availability of IT infrastructure achieved at optimum costs:

- Percentage reduction in the cost of unavailability
- Percentage improvement in the Service Delivery costs
- Timely completion of regular Risk Analysis and system review
- Timely completion of regular cost-benefit analysis

- established for infrastructure Component Failure Impact Analysis (CFIA)
- Percentage reduction in failures of third-party performance on MTRS/MTBF against contract targets
- Reduced time taken to complete (or update) a Risk Analysis
- Reduced time taken to review system resilience
- Reduced time taken to complete an Availability Plan
- Timely production of management reports
- Percentage reduction in the incidence of operational reviews uncovering security and reliability exposures in application designs.

4.4.8 Information Management

The Availability Management process should maintain an AMIS that contains all of the measurements and information required to complete the Availability Management process and provide the appropriate information to the business on the level of IT service provided. This information, covering services, components and supporting services, provides the basis for regular, ad hoc and exception availability reporting and the identification of trends within the data for the instigation of improvement activities. These activities and the information contained within the AMIS provide the basis for developing the content of the Availability Plan.

In order to provide structure and focus to a wide range of initiatives that may need to be undertaken to improve availability, an Availability Plan should be formulated and maintained. The Availability Plan should have aims, objectives and deliverables and should consider the wider issues of people, processes, tools and techniques as well as having a technology focus. In the initial stages it may be aligned with an implementation plan for Availability Management, but the two are different and should not be confused. As the Availability Management process matures, the plan should evolve to cover the following:

- Actual levels of availability versus agreed levels of availability for key IT services. Availability measurements should always be business- and customer-focused and report availability as experienced by the business and users.
- Activities being progressed to address shortfalls in availability for existing IT services. Where investment decisions are required, options with associated costs and benefits should be included.
- Details of changing availability requirements for existing IT services. The plan should document the options available to meet these changed requirements.

- Where investment decisions are required, the associated costs of each option should be included.
- Details of the availability requirements for forthcoming new IT services. The plan should document the options available to meet these new requirements. Where investment decisions are required, the associated costs of each option should be included.
- A forward-looking schedule for the planned SFA assignments.
- Regular reviews of SFA assignments should be completed to ensure that the availability of technology is being proactively improved in conjunction with the SIP.
- A technology futures section to provide an indication of the potential benefits and exploitation opportunities that exist for planned technology upgrades. Anticipated availability benefits should be detailed, where possible based on business-focused measures, in conjunction with Capacity Management. The effort required to realize these benefits where possible should also be quantified.

During the production of the Availability Plan, it is recommended that liaison with all functional, technical and process areas is undertaken. The Availability Plan should cover a period of one to two years, with a more detailed view and information for the first six months. The plan should be reviewed regularly, with minor revisions every quarter and major revisions every half year. Where the technology is only subject to a low level of change, this may be extended as appropriate.

It is recommended that the Availability Plan is considered complementary to the Capacity Plan and Financial Plan, and that publication is aligned with the capacity and business budgeting cycle. If a demand is foreseen for high levels of availability that cannot be met due to the constraints of the existing IT infrastructure or budget, then exception reports may be required for the attention of both senior IT and business management.

In order to facilitate the production of the Availability Plan, Availability Management may wish to consider having its own database repository. The AMIS can be utilized to record and store selected data and information required to support key activities such as report generation, statistical analysis and availability forecasting and planning. The AMIS should be the main repository for the recording of IT availability metrics, measurements, targets and documents, including the Availability Plan, availability measurements, achievement reports, SFA

assignment reports, design criteria, action plans and testing schedules.

Hints and tips

Be pragmatic, define the initial tool requirements and identify what is already deployed that can be used and shared to get started as quickly as possible. Where basic tools are not already available, work with the other IT service and systems management processes to identify common requirements with the aim of selecting shared tools and minimizing costs. The AMIS should address the specific reporting needs of Availability Management not currently provided by existing repositories and integrate with them and their contents.

4.4.9 Challenges, Critical Success Factors and risks

Availability Management faces many challenges, but probably the main challenge is to actually meet the expectations of the customers, the business and senior management. These expectations are that services will always be available not just during their agreed service hours, but that all services will be available on a 24-hour, 365-day basis. When they aren't, it is assumed that they will be recovered within minutes. This is only the case when the appropriate level of investment and design has been applied to the service, and this should only be made where the business impact justifies that level of investment. However, the message needs to be publicized to all customers and areas of the business, so that when services do fail they have the right level of expectation on their recovery. It also means that Availability Management must have access to the right level of quality information on the current business need for IT services and its plans for the future. This is another challenge faced by many Availability Management processes.

Another challenge facing Availability Management is the integration of all of the availability data into an integrated set of information (AMIS) that can be analysed in a consistent manner to provide details on the availability of all services and components. This is particularly challenging when the information from the different technologies is often provided by different tools in differing formats.

Yet another challenge facing Availability Management is convincing the business and senior management of the investment needed in proactive availability measures. Investment is always recognized once failures have occurred, but by then it is really too late. Persuading

businesses and customers to invest in resilience to avoid the possibility of failures that may happen is a difficult challenge. Availability Management should work closely with Service Continuity Management, Security Management and Capacity Management in producing the justifications necessary to secure the appropriate investment.

The main CSFs for the Availability Management process are:

- Manage availability and reliability of IT service
- Satisfy business needs for access to IT services
- Availability of IT infrastructure, as documented in SLAs, provided at optimum costs.

Some of the major risks associated with Availability Management include:

- A lack of commitment from the business to the Availability Management process
- A lack of commitment from the business and a lack of appropriate information on future plans and strategies
- A lack of senior management commitment or a lack of resources and/or budget to the Availability Management process
- The reporting processes become very labour-intensive
- The processes focus too much on the technology and not enough on the services and the needs of the business
- The Availability Management information (AMIS) is maintained in isolation and is not shared or consistent with other process areas, especially ITSCM, Security Management and Capacity Management. This investment is particularly important when considering the necessary service and component backup and recovery tools, technology and processes to meet the agreed needs.

4.5 IT SERVICE CONTINUITY MANAGEMENT

4.5.1 Purpose/goal/objective

'The goal of ITSCM is to support the overall Business Continuity Management process by ensuring that the required IT technical and service facilities (including computer systems, networks, applications, data repositories, telecommunications, environment, technical support and Service Desk) can be resumed within required, and agreed, business timescales.'

As technology is a core component of most business processes, continued or high availability of IT is critical to the survival of the business as a whole. This is achieved by

introducing risk reduction measures and recovery options. Like all elements of ITSM, successful implementation of ITSCM can only be achieved with senior management commitment and the support of all members of the organization. Ongoing maintenance of the recovery capability is essential if it is to remain effective. The purpose of ITSCM is to maintain the necessary ongoing recovery capability within the IT services and their supporting components.

The objectives of ITSCM are to:

- Maintain a set of IT Service Continuity Plans and IT recovery plans that support the overall Business Continuity Plans (BCPs) of the organization
- Complete regular Business Impact Analysis (BIA) exercises to ensure that all continuity plans are maintained in line with changing business impacts and requirements
- Conduct regular Risk Analysis and Management exercises, particularly in conjunction with the business and the Availability Management and Security Management processes, that manage IT services within an agreed level of business risk
- Provide advice and guidance to all other areas of the business and IT on all continuity- and recovery-related issues
- Ensure that appropriate continuity and recovery mechanisms are put in place to meet or exceed the agreed business continuity targets
- Assess the impact of all changes on the IT Service Continuity Plans and IT recovery plans
- Ensure that proactive measures to improve the availability of services are implemented wherever it is cost-justifiable to do so
- Negotiate and agree the necessary contracts with suppliers for the provision of the necessary recovery capability to support all continuity plans in conjunction with the Supplier Management process.

4.5.2 Scope

ITSCM focuses on those events that the business considers significant enough to be considered a disaster. Less significant events will be dealt with as part of the Incident Management process. What constitutes a disaster will vary from organization to organization. The impact of a loss of a business process, such as financial loss, damage to reputation or regulatory breach, is measured through a BIA exercise, which determines the minimum critical requirements. The specific IT technical and service requirements are supported by ITSCM. The scope of ITSCM within an organization is determined by the organizational

structure, culture and strategic direction (both business and technology) in terms of the services provided and how these develop and change over time.

ITSCM primarily considers the IT assets and configurations that support the business processes. If (following a disaster) it is necessary to relocate to an alternative working location, provision will also be required for items such as office and personnel accommodation, copies of critical paper records, courier services and telephone facilities to communicate with customers and third parties.

The scope will need to take into account the number and location of the organization's offices and the services performed in each.

ITSCM does not usually directly cover longer-term risks such as those from changes in business direction, diversification, restructuring, major competitor failure, and so on. While these risks can have a significant impact on IT service elements and their continuity mechanisms, there is usually time to identify and evaluate the risk and include risk mitigation through changes or shifts in business and IT strategies, thereby becoming part of the overall business and IT Change Management programme.

Similarly, ITSCM does not usually cover minor technical faults (for example, non critical disk failure), unless there is a possibility that the impact could have a major impact on the business. These risks would be expected to be covered mainly through the Service Desk and the Incident Management process, or resolved through the planning associated with the processes of Availability Management, Problem Management, Change Management, Configuration Management and 'business as usual' operational management.

The ITSCM process includes:

- The agreement of the scope of the ITSCM process and the policies adopted.
- Business Impact Analysis (BIA) to quantify the impact loss of IT service would have on the business.
- Risk Analysis (RA) – the risk identification and risk assessment to identify potential threats to continuity and the likelihood of the threats becoming reality. This also includes taking measures to manage the identified threats where this can be cost-justified.
- Production of an overall ITSCM strategy that must be integrated into the BCM strategy. This can be produced following the two steps identified above, and is likely to include elements of risk reduction as well as selection of appropriate and comprehensive recovery options.

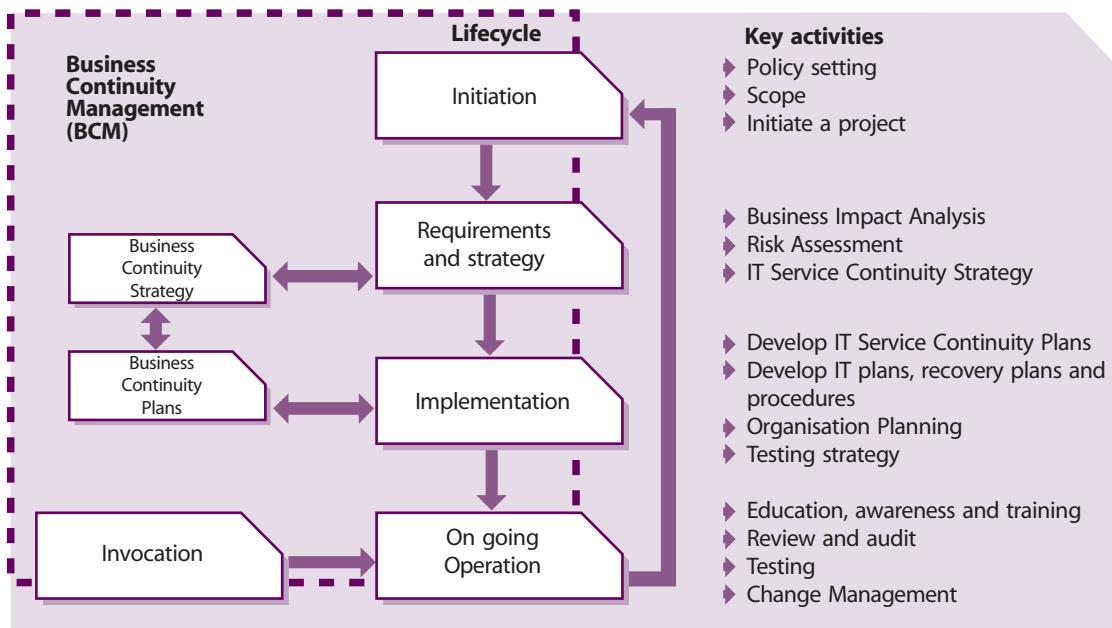


Figure 4.21
Lifecycle of
Service
Continuity
Management

- Production of an ITSCM plan, which again must be integrated with the overall BCM plans.
- Testing of the plans.
- Ongoing operation and maintenance of the plans.

4.5.3 Value to the business

ITSCM provides an invaluable role in supporting the Business Continuity Planning process. In many organizations, ITSCM is used to raise awareness of continuity and recovery requirements and is often used to justify and implement a Business Continuity Planning process and Business Continuity Plans. The ITSCM should be driven by business risk as identified by Business Continuity Planning, and ensures that the recovery arrangements for IT services are aligned to identified business impacts, risks and needs.

4.5.4 Policies/principles/basic concepts

A lifecycle approach should be adopted to the setting up and operation of an ITSCM process. Figure 4.21 shows the lifecycle of ITSCM, from initiation through to continual assurance that the protection provided by the plan is current and reflects all changes to services and service levels. ITSCM is a cyclic process through the lifecycle to ensure that once service continuity and recovery plans have been developed they are kept aligned with Business Continuity Plans (BCPs) and business priorities. Figure 4.21 also shows the role played within the ITSCM process of BCM.

Initiation and requirements stages are principally BCM activities. ITSCM should only be involved in these stages to support the BCM activities and to understand the

relationship between the business processes and the impacts caused on them by loss of IT service. As a result of these initial BIA and Risk Analysis activities, BCM should produce a Business Continuity Strategy, and the first real ITSCM task is to produce an ITSCM strategy that underpins the BCM strategy and its needs.

The Business Continuity Strategy should principally focus on business processes and associated issues (e.g. business process continuity, staff continuity, buildings continuity). Once the Business Continuity Strategy has been produced, and the role that IT services has to provide within the strategy has been determined, an ITSCM strategy can be produced that supports and enables the Business Continuity Strategy. This ensures that cost-effective decisions can be made, considering all the 'resources' to deliver a business process. Failure to do this tends to encourage ITSCM options that are faster, more elaborate and expensive than are actually needed.

The activities to be considered during initiation depend on the extent to which continuity facilities have been applied within the organization. Some parts of the business may have established individual Business Continuity Plans based around manual work-arounds, and IT may have developed continuity plans for systems perceived to be critical. This is good input to the process. However, effective ITSCM depends on supporting critical business functions. The only way of implementing effective ITSCM is through the identification of critical business processes and the analysis and coordination of the required technology and supporting IT services.

This situation may be even more complicated in outsourcing situations where an ITSCM process within an

external service provider or outsourcer organization has to meet the needs not only of the customer BCM process and strategy, but also of the outsourcer's own BCM process and strategy. These needs may be in conflict with one another, or may conflict with the BCM needs of one of the other outsourcing organization's customers.

However, in many organizations BCM is absent or has very little focus, and often ITSCM is required to fulfil many of the requirements and activities of BCM. The rest of this section has assumed that ITSCM has had to perform many of the activities required by BCM. Where a BCM process is established with Business Continuity Strategies and Plans in place, these documents should provide the focus and drive for establishing ITSCM.

4.5.5 Process activities, methods and techniques

The following sections contain details of each of the stages within the ITSCM lifecycle.

4.5.5.1 Stage 1 – Initiation

The initiation process covers the whole of the organization and consists of the following activities:

- **Policy setting** – this should be established and communicated as soon as possible so that all members of the organization involved in, or affected by, Business Continuity issues are aware of their responsibilities to comply with and support ITSCM. As a minimum, the policy should set out management intention and objectives.
- **Specify terms of reference and scope** – this includes defining the scope and responsibilities of all staff in the organization. It covers such tasks as undertaking a Risk Analysis and Business Impact Analysis and determination of the command and control structure required to support a business interruption. There is also a need to take into account such issues as outstanding audit points, regulatory or client requirements and insurance organization stipulations, and compliance with standards such as ISO 27001, the Standard on Information Security Management, which also addresses Service Continuity requirements.
- **Allocate resources** – the establishment of an effective Business Continuity environment requires considerable resource in terms of both money and manpower. Depending on the maturity of the organization, with respect to ITSCM, there may be a requirement to familiarize and/or train staff to accomplish the Stage 2 tasks. Alternatively, the use of experienced external consultants may assist in completing the analysis more quickly. However, it is important that the organization

can then maintain the process going forward without the need to rely totally on external support.

■ **Define the project organization and control structure**

structure – ITSCM and BCM projects are potentially complex and need to be well organized and controlled. It is strongly advisable to use a recognized standard project planning methodology such as Projects IN a Controlled Environment (PRINCE2®) or Project Management Body Of Knowledge (PMBOK®).

■ **Agree project and quality plans** – plans enable the project to be controlled and variances addressed.

Quality plans ensure that the deliverables are achieved and to an acceptable level of quality. They also provide a mechanism for communicating project resource requirements and deliverables, thereby obtaining 'buy-in' from all necessary parties.

4.5.5.2 Stage 2 – Requirements and strategy

Ascertaining the business requirements for IT service continuity is a critical component in order to determine how well an organization will survive a business interruption or disaster and the costs that will be incurred. If the requirements analysis is incorrect, or key information has been missed, this could have serious consequences on the effectiveness of ITSCM mechanisms.

This stage can effectively be split into two sections:

- **Requirements** – perform Business Impact Analysis and risk assessment
- **Strategy** – following the requirements analysis, the strategy should document the required risk reduction measures and recovery options to support the business.

Requirements – Business Impact Analysis

The purpose of a Business Impact Analysis (BIA) is to quantify the impact to the business that loss of service would have. This impact could be a 'hard' impact that can be precisely identified – such as financial loss – or 'soft' impact – such as public relations, morale, health and safety or loss of competitive advantage. The BIA will identify the most important services to the organization and will therefore be a key input to the strategy.

The BIA identifies:

- The form that the damage or loss may take – for example:
 - Lost income
 - Additional costs
 - Damaged reputation
 - Loss of goodwill
 - Loss of competitive advantage
 - Breach of law, health and safety

- Risk to personal safety
 - Immediate and long-term loss of market share
 - Political, corporate or personal embarrassment
 - Loss of operational capability – for example, in a command and control environment
- How the degree of damage or loss is likely to escalate after a service disruption, and the times of the day, week, month or year when disruption will be most severe
- The staffing, skills, facilities and services (including the IT services) necessary to enable critical and essential business processes to continue operating at a minimum acceptable level
- The time within which minimum levels of staffing, facilities and services should be recovered
- The time within which all required business processes and supporting staff, facilities and services should be fully recovered
- The relative business recovery priority for each of the IT services.

One of the key outputs from a BIA exercise is a graph of the anticipated business impact caused by the loss of a business process or the loss of an IT service over time, as illustrated in Figure 4.22.

This graph can then be used to drive the business and IT continuity strategies and plans. More preventative measures need to be adopted with regard to those processes and services with earlier and higher impacts,

whereas greater emphasis should be placed on continuity and recovery measures for those where the impact is lower and takes longer to develop. A balanced approach of both measures should be adopted to those in between.

These items provide the drivers for the level of ITSCM mechanisms that need to be considered or deployed. Once presented with these options, the business may decide that lower levels of service or increased delays are more acceptable, based on a cost-benefit analysis, or it maybe that comprehensive disaster prevention measures will need to be implemented.

These assessments enable the mapping of critical service, application and technology components to critical business processes, thus helping to identify the ITSCM elements that need to be provided. The business requirements are ranked and the associated ITSCM elements confirmed and prioritized in terms of risk reduction and recovery planning. The results of the BIA, discussed earlier, are invaluable input to several areas of process design including Service Level Management to understand the required service levels.

Impacts should be measured against particular scenarios for each business process, such as an inability to settle trades in a money market dealing process, or an inability to invoice for a period of days. An example is a money market dealing environment where loss of market data information could mean that the organization starts to lose money immediately as trading cannot continue. In

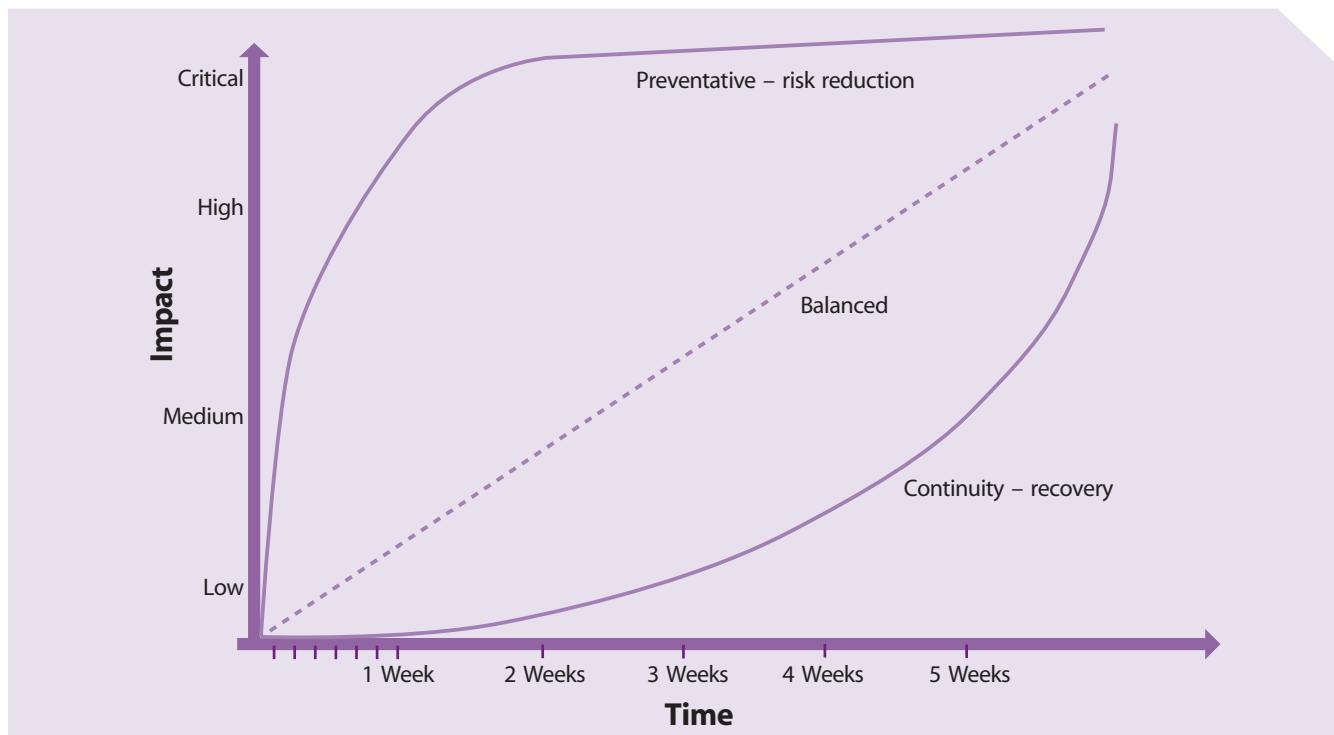


Figure 4.22 Graphical representation of business impacts

addition, customers may go to another organization, which would mean potential loss of core business. Loss of the settlement system does not prevent trading from taking place, but if trades already conducted cannot be settled within a specified period of time, the organization may be in breach of regulatory rules or settlement periods and suffer fines and damaged reputation. This may actually be a more significant impact than the inability to trade because of an inability to satisfy customer expectations.

It is also important to understand how impacts may change over time. For instance, it may be possible for a business to function without a particular process for a short period of time. In a balanced scenario, impacts to the business will occur and become greater over time. However, not all organizations are affected in this way. In some organizations, impacts are not apparent immediately. At some point, however, for any organization, the impacts will accrue to such a level that the business can no longer operate. ITSCM ensures that contingency options are identified so that the appropriate measure can be applied at the appropriate time to keep business impacts from service disruption to a minimum level.

When conducting a BIA, it is important that senior business area representatives' views are sought on the impact following loss of service. It is also equally important that the views of supervisory staff and more junior staff are sought to ensure all aspects of the impact following loss of service are ascertained. Often different levels of staff will have different views on the impact, and all will have to be taken into account when producing the overall strategy.

In many organizations it will be impossible, or it will not be cost-justifiable, to recover the total service in a very short timescale. In many cases, business processes can be re-established without a full complement of staff, systems and other facilities, and still maintain an acceptable level of service to clients and customers. The business recovery objectives should therefore be stated in terms of:

- The time within which a pre-defined team of core staff and stated minimum facilities must be recovered
- The timetable for recovery of remaining staff and facilities.

It may not always be possible to provide the recovery requirements to a detailed level. There is a need to balance the potential impact against the cost of recovery

to ensure that the costs are acceptable. The recovery objectives do, however, provide a starting point from which different business recovery and ITSCM options can be evaluated.

Requirements – Risk Analysis

The second driver in determining ITSCM requirements is the likelihood that a disaster or other serious service disruption will actually occur. This is an assessment of the level of threat and the extent to which an organization is vulnerable to that threat. Risk Analysis can also be used in assessing and reducing the chance of normal operational incidents and is a technique used by Availability Management to ensure the required availability and reliability levels can be maintained. Risk Analysis is also a key aspect of Information Security Management. A diagram on Risk Analysis and Management (Figure 4.20) is contained within the Availability Management process in section 4.4.

A number of Risk Analysis and Management methods are available for both the commercial and government sectors. Risk Analysis is the assessment of the risks that may give rise to service disruption or security violation. Risk management is concerned with identifying appropriate risk responses or cost-justifiable counter-measures to combat those risks.

A standard methodology, such as the Management of Risk (M_o_R), should be used to assess and manage risks within an organization. The M_o_R framework is illustrated in Figure 4.23.

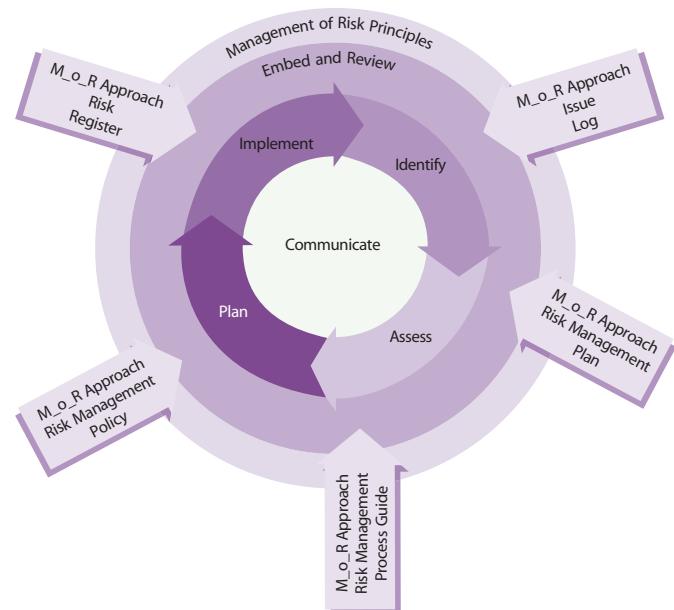


Figure 4.23 Management of Risk

The M_o_R approach is based around the above framework, which consists of the following:

- **M_o_R principles:** these principles are essential for the development of good risk management practice and are derived from corporate governance principles.
- **M_o_R approach:** an organization's approach to these principles needs to be agreed and defined within the following living documents:
 - Risk Management Policy
 - Process Guide
 - Plans
 - risk registers
 - Issue Logs.
- **M_o_R Processes:** the following four main steps describe the inputs, outputs and activities that ensure that risks are controlled:
 - **Identify:** the threats and opportunities within an activity that could impact the ability to reach its objective
 - **Assess:** the understanding of the net effect of the identified threats and opportunities associated with an activity when aggregated together
 - **Plan:** to prepare a specific management response that will reduce the threats and maximize the opportunities
 - **Implement:** the planned risk management actions, monitor their effectiveness and take corrective action where responses do not match expectations.
- **Embedding and reviewing M_o_R:** having put the principles, approach and processes in place, they need to be continually reviewed and improved to ensure they remain effective.
- **Communication:** having the appropriate communication activities in place to ensure that everyone is kept up-to-date with changes in threats, opportunities and any other aspects of risk management.

This M_o_R method requires the evaluation of risks and the development of a risk profile, such as the example in Figure 4.24.

Figure 4.24 shows an example risk profile, containing many risks that are outside the defined level of 'acceptable risk'. Following the Risk Analysis it is possible to determine appropriate risk responses or risk reduction measures (ITSCM mechanisms) to manage the risks, i.e. reduce the risk to an acceptable level or mitigate the risk. Wherever possible, appropriate risk responses should be implemented to reduce either the impact or the

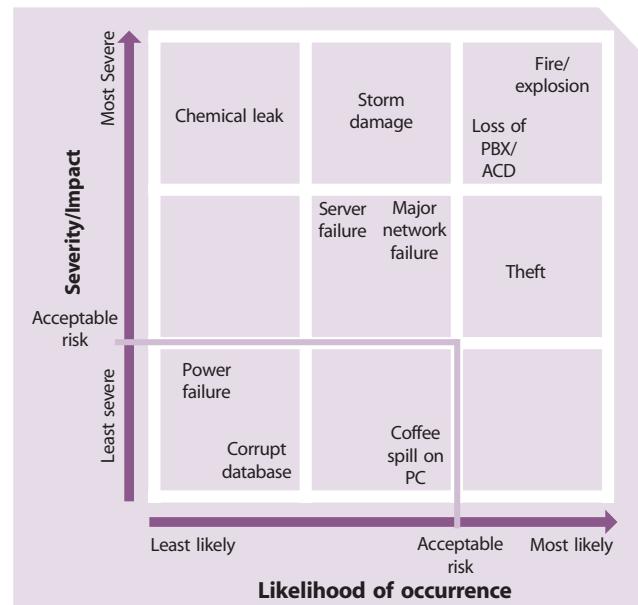


Figure 4.24 Example summary risk profile

likelihood, or both, of these risks from manifesting themselves.

In the context of ITSCM, there are a number of risks that need to be taken into consideration. The following is not a comprehensive list but does give some examples of risks and threats that need to be addressed by the ITSCM process.

IT Service Continuity Strategy

The results of the Business Impact Analysis and the Risk Analysis will enable appropriate Business and IT Service Continuity strategies to be produced in line with the business needs. The strategy will be an optimum balance of risk reduction and recovery or continuity options. This includes consideration of the relative service recovery priorities and the changes in relative service priority for the time of day, day of the week, and monthly and annual variations. Those services that have been identified as high impacts in the short term within the BIA will want to concentrate efforts on preventative risk reduction methods – for example, through full resilience and fault tolerance – while an organization that has low short-term impacts would be better suited to comprehensive recovery options, as described in the following sections. Similar advice and guidance can be found in the Business Continuity Institute's BCI Good Practice Guidelines.

Risk response measures

Most organizations will have to adopt a balanced approach where risk reduction and recovery are complementary and both are required. This entails reducing, as far as possible, the risks to the continued

Table 4.1 Examples of risks and threats

Risk	Threat
Loss of internal IT systems/networks, PABXs, ACDs, etc.	Fire Power failure Arson and vandalism Flood Aircraft impact Weather damage, e.g. hurricane Environmental disaster Terrorist attack Sabotage Catastrophic failure Electrical damage, e.g. lightning Accidental damage Poor-quality software
Loss of external IT systems/networks, e.g. e-commerce servers, cryptographic systems	All of the above Excessive demand for services Denial of service attack, e.g. against an internet firewall Technology failure, e.g. cryptographic system
Loss of data	Technology failure Human error Viruses, malicious software, e.g. attack applets
Loss of network services	Damage or denial of access to network service provider's premises Loss of service provider's IT systems/networks Loss of service provider's data Failure of the service provider
Unavailability of key technical and support staff	Industrial action Denial of access to premises Resignation Sickness/injury Transport difficulties
Failure of service providers, e.g. outsourced IT	Commercial failure, e.g. insolvency Denial of access to premises Unavailability of service provider's staff Failure to meet contractual service levels

provision of the IT service and is usually achieved through Availability Management. However well planned, it is impossible to completely eliminate all risks – for example, a fire in a nearby building will probably result in damage, or at least denial of access, as a result of the implementation of a cordon. As a general rule, the invocation of a recovery capability should only be taken as a last resort. Ideally, an organization should assess all of the risks to reduce the potential requirement to recover the business, which is likely to include the IT services.

The risk reduction measures need to be implemented and should be instigated in conjunction with Availability Management, as many of these reduce the probability of

failure affecting the availability of service. Typical risk reduction measures include:

- Installation of UPS and backup power to the computer
- Fault-tolerant systems for critical applications where even minimal downtime is unacceptable – for example, a banking system
- RAID arrays and disk mirroring for LAN servers to prevent against data loss and to ensure continued availability of data
- Spare equipment/components to be used in the event of equipment or component failure – for example, a spare LAN server already configured with the standard configuration and available to replace a faulty server with minimum build and configuration time

- The elimination of SpoFs, such as single access network points or single power supply into a building
- Resilient IT systems and networks
- Outsourcing services to more than one provider
- Greater physical and IT-based security controls
- Better controls to detect service disruptions, such as fire detection systems, coupled with suppression systems
- A comprehensive backup and recovery strategy, including off-site storage.

The above measures will not necessarily solve an ITSCM issue and remove the risk totally, but all or a combination of them may significantly reduce the risks associated with the way in which services are provided to the business.

Off-site storage

One risk response method is to ensure all vital data is backed up and stored off-site. Once the recovery strategy has been defined, an appropriate backup strategy should be adopted and implemented to support it. The backup strategy must include regular (probably daily) removal of data (including the CMS to ease recovery) from the main data centres to a suitable off-site storage location. This will ensure retrieval of data following relatively minor operational failure as well as total and complete disasters. As well as the electronic data, all other important information and documents should be stored off-site, with the main example being the ITSCM plans.

ITSCM recovery options

An organization's ITSCM strategy is a balance between the cost of risk reduction measures and recovery options to support the recovery of critical business processes within agreed timescales. The following is a list of the potential IT recovery options that need to be considered when developing the strategy.

Manual work-arounds

For certain types of services, manual work-arounds can be an effective interim measure for a limited timeframe until the IT service is resumed. For instance, a Service Desk call-logging service could survive for a limited time using paper forms linked to a laptop computer with a spreadsheet.

Reciprocal arrangements

In the past, reciprocal arrangements were typical contingency measures where agreements were put in place with another organization using similar technology. This is no longer effective or possible for most types of IT systems, but can still be used in specific cases – for example, setting up an agreement to share high-speed

printing facilities. Reciprocal arrangements can also be used for the off-site storage of backups and other critical information.

Gradual recovery

This option (sometimes referred to as 'cold standby') includes the provision of empty accommodation, fully equipped with power, environmental controls and local network cabling infrastructure, telecommunications connections, and available in a disaster situation for an organization to install its own computer equipment. It does not include the actual computing equipment, so is not applicable for services requiring speedy recovery, as set-up time is required before recovery of services can begin. This recovery option is only recommended for services that can bear a delay of recovery time in days or weeks, not hours. Any non-critical service that can bear this type of delay should take into account the cost of this option versus the benefit to the business before determining if a gradual recovery option should be included in the ITSCM options for the organization.

The accommodation may be provided commercially by a third party, for a fee, or may be private, (established by the organization itself) and provided as either a fixed or portable service.

A portable facility is typically a prefabricated building provided by a third party and located, when needed, at a predetermined site agreed with the organization. This may be in another location some distance from the home site, perhaps another owned building. The replacement computer equipment will need to be planned, but suppliers of computing equipment do not always guarantee replacement equipment within a fixed deadline, though they would normally do so under their best efforts.

Intermediate recovery

This option (sometimes referred to as 'warm standby') is selected by organizations that need to recover IT facilities within a predetermined time to prevent impacts to the business process. The predetermined time will have been agreed with the business during the BIA.

Most common is the use of commercial facilities, which are offered by third-party recovery organizations to a number of subscribers, spreading the cost across those subscribers. Commercial facilities often include operation, system management and technical support. The cost varies depending on the facilities requested, such as processors, peripherals, communications, and how quickly the services must be restored.

The advantage of this service is that the customer can have virtually instantaneous access to a site, housed in a

secure building, in the event of a disaster. It must be understood, however, that the restoration of services at the site may take some time, as delays may be encountered while the site is re-configured for the organization that invokes the service, and the organization's applications and data will need to be restored from backups.

One potentially major disadvantage is the security implications of running IT services at a third party's data centre. This must be taken into account when planning to use this type of facility. For some organizations, the external intermediate recovery option may not be appropriate for this reason.

If the site is invoked, there is often a daily fee for use of the service in an emergency, although this may be offset against additional cost of working insurance.

Commercial recovery services can be provided in self-contained, portable or mobile form where an agreed system is delivered to a customer's site, within an agreed time.

Fast recovery

This option (sometimes referred to as 'hot standby') provides for fast recovery and restoration of services and is sometimes provided as an extension to the intermediate recovery provided by a third-party recovery provider. Some organizations will provide their own facilities within the organization, but not on an alternative site to the one used for the normal operations. Others implement their own internal second locations on an alternative site to provide more resilient recovery.

Where there is a need for a fast restoration of a service, it is possible to 'rent' floor space at the recovery site and install servers or systems with application systems and

communications already available, and data mirrored from the operational servers. In the event of a system failure, the customers can then recover and switch over to the backup facility with little loss of service. This typically involves the re-establishment of the critical systems and services within a 24-hour period.

Immediate recovery

This option (also often referred to as 'hot standby', 'mirroring', 'load balancing' or 'split site') provides for immediate restoration of services, with no loss of service. For business critical services, organizations requiring continuous operation will provide their own facilities within the organization, but not on the same site as the normal operations. Sufficient IT equipment will be 'dual located' in either an owned or hosted location to run the compete service from either location in the event of loss of one facility, with no loss of service to the customer. The second site can then be recovered whilst the service is provided from the single operable location. This is an expensive option, but may be justified for critical business processes or VBFs where non-availability for a short period could result in a significant impact, or where it would not be appropriate to be running IT services on a third party's premises for security or other reasons. The facility needs to be located separately and far enough away from the home site that it will not be affected by a disaster affecting that location. However, these mirrored servers and sites options should be implemented in close liaison with Availability Management as they support services with high levels of availability.

The strategy is likely to include a combination of risk response measures and a combination of the above recovery options, as illustrated in Figure 4.25.

	Manual	Immediate	Fast	Intermediate	Gradual
Service Desk	Yes		Yes	Yes	Yes
Mainframe payroll	Yes			Yes	Yes
Financial system			Yes		Yes
Dealer system		Yes		Yes	Yes

Figure 4.25 Example set of recovery options

Figure 4.25 shows that a number of options may be used to provide continuity of service. An example from Figure 4.25 shows that, initially, continuity of the Service Desk is provided using manual processes such as a set of forms, and maybe a spreadsheet operating from a laptop computer, whilst recovery plans for the service are completed on an alternative 'fast recovery' site. Once the alternative site has become operational, the Service Desk can switch back to using the IT service. However, use of the external 'fast recovery' alternative site is probably limited in duration, so while running temporarily from this site, the 'intermediate site' can be made operational and long-term operations can be transferred there.

Different services within an organization require different in-built resilience and different recovery options. Whatever option is chosen, the solution will need to be cost-justified. As a general rule, the longer the business can survive without a service, the cheaper the solution will be. For example, a critical healthcare system that requires continuous operation will be very costly, as potential loss of service will need to be eliminated by the use of immediate recovery, whereas a service the absence of which does not severely affect the business for a week or so could be supported by a much cheaper solution, such as intermediate recovery.

As well as the recovery of the computing equipment, planning needs to include the recovery of accommodation and infrastructure for both IT and user staff. Other areas to be taken into account include critical services such as power, telecommunications, water, couriers, post, paper records and reference material.

It is important to remember that the recovery is based around a series of stand-by arrangements including accommodation, procedures and people, as well as systems and telecommunications. Certain actions are necessary to implement the stand-by arrangements. For example:

- Negotiating for third-party recovery facilities and entering into a contractual arrangement
- Preparing and equipping the stand-by accommodation
- Purchasing and installing stand-by computer systems.

4.5.5.3 Stage 3 – Implementation

Once the strategy has been approved, the IT Service Continuity Plans need to be produced in line with the Business Continuity Plans.

ITSCM plans need to be developed to enable the necessary information for critical systems, services and facilities to either continue to be provided or to be reinstated within an acceptable period to the business. An

example ITSCM recovery plan is contained in Appendix K. Generally the Business Continuity Plans rely on the availability of IT services, facilities and resources. As a consequence of this, ITSCM plans need to address all activities to ensure that the required services, facilities and resources are delivered in an acceptable operational state and are 'fit for purpose' when accepted by the business. This entails not only the restoration of services and facilities, but also the understanding of dependencies between them, the testing required prior to delivery (performance, functional, operational and acceptance testing) and the validation of data integrity and consistency.

It should be noted that the continuity plans are more than just recovery plans, and should include documentation of the resilience measures and the measures that have been put into place to enable recovery, together with explanations of why a particular approach has been taken (this facilitates decisions should invocation determine that the particular situation requires a modification to the plan). However, the format of the plan should enable rapid access to the recovery information itself, perhaps as an appendix that can be accessed directly. All key staff should have access to copies of all the necessary recovery documentation.

Management of the distribution of the plans is important to ensure that copies are available to key staff at all times. The plans should be controlled documents (with formalized documents maintained under Change Management and Configuration Management control) to ensure that only the latest versions are in circulation and each recipient should ensure that a personal copy is maintained off-site.

The plan should ensure that all details regarding recovery of the IT services following a disaster are fully documented. It should have sufficient details to enable a technical person unfamiliar with the systems to be able to follow the procedures. The recovery plans include key details such as the data recovery point, a list of dependent systems, the nature of the dependency and their data recovery points, system hardware and software requirements, configuration details and references to other relevant or essential information about the service and systems.

It is a good idea to include a checklist that covers specific actions required during all stages of recovery for the service and system. For example, after the system has been restored to an operational state, connectivity checks, functionality checks or data consistency and integrity checks should be carried out prior to handing the service over to the business.

There are a number of technical plans that may already exist within an organization, documenting recovery procedures from a normal operational failure. The development and maintenance of these plans will be the responsibility of the specialist teams, but will be coordinated by the Business Continuity Management team. These will be useful additions or appendices to the main plan. Additionally, plans that will need to be integrated with the main BCP are:

- **Emergency Response Plan:** to interface to all emergency services and activities
- **Damage Assessment Plan:** containing details of damage assessment contacts, processes and plans
- **Salvage Plan:** containing information on salvage contacts, activities and processes
- **Vital Records Plan:** details of all vital records and information, together with their location, that are critical to the continued operation of the business
- **Crisis Management and Public Relations Plan:** the plans on the command and control of different crisis situations and management of the media and public relations
- **Accommodation and Services Plan:** detailing the management of accommodation, facilities and the services necessary for their continued operation
- **Security Plan:** showing how all aspects of security will be managed on all home sites and recovery sites
- **Personnel Plan:** containing details of how all personnel issues will be managed during a major incident
- **Communication Plan:** showing how all aspects of communication will be handled and managed with all relevant areas and parties involved during a major incident
- **Finance and Administration Plan:** containing details of alternative methods and processes for obtaining possible emergency authorization and access to essential funds during a major incident.

Finally, each critical business area is responsible for the development of a plan detailing the individuals who will be in the recovery teams and the tasks to be undertaken on invocation of recovery arrangements.

The ITSCM Plan must contain all the information needed to recover the IT systems, networks and telecommunications in a disaster situation once a decision to invoke has been made, and then to manage the business return to normal operation once the service disruption has been resolved. One of the most important inputs into the plan development is the results of the Business Impact Analysis. Additionally other areas will

need to be analysed, such as Service Level Agreements (SLA), security requirements, operating instructions and procedures and external contracts. It is likely that a separate SLA with alternative targets will have been agreed if running at a recovery site following a disaster.

Other areas that will need to be implemented following the approval of the strategy are:

Organization planning

During the disaster recovery process, the organizational structure will inevitably be different from normal operation and is based around:

- Executive – including senior management/executive board, with overall authority and control within the organization and responsible for crisis management and liaison with other departments, divisions, organizations, the media, regulators, emergency services etc.
- Coordination – typically one level below the executive group and responsible for coordinating the overall recovery effort within the organization
- Recovery – a series of business and service recovery teams, representing the critical business functions and the services that need to be established to support these functions. Each team is responsible for executing the plans within their own areas and for liaison with staff, customers and third parties. Within IT the recovery teams should be grouped by IT service and application. For example, the infrastructure team may have one or more people responsible for recovering external connections, voice services, local area networks, etc. and the support teams may be split by platform, operating system or application. In addition, the recovery priorities for the service, application or its components identified during the Business Impact Analysis should be documented within the recovery plans and applied during their execution.

Testing

Experience has shown that recovery plans that have not been fully tested do not work as intended, if at all. Testing is therefore a critical part of the overall ITSCM process and the only way of ensuring that the selected strategy, standby arrangements, logistics, business recovery plans and procedures will actually work in practice.

The IT service provider is responsible for ensuring that the IT services can be recovered in the required timescales with the required functionality and the required performance following a disaster.

There are four basic types of tests that can be undertaken:

- **Walk-through tests** can be conducted when the plan has been produced simply by getting the relevant people together to see if the plan(s) at least work in a simulated way.
- **Full tests** should be conducted as soon as possible after the plan production and at regular intervals of at least annually thereafter. They should involve the business units to assist in proving the capability to recover the services appropriately. They should, as far as possible, replicate an actual invocation of all standby arrangements and should involve external parties if they are planned to be involved in an actual invocation. The tests must not only prove recovery of the IT services but also the recovery of the business processes. It is recommended that an independent observer records all the activities of the tests and the timings of the service recovery. The observer's documentation of the tests will be vital input into the subsequent post mortem review. The full tests may be announced or unannounced. The first test of the plan is likely to be announced and carefully planned, but subsequent tests may be 'sprung' on key players without warning. It is also essential that many different people get involved, including those not very familiar with the IT service and systems, as the people with the most knowledge may not be available when a disaster actually occurs.
- **Partial tests** can also be undertaken where recovery of certain elements of the overall plan is tested, such as single services or servers. These types of tests should be in addition to the full test not instead of the full test. The full test is the best way of testing that all services can be recovered in required timescales and can run together on the recovery systems.
- **Scenario tests** can be used to test reactions and plans to specific conditions, events and scenarios. They can include testing that BCPs and IT Service Continuity Plans interface with each other, as well as interfacing with all other plans involved in the handling and management of a major incident.

All tests need to be undertaken against defined test scenarios, which are described as realistically as possible. It should be noted, however, that even the most comprehensive test does not cover everything. For example, in a service disruption where there has been injury or even death to colleagues, the reaction of staff to a crisis cannot be tested and the plans need to make allowance for this. In addition, tests must have clearly defined objectives and Critical Success Factors, which will

be used to determine the success or otherwise of the exercise.

4.5.5.4 Stage 4 – Ongoing operation

This stage consists of the following:

- **Education, awareness and training** – this should cover the organization and, in particular, the IT organization, for service continuity-specific items. This ensures that all staff are aware of the implications of business continuity and of service continuity and consider these as part of their normal working, and that everyone involved in the plan has been trained in how to implement their actions.
- **Review** – regular review of all of the deliverables from the ITSCM process needs to be undertaken to ensure that they remain current.
- **Testing** – following the initial testing, it is necessary to establish a programme of regular testing to ensure that the critical components of the strategy are tested, preferably at least annually, although testing of IT Service Continuity Plans should be arranged in line with business needs and the needs of the BCPs. All plans should also be tested after every major business change. It is important that any changes to the IT technology are also included in the strategy, implemented in an appropriate fashion and tested to ensure that they function correctly within the overall provision of IT following a disaster. The backup and recovery of IT service should also be monitored and tested to ensure that when they are needed during a major incident, they will operate as needed. This aspect is covered more fully in the Service Operation publication
- **Change Management** – the Change Management process should ensure that all changes are assessed for their potential impact on the ITSCM plans. If the planned change will invalidate the plans, then the plan must be updated before the change is implemented, and it should be tested as part of the change testing. The plans themselves must be under very strict Change Management and Configuration Management control. Inaccurate plans and inadequate recovery capabilities may result in the failure of BCPs. Also, on an ongoing basis, whenever there are new services or where services have major changes, it is essential that a BIA and risk assessment is conducted on the new or changed service and the strategy and plans updated accordingly.

Invocation

Invocation is the ultimate test of the Business Continuity and ITSCM Plans. If all the preparatory work has been successfully completed, and plans developed and tested, then an invocation of the Business Continuity Plans should be a straightforward process, but if the plans have not been tested, failures can be expected. It is important that due consideration is given to the design of all invocation processes, to ensure that they are fit for purpose and interface to all other relevant invocation processes.

Invocation is a key component of the plans, which must include the invocation process and guidance. It should be remembered that the decision to invoke, especially if a third-party recovery facility is to be used, should not be taken lightly. Costs will be involved and the process will involve disruption to the business. This decision is typically made by a 'crisis management' team, comprising senior managers from the business and support departments (including IT), using information gathered through damage assessment and other sources.

A disruption could occur at any time of the day or night, so it is essential that guidance on the invocation process is readily available. Plans must be available to key staff in the office and away from the office.

The decision to invoke must be made quickly, as there may be a lead-time involved in establishing facilities at a recovery site. In the case of a serious building fire, the decision may be fairly easy to make. However, in the case of power failure or hardware fault, where a resolution is expected within a short period, a deadline should be set by which time if the incident has not been resolved, invocation will take place. If using external services providers, they should be warned immediately if there is a chance that invocation might take place.

The decision to invoke needs to take into account the:

- Extent of the damage and scope of the potential invocation
- Likely length of the disruption and unavailability of premises and/or services
- Time of day/month/year and the potential business impact. At year-end, the need to invoke may be more pressing, to ensure that year-end processing is completed on time.

Therefore the design of the invocation process must provide guidance on how all of these areas and circumstances should be assessed to assist the person invoking the continuity plan.

The ITSCM Plan should include details of activities that need to be undertaken, including:

- Retrieval of backup tapes or use of data vaulting to retrieve data
- Retrieval of essential documentation, procedures, workstation images, etc. stored off-site
- Mobilization of the appropriate technical personnel to go to the recovery site to commence the recovery of required systems and services
- Contacting and putting on alert telecommunications suppliers, support services, application vendors, etc. who may be required to undertake actions or provide assistance in the recovery process.

The invocation and initial recovery is likely to be a time of high activity, involving long hours for many individuals. This must be recognized and managed by the recovery team leaders to ensure that breaks are provided and prevent 'burn-out'. Planning for shifts and handovers must be undertaken to ensure that the best use is made of the facilities available. It is also vitally important to ensure that the usual business and technology controls remain in place during invocation, recovery and return to normal to ensure that information security is maintained at the correct level and that data protection is preserved.

Once the recovery has been completed, the business should be able to operate from the recovery site at the level determined and agreed in the strategy and relevant SLA. The objective, however, will be to build up the business to normal levels, maintain operation from the recovery site in the short term and vacate the recovery site in the shortest possible time. Details of all these activities need to be contained within the plans. If using external services, there will be a finite contractual period for using the facility. Whatever the period, a return to normal must be carefully planned and undertaken in a controlled fashion. Typically this will be over a weekend and may include some necessary downtime in business hours. It is important that this is managed well and that all personnel involved are aware of their responsibilities to ensure a smooth transition.

4.5.6 Triggers, inputs, outputs and interfaces

Many events may trigger ITSCM activity. These include:

- New or changed business needs, or new or changed services
- New or changed targets within agreements, such as SLRs, SLAs, OLAs or contracts
- The occurrence of a major incident that requires assessment for potential invocation of either Business or IT Continuity Plans

- Periodic activities such as the BIA or Risk Analysis activities, maintenance of Continuity Plans or other reviewing, revising or reporting activities
 - Assessment of changes and attendance at Change Advisory Board meetings
 - Review and revision of business and IT plans and strategies
 - Review and revision of designs and strategies
 - Recognition or notification of a change of risk or impact of a business process or VBF, an IT service or component
 - Initiation of tests of continuity and recovery plans.
- Integration and interfaces exist from ITSCM to all other processes. Important examples are as follows:
- **Change Management** – all changes need to be considered for their impact on the continuity plans, and if amendments are required to the plan, updates to the plan need to be part of the change. The plan itself must be under Change Management control.
 - **Incident and Problem Management** – incidents can easily evolve into major incidents or disasters. Clear criteria need to be agreed and documented on for the invocation of the ITSCM plans.
 - **Availability Management** – undertaking Risk Analysis and implementing risk responses should be closely coordinated with the availability process to optimize risk mitigation.
 - **Service Level Management** – recovery requirements will be agreed and documented in the SLAs. Different service levels could be agreed and documented that could be acceptable in a disaster situation.
 - **Capacity Management** – ensuring that there are sufficient resources to enable recovery onto replacement computers following a disaster.
 - **Configuration Management** – the CMS documents the components that make up the infrastructure and the relationship between the components. This information is invaluable for all the stages of the ITSCM lifecycle, the maintenance of plans and recovery facilities.
 - **Information Security Management** – a very close relationship exists between ITSCM and Information Security Management. A major security breach could be considered a disaster, so when conducting BIA and Risk Analysis, security will be a very important consideration.

4.5.6.1 Inputs

There are many sources of input required by the ITSCM process:

- Business information: from the organization's business strategy, plans and financial plans, and information on their current and future requirements
- IT information: from the IT strategy and plans and current budgets
- A Business Continuity Strategy and a set of Business Continuity Plans: from all areas of the business
- Service information: from the SLM process, with details of the services from the Service Portfolio and the Service Catalogue and service level targets within SLAs and SLRs
- Financial information: from Financial Management, the cost of service provision, the cost of resources and components
- Change information: from the Change Management process, with a Change Schedule and a need to assess all changes for their impact on all ITSCM plans
- CMS: containing information on the relationships between the business, the services, the supporting services and the technology
- Business Continuity Management and Availability Management testing schedules
- IT Service Continuity Plans and test reports from supplier and partners, where appropriate.

4.5.6.2 Outputs

The outputs from the ITSCM process include:

- A revised ITSCM policy and strategy
- A set of ITSCM plans, including all Crisis Management, Emergency Response Plans and Disaster Recovery Plans, together with a set of supporting plans and contracts with recovery service providers
- Business Impact Analysis exercises and reports, in conjunction with BCM and the business
- Risk Analysis and Management reviews and reports, in conjunction with the business, Availability Management and Security Management
- An ITSCM testing schedule
- ITSCM test scenarios
- ITSCM test reports and reviews.

Forecasts and predictive reports are used by all areas to analyse, predict and forecast particular business and IT scenarios and their potential solutions.

4.5.7 Key Performance Indicators

IT services are delivered and can be recovered to meet business objectives:

- Regular audits of the ITSCM Plans to ensure that, at all times, the agreed recovery requirements of the business can be achieved

- All service recovery targets are agreed and documented in SLAs and are achievable within the ITSCM Plans
- Regular and comprehensive testing of ITSCM Plans
- Regular reviews are undertaken, at least annually, of the business and IT continuity plans with the business areas
- Negotiate and manage all necessary ITSCM contracts with third party
- Overall reduction in the risk and impact of possible failure of IT services.

Awareness throughout the organizations of the plans:

- Ensure awareness of business impact, needs and requirements throughout IT
- Ensure that all IT service areas and staff are prepared and able to respond to an invocation of the ITSCM Plans
- Regular communication of the ITSCM objectives and responsibilities within the appropriate business and IT service areas.

4.5.8 Information Management

ITSCM needs to record all of the information necessary to maintain a comprehensive set of ITSCM plans. This information base should include:

- Information from the latest version of the BIA
- Comprehensive information on risk within a Risk Register, including risk assessment and risk responses
- The latest version of the BCM strategy and BCPs
- Details relating to all completed tests and a schedule of all planned tests
- Details of all ITSCM Plans and their contents
- Details of all other plans associated with ITSCM Plans
- Details of all existing recovery facilities, recovery suppliers and partners, recovery agreements and contracts, spare and alternative equipment
- Details of all backup and recovery processes, schedules, systems and media and their respective locations.

All the above information needs to be integrated and aligned with all BCM information and all the other information required by ITSCM. Interfaces to many other processes are required to ensure that this alignment is maintained.

4.5.9 Challenges, Critical Success Factors and risks

One of the major challenges facing ITSCM is to provide appropriate plans when there is no BCM process. If there is no BCM process, then IT is likely to make incorrect assumptions about business criticality of business processes and therefore adopt the wrong continuity strategies and options. Without BCM, expensive ITSCM solutions and plans will be rendered useless by the absence of corresponding plans and arrangements within the business. Also, if BCM is absent, then the business may fail to identify inexpensive non-IT solutions and waste money on ineffective, expensive IT solutions.

In some organizations, the business perception is that continuity is an IT responsibility, and therefore the business assumes that IT will be responsible for disaster recovery and that IT services will continue to run under any circumstances. This is especially true in some outsourced situations where the business may be reluctant to share its BCM information with an external service provider.

If there is a BCM process established, then the challenge becomes one of alignment and integration. ITSCM must ensure that accurate information is obtained from the BCM process on the needs, impact and priorities of the business, and that the ITSCM information and plans are aligned and integrated with those of the business. Having achieved that alignment, the challenge becomes one of keeping them aligned by management and control of business and IT change. It is essential, therefore, that all documents and plans are maintained under strict Change Management and Configuration Management control.

The main CSFs for the ITSCM process are:

- IT services are delivered and can be recovered to meet business objectives
- Awareness throughout the organization of the business and IT Service Continuity Plans.

Some of the major risks associated with ITSCM include:

- Lack of commitment from the business to the ITSCM processes and procedures
- Lack of commitment from the business and a lack of appropriate information on future plans and strategies
- Lack of senior management commitment or a lack of resources and/or budget for the ITSCM process
- The processes focus too much on the technology issues and not enough on the IT services and the needs and priorities of the business

- Risk Analysis and Management are conducted in isolation and not in conjunction with Availability Management and Security Management
- ITSCM plans and information become out-of-date and lose alignment with the information and plans of the business and BCM.

4.6 INFORMATION SECURITY MANAGEMENT

4.6.1 Purpose/goal/objective

'The goal of the ISM process is to align IT security with business security and ensure that information security is effectively managed in all service and Service Management activities'.

ISM needs to be considered within the overall corporate governance framework. Corporate governance is the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring the objectives are achieved, ascertaining the risks are being managed appropriately and verifying that the enterprise's resources are used effectively.

Information security is a management activity within the corporate governance framework, which provides the strategic direction for security activities and ensures objectives are achieved. It further ensures that the information security risks are appropriately managed and that enterprise information resources are used responsibly. The purpose of ISM is to provide a focus for all aspects of IT security and manage all IT security activities.

The term 'information' is used as a general term and includes data stores, databases and metadata. The objective of information security is to protect the interests of those relying on information, and the systems and communications that deliver the information, from harm resulting from failures of availability, confidentiality and integrity.

For most organizations, the security objective is met when:

- Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures (availability)
- Information is observed by or disclosed to only those who have a right to know (confidentiality)
- Information is complete, accurate and protected against unauthorized modification (integrity)
- Business transactions, as well as information exchanges between enterprises, or with partners, can be trusted (authenticity and non-repudiation).

Prioritization of confidentiality, integrity and availability must be considered in the context of business and business processes. The primary guide to defining what must be protected and the level of protection has to come from the business. To be effective, security must address entire business processes from end to end and cover the physical and technical aspects. Only within the context of business needs and risks can management define security.

4.6.2 Scope

The ISM process should be the focal point for all IT security issues, and must ensure that an Information Security Policy is produced, maintained and enforced that covers the use and misuse of all IT systems and services. ISM needs to understand the total IT and business security environment, including the:

- Business Security Policy and plans
- Current business operation and its security requirements
- Future business plans and requirements
- Legislative requirements
- Obligations and responsibilities with regard to security contained within SLAs
- The business and IT risks and their management.

Understanding all of this will enable ISM to ensure that all the current and future security aspects and risks of the business are cost-effectively managed.

The ISM process should include:

- The production, maintenance, distribution and enforcement of an Information Security Policy and supporting security policies
- Understanding the agreed current and future security requirements of the business and the existing Business Security Policy and plans
- Implementation of a set of security controls that support the Information Security Policy and manage risks associated with access to services, information and systems
- Documentation of all security controls, together with the operation and maintenance of the controls and their associated risks
- Management of suppliers and contracts regarding access to systems and services, in conjunction with Supplier Management
- Management of all security breaches and incidents associated with all systems and services
- The proactive improvement of security controls, and security risk management and the reduction of security risks

- Integration of security aspects within all other IT SM processes.

To achieve effective information security governance, management must establish and maintain an Information Security Management System (ISMS) to guide the development and management of a comprehensive information security programme that supports the business objectives.

4.6.3 Value to the business

ISM ensures that an Information Security Policy is maintained and enforced that fulfils the needs of the Business Security Policy and the requirements of corporate governance. ISM raises awareness of the need for security within all IT services and assets throughout the organization, ensuring that the policy is appropriate for the needs of the organization. ISM manages all aspects of IT and information security within all areas of IT and Service Management activity.

ISM provides assurance of business processes by enforcing appropriate security controls in all areas of IT and by managing IT risk in line with business and corporate risk management processes and guidelines.

4.6.4 Policies/principles/basic concepts

Prudent business practices require that IT processes and initiatives align with business processes and objectives. This is critical when it comes to information security, which must be closely aligned with business security and business needs. Additionally all processes within the IT organization must include security considerations.

Executive management is ultimately responsible for the organization's information and is tasked with responding to issues that affect its protection. In addition, boards of directors are expected to make information security an integral part of corporate governance. All IT service provider organizations must therefore ensure that they have a comprehensive ISM policy(s) and the necessary security controls in place to monitor and enforce the policies.

4.6.4.1 Security framework

The Information Security Management process and framework will generally consist of:

- An Information Security Policy and specific security policies that address each aspect of strategy, controls and regulation
- An Information Security Management System (ISMS), containing the standards, management

procedures and guidelines supporting the information security policies

- A comprehensive security strategy, closely linked to the business objectives, strategies and plans
- An effective security organizational structure
- A set of security controls to support the policy
- The management of security risks
- Monitoring processes to ensure compliance and provide feedback on effectiveness
- Communications strategy and plan for security
- Training and awareness strategy and plan.

4.6.4.2 The Information Security Policy

Information Security Management activities should be focused on and driven by an overall Information Security Policy and a set of underpinning specific security policies. The ITP should have the full support of top executive IT management and ideally the support and commitment of top executive business management. The policy should cover all areas of security, be appropriate, meet the needs of the business and should include:

- An overall Information Security Policy
- Use and misuse of IT assets policy
- An access control policy
- A password control policy
- An e-mail policy
- An internet policy
- An anti-virus policy
- An information classification policy
- A document classification policy
- A remote access policy
- A policy with regard to supplier access of IT service, information and components
- An asset disposal policy.

These policies should be widely available to all customers and users, and their compliance should be referred to in all SLRs, SLAs, contracts and agreements. The policies should be authorized by top executive management within the business and IT, and compliance to them should be endorsed on a regular basis. All security policies should be reviewed – and, where necessary, revised – on at least an annual basis.

4.6.4.3 The Information Security Management System (ISMS)

The framework or the ISMS in turn provides a basis for the development of a cost-effective information security programme that supports the business objectives. It will involve the Four Ps of People, Process, Products and

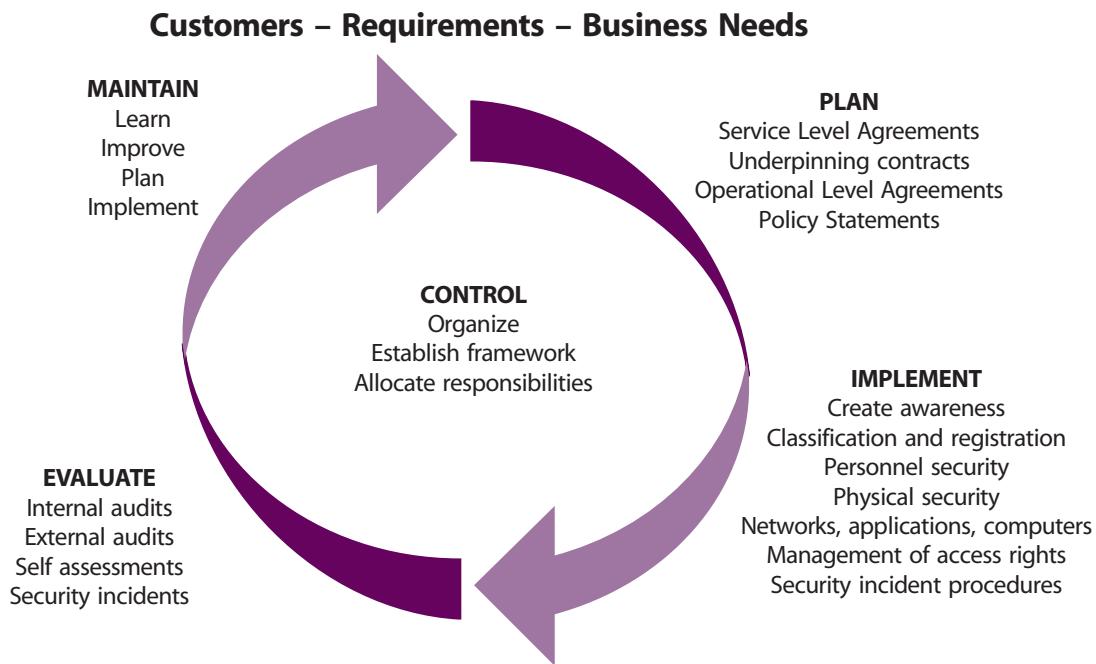


Figure 4.26 Framework for managing IT security

technology as well as Partners and suppliers to ensure high levels of security are in place.

ISO 27001 is the formal standard against which organizations may seek independent certification of their ISMS (meaning their frameworks to design, implement, manage, maintain and enforce information security processes and controls systematically and consistently throughout the organizations). The ISMS shown in Figure 4.26 shows an approach that is widely used and is based on the advice and guidance described in many sources, including ISO 27001.

The five elements within this framework are as follows:

Control

The objectives of the control element of the ISMS are to:

- Establish a management framework to initiate and manage information security in the organization
- Establish an organization structure to prepare, approve and implement the Information Security Policy
- Allocate responsibilities
- Establish and control documentation.

Plan

The objective of the plan element of the ISMS is to devise and recommend the appropriate security measures, based on an understanding of the requirements of the organization.

The requirements will be gathered from such sources as business and service risk, plans and strategies, SLAs

and OLAs and the legal, moral and ethical responsibilities for information security. Other factors, such as the amount of funding available and the prevailing organization culture and attitudes to security, must be considered.

The Information Security Policy defines the organization's attitude and stance on security matters. This should be an organization-wide document, not just applicable to the IT service provider. Responsibility for the upkeep of the document rests with the Information Security Manager.

Implement

The objective of the implementation of the ISMS is to ensure that appropriate procedures, tools and controls are in place to underpin the Information Security Policy.

Amongst the measures are:

- **Accountability for assets** – Configuration Management and the CMS are invaluable here
- **Information classification** – information and repositories should be classified according to the sensitivity and the impact of disclosure.

The successful implementation of the security controls and measures is dependent on a number of factors:

- The determination of a clear and agreed policy, integrated with the needs of the business
- Security procedures that are justified, appropriate and supported by senior management
- Effective marketing and education in security requirements
- A mechanism for improvement.

Evaluation

The objectives of the evaluation element of the ISMS are to:

- Supervise and check compliance with the security policy and security requirements in SLAs and OLAs
- Carry out regular audits of the technical security of IT systems
- Provide information to external auditors and regulators, if required.

Maintain

The objectives of this maintain element of the ISMS are to:

- Improve security agreements as specified in, for example, SLAs and OLAs
- Improve the implementation of security measures and controls.

This should be achieved using a PDCA (Plan–Do–Check–Act) cycle, which is a formal approach suggested by ISO 27001 for the establishment of the Information Security Management System (ISMS) or framework. This cycle is described in more detail in the Continual Service Improvement publication.

Security governance

Information security governance, when properly implemented, should provide six basic outcomes:

- Strategic alignment:
 - Security requirements should be driven by enterprise requirements
 - Security solutions need to fit enterprise processes
 - Investment in information security should be aligned with the enterprise strategy and agreed-on risk profile.
- Value delivery:
 - A standard set of security practices, i.e. baseline security requirements following best practices
 - Properly prioritized and distributed effort to areas with greatest impact and business benefit
 - Institutionalized and commoditized solutions
 - Complete solutions, covering organization and process as well as technology
 - A culture of continual improvement.
- Risk management:
 - Agreed-on risk profile
 - Understanding of risk exposure
 - Awareness of risk management priorities
 - Risk mitigation
 - Risk acceptance/deference.

Performance Management:

- Defined, agreed and meaningful set of metrics
- Measurement process that will help identify shortcomings and provide feedback on progress made resolving issues
- Independent assurance.

Resource management:

- Knowledge is captured and available
- Documented security processes and practices
- Developed security architecture(s) to efficiently utilize infrastructure resources.

Business process assurance.

4.6.5 Process activities, methods and techniques

The purpose of the ISM process is to ensure that the security aspects with regard to services and all Service Management activities are appropriately managed and controlled in line with business needs and risks:

The key activities within the ISM process are:

- Production, review and revision of an overall Information Security Policy and a set of supporting specific policies
- Communication, implementation and enforcement of the security policies
- Assessment and classification of all information assets and documentation
- Implementation, review, revision and improvement of a set of security controls and risk assessment and responses
- Monitoring and management of all security breaches and major security incidents
- Analysis, reporting and reduction of the volumes and impact of security breaches and incidents
- Schedule and completion of security reviews, audits and penetration tests.

The interactions between these key activities are illustrated in Figure 4.27.

The developed Information Security Management processes, together with the methods, tools and techniques, constitute the security strategy. The security manager should ensure that technologies, products and services are in place and that the overall policy is developed and well published. The security manager is also responsible for security architecture, authentication, authorization, administration and recovery.

The security strategy also needs to consider how it will embed good security practices into every area of the business. Training and awareness are vital in the overall

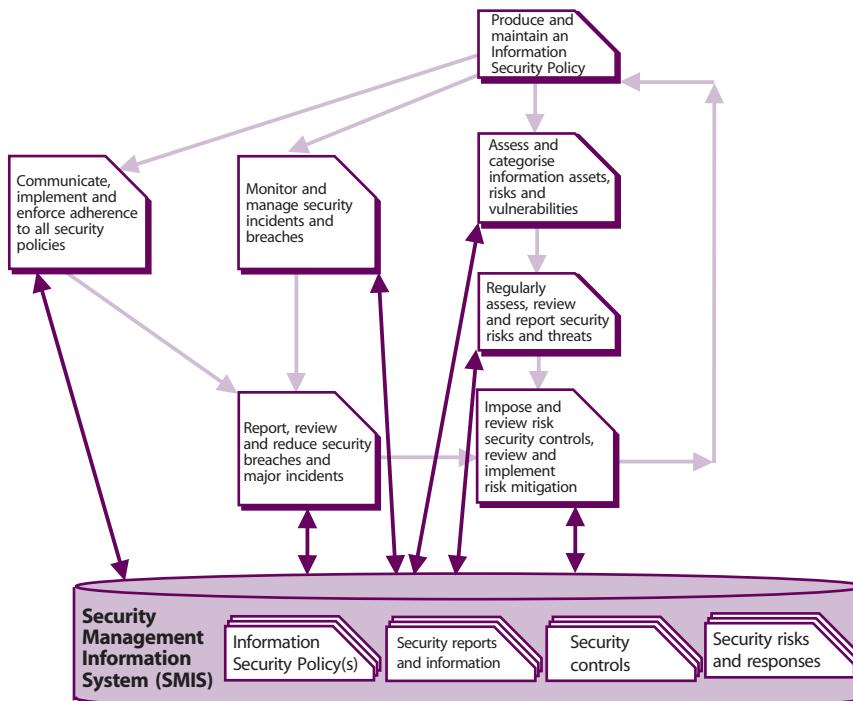


Figure 4.27 IT Security Management process

strategy, as security is often weakest at the end-user stage. It is here, as well, that there is a need to develop methods and processes that enable the policies and standards to be more easily followed and implemented.

Resources need to be assigned to track developments in these enabling technologies and the products they support. For example, privacy continues to be important and, increasingly, the focus of government regulation, making privacy compliance technologies an important enabling technology.

4.6.5.1 Security controls

The Information Security Manager must understand that security is not a step in the lifecycle of services and systems and that security cannot be solved through technology. Rather, information security must be an integral part of all services and systems and is an ongoing process that needs to be continuously managed using a set of security controls, as shown in Figure 4.28.

The set of security controls should be designed to support and enforce the Information Security Policy and to minimize all recognized and identified threats. The controls will be considerably more cost-effective if included within the design of all services. This will ensure the continued protection of all existing services and that new services and access to them are in line with the policy.

Security measures can be used at a specific stage in the prevention and handling of security incidents, as illustrated in Figure 4.28. Security incidents are not solely caused by technical threats – statistics show that, for example, the large majority stem from human errors (intended or not) or procedural errors, and often have implications in other fields such as safety, legal or health.

The following stages can be identified. At the start there is a risk that a threat will materialize. A threat can be anything that disrupts the business process or has negative impact on the business. When a threat

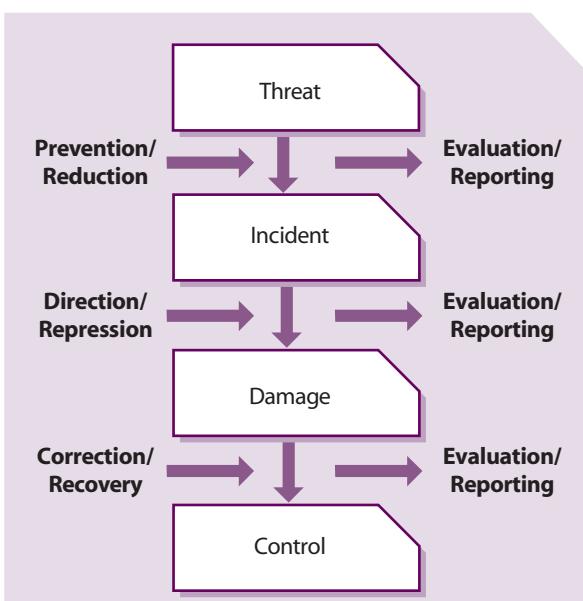


Figure 4.28 Security controls for threats and incidents

materializes, we speak of a security incident. This security incident may result in damage (to information or to assets) that has to be repaired or otherwise corrected. Suitable measures can be selected for each of these stages. The choice of measures will depend on the importance attached to the information.

- **Preventive:** security measures are used to prevent a security incident from occurring. The best-known example of preventive measures is the allocation of access rights to a limited group of authorized people. The further requirements associated with this measure include the control of access rights (granting, maintenance and withdrawal of rights), authorization (identifying who is allowed access to which information and using which tools), identification and authentication (confirming who is seeking access) and access control (ensuring that only authorized personnel can gain access).
- **Reductive:** further measures can be taken in advance to minimize any possible damage that may occur. These are 'reductive' measures. Familiar examples of reduction measures are making regular backups and the development, testing and maintenance of contingency plans.
- **Detective:** if a security incident occurs, it is important to discover it as soon as possible – detection. A familiar example of this is monitoring, linked to an alert procedure. Another example is virus-checking software.
- **Repressive:** measures are then used to counteract any continuation or repetition of the security incident. For example, an account or network address is temporarily blocked after numerous failed attempts to log on or the retention of a card when multiple attempts are made with a wrong PIN number.
- **Corrective:** The damage is repaired as far as possible using corrective measures. For example, corrective measures include restoring the backup, or returning to a previous stable situation (roll-back, back-out). Fallback can also be seen as a corrective measure.

The documentation of all controls should be maintained to reflect accurately their operation, maintenance and their method of operation.

4.6.5.2 Management of security breaches and incidents

In the case of serious security breaches or incidents, an evaluation is necessary in due course, to determine what went wrong, what caused it and how it can be prevented in the future. However, this process should not be limited

to serious security incidents. All breaches of security and security incidents need to be studied in order to gain a full picture of the effectiveness of the security measures as a whole. A reporting procedure for security incidents is required to be able to evaluate the effectiveness and efficiency of the present security measures based on an insight into all security incidents. This is facilitated by the maintenance of log files and audit files and, of course, the incident records of the Service Desk function. The analysis of these statistics on security issues should lead to improvement actions focused on the reduction of the impact and volume of all security breaches and incidents, in conjunction with Problem Management.

4.6.6 Triggers, inputs, outputs and interfaces

ISM activity can be triggered by many events. These include:

- New or changed corporate governance guidelines
- New or changed Business Security Policy
- New or changed corporate risk management processes and guidelines
- New or changed business needs or new or changed services
- New or changed requirements within agreements, such as SLRs, SLAs, OLAs or contracts
- Review and revision of business and IT plans and strategies
- Review and revision of designs and strategies
- Service or component security breaches or warnings, events and alerts, including threshold events, exception reports
- Periodic activities, such as reviewing, revising or reporting, including review and revision of ISM policies, reports and plans
- Recognition or notification of a change of risk or impact of a business process or VBF, an IT service or component
- Requests from other areas, particularly SLM for assistance with security issues.

The effective and efficient implementation of an Information Security Policy within an organization will, to a large extent, be dependent on good Service Management processes. Indeed, the effective implementation of some processes can be seen as a prerequisite for effective security control. The key interfaces that ISM has with other processes are as follows:

- Incident and Problem Management: in providing assistance with the resolution and subsequent justification and correction of security incidents and

- problems. The Incident Management process must include the ability to identify and deal with security incidents. Service Desk and Service Operations staff must 'recognize' a security incident.
- ITSCM: with the assessment of business impact and risk, and the provision of resilience, fail-over and recovery mechanisms. Security is a major issue when continuity plans are tested or invoked. A working ITSCM plan is a mandatory requirement for ISO 27001.
 - SLM: assistance with the determining of security requirements and responsibilities and their inclusion within SLRs and SLAs, together with the investigation and resolution of service and component security breaches.
 - Change Management: ISM should assist with the assessment of every change for impact on security and security controls. Also ISM can provide information on unauthorized changes.
 - Legal and HR issues must be considered when investigating security issues.
 - Configuration Management will give the ability to provide accurate asset information to assist with security classifications. Having an accurate CMS is therefore an extremely useful ISM input.
 - Security is often seen as an element of Availability Management, with Confidentiality Integrity and Availability (CIA) being the essence of Availability and ISM. Also, ISM should work with both Availability Management and ITSCM to conduct integrated Risk Analysis and Management exercises.
 - Capacity Management must consider security implications when selecting and introducing new technology. Security is an important consideration when procuring any new technology or software.
 - Financial Management should provide adequate funds to finance security requirements.
 - Supplier Management should assist with the joint management of suppliers and their access to services and systems, and the terms and conditions to be included within contracts concerning supplier responsibilities.

4.6.6.1 Inputs

Information Security Management will need to obtain input from many areas, including:

- Business information: from the organization's business strategy, plans and financial plans, and information on their current and future requirements.

- Corporate governance and business security policies and guidelines, security plans, Risk Analysis and responses
- IT information: from the IT strategy and plans and current budgets
- Service information: from the SLM process with details of the services from the Service Portfolio and the Service Catalogue and service level targets within SLAs and SLRs, and possibly from the monitoring of SLAs, service reviews and breaches of the SLAs
- Risk Analysis processes and reports: from ISM, Availability Management and ITSCM
- Details of all security events and breaches: from all areas of IT and SM, especially Incident Management and Problem Management
- Change information: from the Change Management process with a Change Schedule and a need to assess all changes for their impact on all security policies, plans and controls
- CMS: containing information on the relationships between the business, the services, supporting services and the technology
- Details of partner and supplier access: from Supplier Management and Availability Management on external access to services and systems.

4.6.6.2 Outputs

The outputs produced by the Information Security Management process are used in all areas and should include:

- An overall Information Security Management Policy, together with a set of specific security policies
- A Security Management Information System (SMIS), containing all the information relating to ISM
- Revised security risk assessment processes and reports
- A set of security controls, together with details of the operation and maintenance and their associated risks
- Security audits and audit reports
- Security test schedules and plans, including security penetration tests and other security tests and reports
- A set of security classifications and a set of classified information assets
- Reviews and reports of security breaches and major incidents
- Policies, processes and procedures for managing partners and suppliers and their access to services and information.

4.6.7 Key Performance Indicators

Many KPIs and metrics can be used to assess the effectiveness and efficiency of the ISM process and activities. These metrics need to be developed from the service, customer and business perspective such as:

- Business protected against security violations:
 - Percentage decrease in security breaches reported to the Service Desk
 - Percentage decrease in the impact of security breaches and incidents
 - Percentage increase in SLA conformance to security clauses.
- The determination of a clear and agreed policy, integrated with the needs of the business: decrease in the number of non-conformances of the ISM process with the business security policy and process.
- Security procedures that are justified, appropriate and supported by senior management:
 - Increase in the acceptance and conformance of security procedures
 - Increased support and commitment of senior management.
- A mechanism for improvement:
 - The number of suggested improvements to security procedures and controls
 - Decrease in the number of security non-conformance detected during audits and security testing.
- Information security is an integral part of all IT services and all ITSM processes: increase in the number of services and processes conformant with security procedures and controls.
- Effective marketing and education in security requirements, IT staff awareness of the technology supporting the services:
 - Increased awareness of the security policy and its contents, throughout the organization
 - Percentage increase in completeness of the technical Service Catalogue against IT components supporting the services
 - Service Desk supporting all services.

4.6.8 Information Management

All the information required by ISM should be contained within the SMIS. This should include all security controls, risks, breaches, processes and reports necessary to support and maintain the Information Security Policy and the ISMS. This information should cover all IT services and

components and needs to be integrated and maintained in alignment with all other IT information management systems, particularly the Service Portfolio and the CMS. The SMIS will also provide the input to security audits and reviews and to the continual improvement activities so important to all ISMSs. The SMIS will also provide invaluable input to the design of new systems and services.

4.6.9 Challenges, Critical Success Factors and risks

ISM faces many challenges in establishing an appropriate Information Security Policy with an effective supporting process and controls. One of the biggest challenges is to ensure that there is adequate support from the business, business security and senior management. If these are not available, it will be impossible to establish an effective ISM process. If there is senior IT management support, but there is no support from the business, IT security controls and risk assessment will be severely limited in what they can achieve because of this lack of support from the business. It is pointless implementing security policies, procedures and controls in IT if these cannot be enforced throughout the business. The major use of IT services and assets is outside of IT, and so are the majority of security threats and risks.

In some organizations the business perception is that security is an IT responsibility, and therefore the business assumes that IT will be responsible for all aspects of IT security and that IT services will be adequately protected. However, without the commitment and support of the business and business personnel, money invested in expensive security controls and procedures will be largely wasted and they will mostly be ineffective.

If there is a business security process established, then the challenge becomes one of alignment and integration. ISM must ensure that accurate information is obtained from the business security process on the needs, risks, impact and priorities of the business and that the ISM policies, information and plans are aligned and integrated with those of the business. Having achieved that alignment, the challenge becomes one of keeping them aligned by management and control of business and IT change using strict Change Management and Configuration Management control. Again, this requires support and commitment from the business and senior management.

The main CSFs for the ISM process are:

- Business protected against security violations
- The determination of a clear and agreed policy, integrated with the needs of the business

- Security procedures that are justified, appropriate and supported by senior management
- Effective marketing and education in security requirements
- A mechanism for improvement
- Information security is an integral part of all IT services and all ITSM processes
- The availability of services is not compromised by security incidents
- Clear ownership and awareness of the security policies amongst the customer community.

Information systems can generate many direct and indirect benefits, and as many direct and indirect risks. These risks have led to a gap between the need to protect systems and services and the degree of protection applied. The gap is caused by internal and external factors, including the widespread use of technology, increasing dependence of the business on IT, increasing complexity and interconnectivity of systems, disappearance of the traditional organizational boundaries and increasingly onerous regulatory requirements.

This means that there are new risk areas that could have a significant impact on critical business operations, such as:

- Increasing requirements for availability and robustness
- Growing potential for misuse and abuse of information systems affecting privacy and ethical values
- External dangers from hackers, leading to denial-of-service and virus attacks, extortion, industrial espionage and leakage of organizational information or private data.

Because new technology provides the potential for dramatically enhanced business performance, improved and demonstrated information security can add real value to the organization by contributing to interaction with trading partners, closer customer relationships, improved competitive advantage and protected reputation. It can also enable new and easier ways to process electronic transactions and generate trust. In today's competitive global economy, if an organization wants to do business, it may well be asked to present details of its security posture and results of its past performance in terms of tests conducted to ensure security of its information resources.

Other areas of major risks associated with ISM include:

- A lack of commitment from the business to the ISM processes and procedures
- Lack of commitment from the business and a lack of appropriate information on future plans and strategies

- A lack of senior management commitment or a lack of resources and/or budget for the ISM process
- The processes focus too much on the technology issues and not enough on the IT services and the needs and priorities of the business
- Risk assessment and management is conducted in isolation and not in conjunction with Availability Management and ITSCM
- ISM policies, plans, risks and information become out-of-date and lose alignment with the corresponding relevant information and plans of the business and business security.

4.7 SUPPLIER MANAGEMENT

4.7.1 Purpose/goal/objective

'The goal of the Supplier Management process is to manage suppliers and the services they supply, to provide seamless quality of IT service to the business, ensuring value for money is obtained.'

The Supplier Management process ensures that suppliers and the services they provide are managed to support IT service targets and business expectations. The aim of this section is to raise awareness of the business context of working with partners and suppliers, and how this work can best be directed toward realising business benefit for the organization.

It is essential that Supplier Management processes and planning are involved in all stages of the Service Lifecycle, from strategy and design, through transition and operation, to improvement. The complex business demands require the complete breadth of skills and capability to support provision of a comprehensive set of IT services to a business, therefore the use of value networks and the suppliers and the services they provide are an integral part of any end-to-end solution. Suppliers and the management of suppliers and partners are essential to the provision of quality IT services.

The purpose of the Supplier Management process is to obtain value for money from suppliers and to ensure that suppliers perform to the targets contained within their contracts and agreements, while conforming to all of the terms and conditions.

The main objectives of the Supplier Management process are to:

- Obtain value for money from supplier and contracts
- Ensure that underpinning contracts and agreements with suppliers are aligned to business needs, and

support and align with agreed targets in SLRs and SLAs, in conjunction with SLM

- Manage relationships with suppliers
- Manage supplier performance
- Negotiate and agree contracts with suppliers and manage them through their lifecycle
- Maintain a supplier policy and a supporting Supplier and Contract Database (SCD).

4.7.2 Scope

The Supplier Management process should include the management of all suppliers and contracts needed to support the provision of IT services to the business. Each service provider should have formal processes for the management of all suppliers and contracts. However, the processes should adapt to cater for the importance of the supplier and/or the contract and the potential business impact on the provision of services. Many suppliers provide support services and products that independently have a relatively minor, and fairly indirect, role in value generation, but collectively make a direct and important contribution to value generation and the implementation of the overall business strategy. The greater the contribution the supplier makes to business value, the more effort the service provider should put into the

management of the supplier and the more that supplier should be involved in the development and realization of the business strategy. The smaller the supplier's value contribution, the more likely it is that the relationship will be managed mainly at an operational level, with limited interaction with the business. It may be appropriate in some organizations, particularly large ones, to manage internal teams and suppliers, where different business units may provide support of key elements.

The Supplier Management process should include:

- Implementation and enforcement of the supplier policy
- Maintenance of a Supplier and Contract Database (SCD)
- Supplier and contract categorization and risk assessment
- Supplier and contract evaluation and selection
- Development, negotiation and agreement of contracts
- Contract review, renewal and termination
- Management of suppliers and supplier performance
- Agreement and implementation of service and supplier improvement plans
- Maintenance of standard contracts, terms and conditions

Service Provider

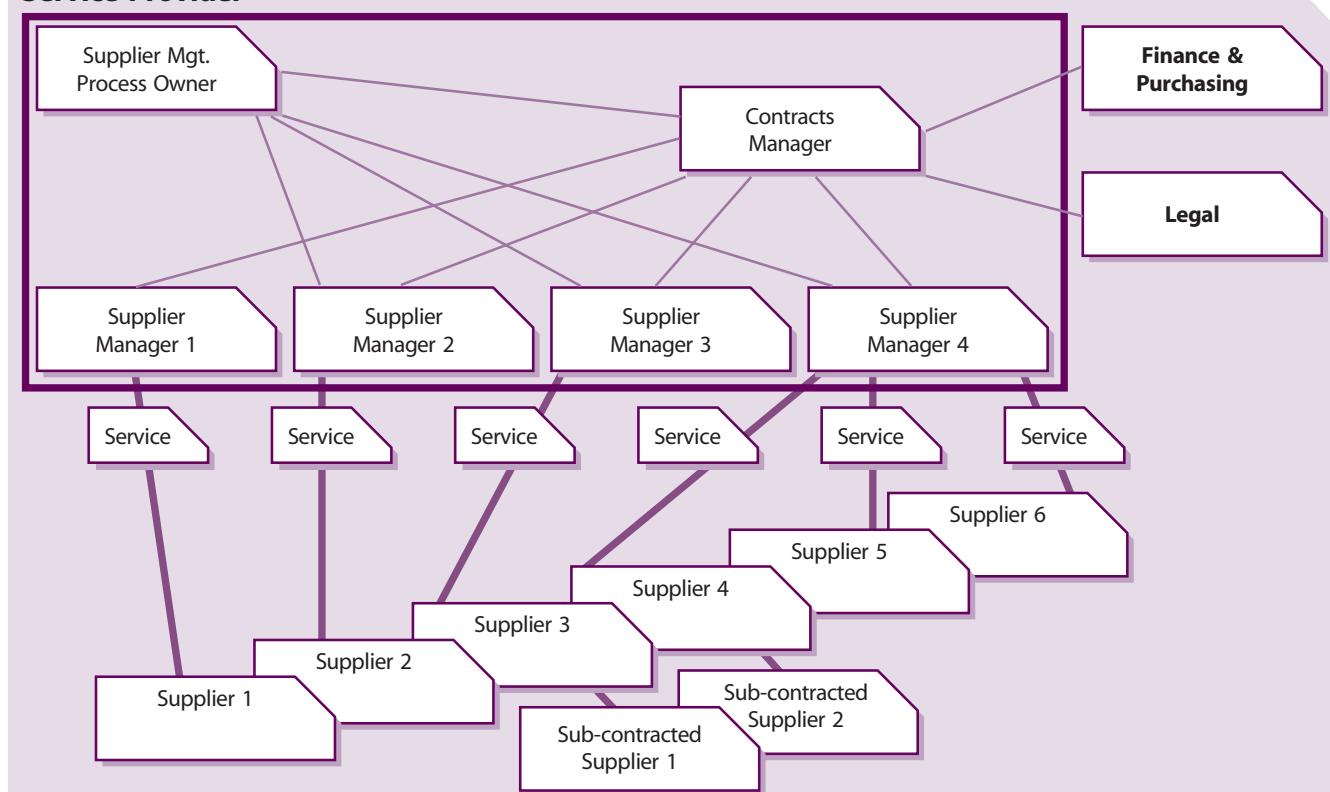


Figure 4.29 Supplier Management – roles and interfaces

- Management of contractual dispute resolution
- Management of sub-contracted suppliers.

IT Supplier Management often has to comply with organizational or corporate standards, guidelines and requirements, particularly those of corporate legal, finance and purchasing, as illustrated in Figure 4.29.

In order to ensure that suppliers provide value for money and meet their service targets, the relationship between each supplier should be owned by an individual within the service provider organization. However, a single individual may own the relationship for one or many suppliers, as illustrated in Figure 4.29. To ensure that relationships are developed in a consistent manner and that suppliers' performance is appropriately reviewed and managed, roles need to be established for a Supplier Management process owner and a Contracts Manager. In smaller organizations, these separate roles may be combined into a single responsibility.

4.7.3 Value to the business

The main objectives of the Supplier Management process are to provide value for money from suppliers and contracts and to ensure that all targets in underpinning supplier contracts and agreements are aligned to business needs and agreed targets within SLAs. This is to ensure the delivery to the business of end-to-end, seamless, quality IT services that are aligned to the business's expectation. The Supplier Management process should align with all

corporate requirements and the requirements of all other IT and SM processes, particularly ISM and ITSCM. This ensures that the business obtains value from supporting supplier services and that they are aligned with business needs.

4.7.4 Policies/principles/basic concepts

The Supplier Management process attempts to ensure that suppliers meet the terms, conditions and targets of their contracts and agreements, whilst trying to increase the value for money obtained from suppliers and the services they provide. All Supplier Management process activity should be driven by a supplier strategy and policy from Service Strategy. In order to achieve consistency and effectiveness in the implementation of the policy, a Supplier and Contracts Database (SCD) should be established, as illustrated in Figure 4.30, together with clearly defined roles and responsibilities.

Ideally the SCD should form an integrated element of a comprehensive CMS or SKMS, recording all supplier and contract details, together with details of the type of service(s) or product(s) provided by each supplier, and all other information and relationships with other associated CIs. The services provided by suppliers will also form a key part of the Service Portfolio and the Service Catalogue. The relationship between the supporting services and the IT and business services they support are key to providing quality IT services.

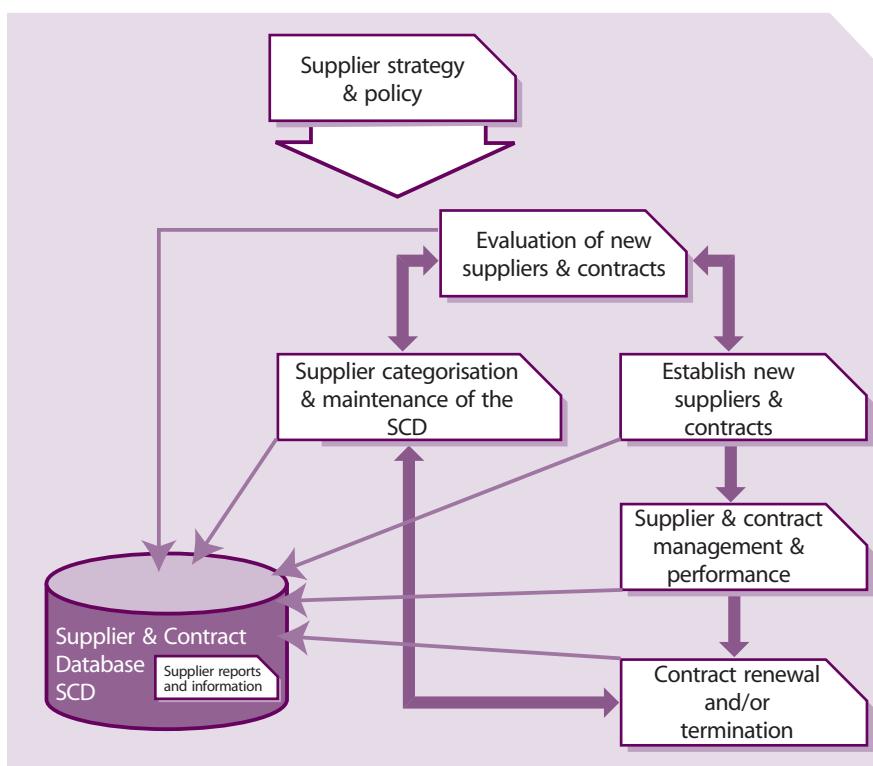


Figure 4.30 Supplier Management process

This information within the SCD will provide a complete set of reference information for all Supplier Management procedures and activities:

- Supplier categorization and maintenance of the Supplier and Contracts Database (SCD)
- Evaluation and set-up of new suppliers and contracts
- Establishing new suppliers
- Supplier and Contract Management and performance
- Contract renewal and termination.

The first two elements within the above list are covered within the Service Design stage. The third element is part of Service Transition, and the last two are part of the Service Operation stage and are covered in more detail in those publications.

4.7.5 Process activities, methods and techniques

This section provides more detail on the Supplier Management process, its sub-processes and activities, and the management of the contract lifecycle.

When dealing with external suppliers, it is strongly recommended that a formal contract with clearly defined, agreed and documented responsibilities and targets is established and managed through the stages of its lifecycle, from the identification of the business need to the operation and cessation of the contract:

- Identification of business need and preparation of the business case:
 - Produce a Statement of Requirement (SOR) and/or Invitation To Tender (ITT)
 - Ensure conformance to strategy/policy
 - Prepare the initial business case, including options (internal and external), costs, timescales, targets, benefits, risk assessment.
- Evaluation and procurement of new contracts and suppliers:
 - Identify method of purchase or procurement
 - Establish evaluation criteria – for example, services, capability (both personnel and organization), quality and cost
 - Evaluate alternative options
 - Select
 - Negotiate contracts, targets and the terms and conditions, including responsibilities, closure, renewal, extension, dispute, transfer
 - Agree and award the contract.

- Establish new suppliers and contracts:
 - Set up the supplier service and contract, within the SCD and any other associated corporate systems
 - Transition of service
 - Establish contacts and relationships.
- Supplier and contract categorization:
 - Assessment or reassessment of the supplier and contract
 - Ensure changes progressed through Service Transition
 - Categorization of the supplier
 - Update of SCD
 - Ongoing maintenance of the SCD.
- Manage the supplier and contract performance:
 - Management and control of the operation and delivery of service/products
 - Monitor and report (service, quality and costs)
 - Review and improve (service, quality and costs)
 - Management of the supplier and the relationship (communication, risks, changes, failures, improvements, contacts, interfaces)
 - Review, at least annually, service scope against business need, targets and agreements
 - Plan for possible closure/renewal/extension.
- End of term:
 - Review (determine benefits delivered, ongoing requirement)
 - Renegotiate and renew or terminate and/or transfer.

The business, IT, finance, purchasing and procurement need to work together to ensure that all stages of the contract lifecycle are managed effectively. All areas need to be jointly involved in selecting the solution and managing the ongoing performance of the supplier, with each area taking responsibility for the interests of their own area, whilst being aware of the implications on the organization as a whole. The processes involved in the stages of the contract lifecycle are explained in detail in the following sections.

4.7.5.1 Evaluation of new suppliers and contracts

The activities associated with the identification of business needs and the subsequent evaluation of new suppliers and contracts are part of the Service Design process. The outputs from this area provide the inputs to all other stages of the contract lifecycle. It is vital to the ongoing success of the contract and the relationship that the

business is closely involved in all aspects of these activities. Every organization should have templates and a formal method for the production of business cases and their approval and sign-off. The detailing of the business needs and the content of the business case should be agreed, approved and signed off by both the business and IT.

When selecting a new supplier or contract, a number of factors need to be taken into consideration, including track record, capability, references, credit rating and size relative to the business being placed. In addition, depending on the type of supplier relationship, there may be personnel issues that need to be considered. Each organization should have processes and procedures for establishing new suppliers and contracts.

While it is recognized that factors may exist that influence the decision on type of relationship or choice of supplier (e.g. politics within the organization, existing relationships), it is essential that in such cases the reasoning is identified and the impact fully assessed to ensure costly mistakes are avoided.

Services may be sourced from a single supplier or multi-sourced. Services are most likely to be sourced from two or more competing suppliers where the requirement is for standard services or products that are readily available 'off-the-shelf'. Multi-sourcing is most likely to be used where cost is the prime determinant, and requirements for developing variants of the services are low, but may also be undertaken to spread risk. Suppliers on a multi-source list may be designated with 'Preferred Supplier' status within the organization, limiting or removing scope for use of other suppliers.

Partnering relationships are established at an executive level and are dependent on a willingness to exchange strategic information to align business strategies. Many strategically important supplier relationships are now positioned as partnering relationships. This reflects a move away from traditionally hierarchical relationships, where the supplier acts subordinately to the customer organization, to one characterized by:

- **Strategic alignment:** good alignment of culture, values and objectives, leading to an alignment of business strategies
- **Integration:** a close integration of the processes of the two organizations
- **Information flow:** good communication and information exchange at all levels, especially at the strategic level, leading to close understanding
- **Mutual trust:** a relationship built on mutual trust between the organizations and their individuals

- **Openness:** when reporting on service performance, costs and Risk Analysis
- **Collective responsibility:** joint partnership teams taking collective responsibility for current performance and future development of the relationship
- **Shared risk and reward:** e.g. agreeing how investment costs and resultant efficiency benefits are shared, or how risks and rewards from fluctuations in material costs are shared.

Both parties derive benefits from partnering. An organization derives progressively more value from a supplier relationship as the supplier's understanding of the organization as a whole increases, from its IT inventory architectures through to its corporate culture, values and business objectives. With time, the supplier is able to respond more quickly and more appropriately to the organization's needs. The supplier benefits from a longer-term commitment from the organization, providing it with greater financial stability, and enabling it to finance longer-term investments, which benefit its customers.

A partnership makes it possible for the parties to align their IT infrastructures. Joint architecture and risk control agreements allow the partners to implement a range of compatible solutions from security, networking, data/information interchange, to workflow and application processing systems. This integration can provide service improvements and lowered costs. Such moves also reduce risks and costs associated with one-off tactical solutions, put in place to bridge a supplier's IT with that of the organization.

The key to a successful partnering relationship is being absolutely clear about the benefits and costs such a relationship will deliver before entering into it. Both parties then know what is expected of them at the outset. The success of the partnership may involve agreeing the transfer of staff to the partner or outsourcing organization as part of the agreement and relationship.

Service provider organizations should have documented and formal processes for evaluating and selecting suppliers based on:

- Importance and impact: the importance of the service to the business, provided by the supplier
- Risk: the risks associated with using the service
- Costs: the cost of the service and its provision.

Often other areas of the service provider organization, such as Legal, Finance and Purchasing, will get involved with this aspect of the process. Service provider organizations should have processes covering:

- Production of business case documents
- Production of SoR and Invitations to Tender or proposal documents
- Formal evaluation and selection of suppliers and contracts
- The inclusion of standard clauses, terms and conditions within contracts, including early termination, benchmarking, exit or transfer of contracts, dispute resolution, management of sub-contracted suppliers and normal termination
- Transitioning of new contracts and suppliers.

These processes may, and should be, different, based on the type, size and category of the supplier and the contract.

The nature and extent of an agreement depends on the relationship type and an assessment of the risks involved. A pre-agreement Risk Analysis is a vital stage in establishing any external supplier agreement. For each party, it exposes the risks that need to be addressed and needs to be as comprehensive as practical, covering a wide variety of risks, including financial, business reputation, operational, regulatory and legal.

A comprehensive agreement minimizes the risk of disputes arising from a difference of expectations. A flexible agreement, which adequately caters for its adaptation across the term of the agreement, is maintainable and supports change with a minimum amount of renegotiation.

The contents of a basic underpinning contract or service agreement are as follows:

- **Basic terms and conditions:** the term (duration) of the contract, the parties, locations, scope, definitions and commercial basis.
- **Service description and scope:** the functionality of the services being provided and its extent, along with constraints on the service delivery, such as performance, availability, capacity, technical interface and security. Service functionality may be explicitly defined, or in the case of well-established services, included by reference to other established documents, such as the Service Portfolio and the Service Catalogue.
- **Service standards:** the service measures and the minimum levels that constitute acceptable performance and quality, e.g. IT may have a performance requirement to respond to a request for a new desktop system in 24 hours, with acceptable service deemed to have occurred where this performance requirement is met in 95% of cases.

Service levels must be realistic, measurable and aligned to the organization's business priorities and underpin the agreed targets within SLRs and SLAs.

- **Workload ranges:** the volume ranges within which service standards apply, or for which particular pricing regimes apply.
- **Management Information (MI):** the data that must be reported by the supplier on operational performance – take care to ensure that MI is focused on the most important or headline reporting measures on which the relationship will be assessed. Key Performance Indicators (KPIs) and Balanced Scorecards (BSCs) may form the core of reported performance data.
- **Responsibilities and dependencies:** description of the obligations of the organization (in supporting the supplier in the service delivery efforts) and of the supplier (in its provision of the service), including communication, contacts and escalation.

An extended service agreement may also contain:

- Service debit and credit regime (incentives and penalties)
- Additional performance criteria.

The following gives a limited sample of the legal and commercial topics typically covered by a service or contractual agreement:

- Scope of services to be provided
- Service performance requirements
- Division and agreement of responsibilities
- Contact points, communication and reporting frequency and content
- Contract review and dispute resolution processes
- Price structure
- Payment terms
- Commitments to change and investment
- Agreement change process
- Confidentiality and announcements
- Intellectual property rights and copyright
- Liability limitations
- Termination rights of each party
- Obligations at termination and beyond.

The final form of an agreement, and some of the terminology, may be dictated by the views and preferences of the procurement and legal departments, or by specialist legal firms.

Tip

Seek legal advice when formalizing external supply agreements.

Formal contracts

Formal contracts are appropriate for external supply arrangements that make a significant contribution to the delivery and development of the business. Contracts provide for binding legal commitments between customer and supplier, and cover the obligations each organization has to the other from the first day of the contract, often extending beyond its termination. A contract is used as the basis for external supplier agreements where an enforceable commitment is required. High-value and/or strategic relationships are underpinned by a formal contract. The formality and binding nature of a contract are not at odds with the culture of a partnering agreement, but rather form the basis on which trust in the relationship may be founded.

A contract is likely to be structured with a main body containing the commercial and legal clauses, and with the elements of a service agreement, as described earlier, attached as schedules. Contracts may also include a number of other related documents as schedules, for example:

- Security requirements
- Business continuity requirements
- Mandated technical standards
- Migration plans (agreed pre-scheduled change)
- Disclosure agreements.

Most large organizations have procurement and legal departments specializing in sourcing contracts. Specialist legal firms may be employed to support the internal procurement and legal function when establishing significant formal contracts.

Underpinning agreements

In ITIL an SLA is defined as a 'written agreement between a service provider and the customer(s) that documents agreed service levels for a service'. Service providers should be aware that SLAs are widely used to formalize service-based relationships, both internally and externally, and that while conforming to the definition above, these agreements vary considerably in the detail covered.

Key message

The views of some organizations, such as the Chartered Institute of Purchase and Supply (CIPS) and various specialist lawyers, are that SLAs ought not to be used to manage external relationships unless they form part of an underlying contract. The Complete Guide to Preparing and Implementing Service Level Agreements (2001) emphasizes that a stand-alone SLA may not be legally enforceable but instead 'represents the goodwill and faith of the parties signing it'. Therefore it is in service providers' and suppliers' interests to ensure that SLAs are incorporated into an appropriate contractual framework that meets the ITIL objective that SLAs are binding agreements.

SLAs, underpinning agreements and contracts should be reviewed on a regular basis to ensure performance conforms to the service levels that have been agreed.

The organization is likely to be dependent on its own internal support groups to some extent. To be able to achieve SLA targets, it is advisable to have formal arrangements in place with these groups. Operational Level Agreements (OLAs) ensure that underpinning services support the business/IT SLA targets. OLAs focus on the operational requirements that the services need to meet. This is a non-contractual, service-oriented document describing services and service standards, with responsibilities and obligations where appropriate.

Just as with SLAs, it is important that OLAs are monitored to highlight potential problems. The Service Level Manager has the overall responsibility to review performance against targets so that action can be taken to remedy, and prevent future recurrence of, any OLA breaches. Depending on the size of the organization and variety of services, e.g. SLAs and OLAs, a Service Level Manager should take responsibility for their service or set of services.

4.7.5.2 Supplier categorization and maintenance of the Supplier and Contracts Database (SCD)

The Supplier Management process should be adaptive and spend more time and effort managing key suppliers than less important suppliers. This means that some form of categorization process should exist within the Supplier Management process to categorize the supplier and their importance to the service provider and the services provided to the business. Suppliers can be categorized in many ways, but one of the best methods for categorizing

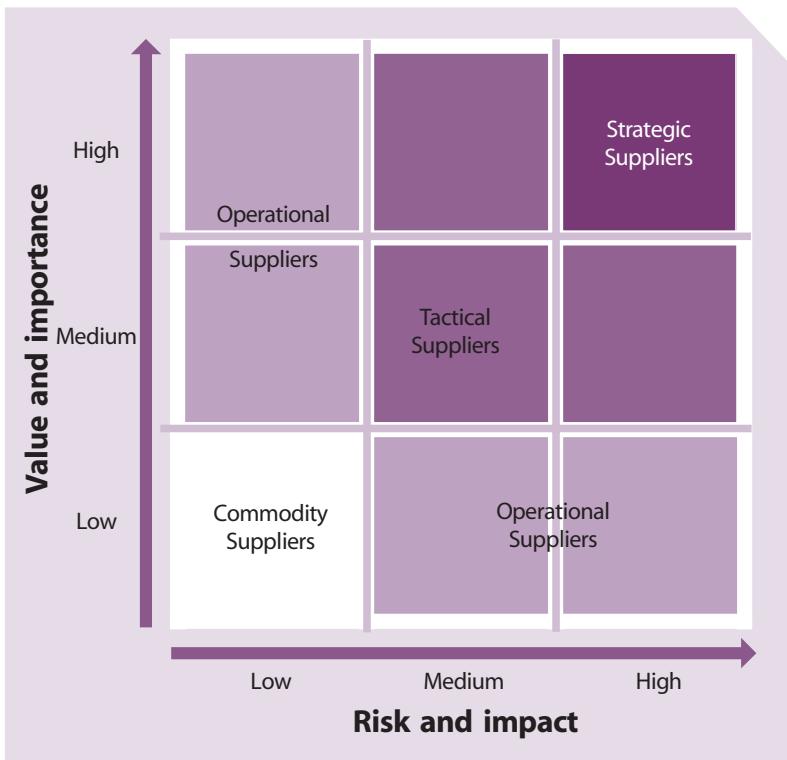


Figure 4.31 Supplier categorization

suppliers is based on assessing the risk and impact associated with using the supplier, and the value and importance of the supplier and their services to the business, as illustrated in Figure 4.31.

The amount of time and effort spent managing the supplier and the relationship can then be appropriate to its categorization:

- **Strategic:** for significant 'partnering' relationships that involve senior managers sharing confidential strategic information to facilitate long-term plans. These relationships would normally be managed and owned at a senior management level within the service provider organization, and would involve regular and frequent contact and performance reviews. These relationships would probably require involvement of Service Strategy and Service Design resources, and would include ongoing specific improvement programmes (e.g. a network service provider, supplying worldwide networks service and their support).

- **Tactical:** for relationships involving significant commercial activity and business interaction. These relationships would normally be managed by middle management and would involve regular contact and performance reviews, often including ongoing improvement programmes (e.g. a hardware maintenance organization providing resolution of server hardware failures).

- **Operational:** for suppliers of operational products or services. These relationships would normally be managed by junior operational management and would involve infrequent but regular contact and performance reviews (e.g. an internet hosting service provider, supplying hosting space for a low-usage, low-impact website or internally used IT service).
- **Commodity:** for suppliers that provide low-value and/or readily available products and services, which could be alternatively sourced relatively easily (e.g. paper or printer cartridge suppliers).

Strategically important supplier relationships are given the greatest focus. It is in these cases that Supplier Managers have to ensure that the culture of the service provider organization is extended into the supplier domain so that the relationship works beyond the initial contract. The rise in popularity of external sourcing, and the increase in the scope and complexity of some sourcing arrangements, has resulted in a diversification of types of supplier relationship. At a strategic level, it is important to understand the options that are available so that the most suitable type of supplier relationship can be established to gain maximum business benefit and evolves in line with business needs.

Tip

To successfully select the most appropriate type of supplier relationship, there needs to be a clear understanding of the business objectives that are to be achieved.

A number of factors, from the nature of the service to the overall cost, determine the importance of a supplier from a business perspective. As shown later, the greater the business significance of a supplier relationship, the more the business needs to be involved in the management and development of a relationship. A formal categorization approach can help to establish this importance.

The business value, measured as the contribution made to the business value chain, provides a more business-aligned assessment than pure contract price. Also, the more standard the services being procured, the lower the dependence the organization has on the supplier, and the more readily the supplier could be replaced (if necessary). Standardized services support the business through minimal time to market when deploying new or changed business services, and in pursuing cost-reduction strategies. More information on this subject can be found in the Service Strategy publication.

The more customized those services are, the greater the difficulty in moving to an alternative supplier.

Customization may benefit the business, contributing to competitive advantage through differentiated service, or may be the result of operational evolution.

Tailored services increase the dependence on the supplier, increase risk and can result in increased cost. From a supplier perspective, tailored services may decrease their ability to achieve economies of scale through common operations, resulting in narrowed margins, and reduced capital available for future investment.

Standard products and services are the preferred approach unless a clear business advantage exists, in which case a strategic supplier delivers the tailored service.

Tip

High-value or high-dependence relationships involve greater risks for the organization. These relationships need comprehensive contracts and active relationship management.

Having established the type of supplier, the relationship then needs to be formalized. In the discussion below, the term 'agreement' is used generically to refer to any formalization of a relationship between customer and supplier organizations, and may range from the informal

to comprehensive legally binding contracts. Simple, low-value relationships may be covered by a supplier's standard terms and conditions, and be managed wholly by IT. A relationship of strategic importance to the business, on the other hand, requires a comprehensive contract that ensures that the supplier supports evolving business needs throughout the life of the contract. A contract needs to be managed and developed in conjunction with procurement and legal departments and business stakeholders.

Tips

The agreement is the foundation for the relationship. The more suitable and complete the agreement, the more likely it is that the relationship will deliver business benefit to both parties.

The quality of the relationship between the service provider and their supplier(s) is often dependent on the individuals involved from both sides. It is therefore vital that individuals with the right attributes, skills, competences and personalities are selected to be involved in these relationships.

A business service may depend on a number of internal and/or external suppliers for its delivery. These may include a mixture of strategic suppliers and commodity suppliers. Some suppliers supply directly to the organization; others are indirect or sub-contracted suppliers working via another supplier. Direct suppliers are directly managed by the service provider; indirect or sub-contracted suppliers are managed by the leading supplier. Any one supplier may provide products or services used to support a number of different business services.

Supply chain analysis shows the mapping between business services and supplier services. Analysis of business processes will reveal the suppliers involved in each process and the points of hand-off between them. Management of the supply chain ensures that functional boundaries and performance requirements are clearly established for each supplier to ensure that overall business service levels are achieved. Business services are most likely to meet their targets consistently where there are a small number of suppliers in the supply chain, and where the interfaces between the suppliers in the chain are limited, simple and well-defined.

Reducing the number of direct suppliers reduces the number of relationships that need to be managed, the number of peer-to-peer supplier issues that need to be resolved, and reduces the complexity of the Supplier Management activities. Some organizations may

successfully reduce or collapse the whole supply chain around a single service provider, often referred to as a 'prime' supplier. Facilities management is often outsourced to a single specialist partner or supplier, who may in turn subcontract restaurant services, vending machine maintenance and cleaning.

Outsourcing entire business services to a single 'prime supplier' may run additional risks. For these reasons, organizations need to consider carefully their supply chain strategies ahead of major outsourcing activity. The scope of outsourced services needs to be considered to reduce the number of suppliers, whilst ensuring that risk is managed and it fits with typical competencies in the supply market.

The SCD is a database containing details of the organization's suppliers, together with details of the products and services that they provide to the business (e.g. e-mail service, PC supply and installation, Service Desk), together with details of the contracts. The SCD contains supplier details, a summary of each product/service (including support arrangements), information on the ordering process and, where applicable, contract details. Ideally the SCD should be contained within the overall CMS.

SCDs are beneficial because they can be used to promote preferred suppliers and to prevent purchasing of unapproved or incompatible items. By coordinating and controlling the buying activity, the organization is more likely to be able to negotiate preferential rates.

4.7.5.3 Establishing new suppliers and contracts

Adding new suppliers or contracts to the SCD needs to be handled via the Change Management process, to ensure that any impact is assessed and understood. In most organizations, the SCD is owned by the Supplier Management process or the procurement or purchasing department. The SCD provides a single, central focal set of information for the management of all suppliers and contracts.

Risk management, working with suppliers, centres on assessing vulnerabilities in each supplier arrangement or contract that pose threats to any aspect of the business, including business impact, probability, customer satisfaction, brand image, market share, profitability, share price or regulatory impacts or penalties (in some industries).

The nature of the relationship affects the degree of risk to the business. Risks associated with an outsourced or

strategic supplier are likely to be greater in number, and more complex to manage, than with internal supply. It is rarely possible to 'outsource' risk, although sometimes some of the risk may be transferred to the outsourcing organization. Blaming a supplier does not impress customers or internal users affected by a security incident or a lengthy system failure. New risks arising from the relationship need to be identified and managed, with communication and escalation as appropriate.

A substantial risk assessment should have been undertaken pre-contract, but this needs to be maintained in the light of changing business needs, changes to the contract scope, or changes in the operational environment.

The service provider organization and the supplier must consider the threats posed by the relationship to their own assets, and have their own risk profile. Each must identify their respective risk owners. In a well-functioning relationship, it is possible for much or all of the assessment to be openly shared with the other party. By involving supplier experts in risk assessments, especially in Operational Risk Assessments (ORAs), the organization may gain valuable insights into how best to mitigate risks, as well as improving the coverage of the assessment.

When evaluating risks of disruption to business services or functions, the business may have different priorities for service/function restoration. Business Impact Analysis (BIA) is a method used to assess the impacts on different areas of the business, resulting from a loss of service. Risk assessment and BIA activities relating to suppliers and contracts should be performed in close conjunction with Service Continuity Management, Availability Management and Information Security Management, with a view to reducing the impact and probability of service failure as a result of supplier or supplier service failure.

Once these activities have been completed and the supplier and contract information has been input into the SCD, including the nominated individuals responsible for managing the new supplier and/or contracts, frequency of service/supplier review meetings and contractual review meetings needs to be established, with appropriate break points, automated thresholds and warnings in place. The introduction of new suppliers and contracts should be handled as major changes through transition and into operation. This will ensure that appropriate contacts and communication points are established.

4.7.5.4 Supplier and Contract Management and performance

At an operational level, integrated processes need to be in place between an organization and its suppliers to ensure efficient day-to-day working practices. For example:

- Is the supplier expected to conform to the organization's Change Management process or any other processes?
- How does the Service Desk notify the supplier of incidents?
- How is CMS information updated when Cls change as a result of supplier actions? Who is responsible?

There may be a conflict of interest between the service provider organization and their supplier, especially with regard to the Change Management, Incident Management, Problem Management and Configuration Management processes. The supplier may want to use their processes and systems, whereas the service provider organization will want to use their own processes and systems. If this is the case, clear responsibilities and interfaces will need to be defined and agreed.

These and many other areas need to be addressed to ensure smooth and effective working at an operational level. To do so, all touch points and contacts need to be identified and procedures put in place so that everyone understands their roles and responsibilities. This should include identification of the single, nominated individual responsible for ownership of each supplier and contract. However, an organization should take care not to automatically impose its own processes, but to take the opportunity to learn from its suppliers.

Example

A contract had been awarded for a customized Stores Control System for which the organization's IT department had developed processes to support the live service once it was installed. This included procedures for recording and documenting work done on the service by field engineers (e.g. changes, repairs, enhancement and reconfigurations). At a project progress meeting, the supplier confirmed that they had looked at the procedures and could follow them if required. However, having been in this situation many times before, they had already developed a set of procedures to deal with such events. These procedures were considerably more elegant, effective and easier to follow than those developed and proposed by the organization.

In addition to process interfaces, it is essential to identify how issues are handled at an operational level. By having clearly defined and communicated escalation routes, issues are likely to be identified and resolved earlier, minimizing the impact. Both the organization and the supplier benefit from the early capture and resolution of issues.

Both sides should strive to establish good communication links. The supplier learns more about the organization's business, its requirements and its plans, helping the supplier to understand and meet the organization's needs. In turn, the organization benefits from a more responsive supplier who is aware of the business drivers and any issues, and is therefore more able to provide appropriate solutions. Close day-to-day links can help each party to be aware of the other's culture and ways of working, resulting in fewer misunderstandings and leading to a more successful and long-lasting relationship.

Two levels of formal review need to take place throughout the contract lifecycle to minimize risk and ensure the business realizes maximum benefit from the contract:

- **Service/supplier performance reviews:** reports on performance should be produced on a regular basis, based on the category of supplier, and should form the basis of service review meetings. The more important the supplier, the more frequent and extensive the reports and reviews should be
- **Service, service scope and contract reviews:** these should also be conducted on a regular basis, at least annually for all major suppliers. The objective of these should be to review the service, overall performance, service scope and targets and the contract, together with any associated agreements. This should be compared with the original business needs and the current business needs to ensure that supplier and contracts remain aligned to business needs and continue to deliver value for money.

Formal performance review meetings must be held on a regular basis to review the supplier's performance against service levels, at a detailed operational level. These meetings provide an opportunity to check that the ongoing service performance management remains focused on supporting business needs. Typical topics include:

- Service performance against targets
- Incident and problem reviews, including any escalated issues
- Business and customer feedback

- Expected major changes that will (or may) affect service during the next service period, as well as failed changes and changes that caused incidents
- Key business events over the next service period that need particular attention from the supplier (e.g. quarter-end processing)
- Best practice and Service Improvement Programmes (SIPs).

Major service improvement initiatives and actions are controlled through SIPs with each supplier, including any actions for dealing with any failures or weaknesses.

Progress of existing SIPs, or the need for a new initiative, is reviewed at service review meetings. Proactive or forward-thinking organizations not only use SIPs to deal with failures but also to improve a consistently achieved service. It is important that a contract provides suitable incentives to both parties to invest in service improvement. These aspects are covered in more detail in the Continual Service Improvement publication.

The governance mechanisms for suppliers and contracts are drawn from the needs of appropriate stakeholders at different levels within each organization, and are structured so that the organization's representatives face-off to their counterparts in the supplier's organization. Defining the responsibilities for each representative, meeting forums and processes ensure that each person is involved at the right time in influencing or directing the right activities.

The scale and importance of the service and/or supplier influence the governance arrangements needed. The more significant the dependency, the greater the commitment and effort involved in managing the relationship. The effort needed on the service provider side to govern an outsourcing contract should not be underestimated, especially in closely regulated industries, such as the finance and pharmaceutical sectors.

A key objective for Supplier Management is to ensure that the value of a supplier to the organization is fully realized. Value is realized through all aspects of the relationship, from operational performance assurance, responsiveness to change requests and demand fluctuations, through to contribution of knowledge and experience to the organization's capability. The service provider must also ensure that the supplier's priorities match the business's priorities. The supplier must understand which of its service levels are most significant to the business.

Example

A large multi-national company had software agreements in place with the same supplier in no less than 24 countries. By arranging a single global licensing deal with the supplier, the company made annual savings of £5,000,000.

To ensure that all activities and contacts for a supplier are consistent and coordinated, each supplier relationship should have a single nominated individual accountable for all aspects of the relationship.

Example

A nationwide retail organization had an overall individual owning the management of their major network services supplier. However, services, contracts and billing were managed by several individuals spread throughout the organization. The individual owner put forward a business case for single ownership of the supplier and all the various contracts, together with consolidation of all the individual invoices into a single quarterly bill. The estimated cost savings to the organization were in excess of £600,000 per annum.

Satisfaction surveys also play an important role in revealing how well supplier service levels are aligned to business needs. A survey may reveal instances where there is dissatisfaction with the service, yet the supplier is apparently performing well against its targets (and vice versa). This may happen where service levels are inappropriately defined and should result in a review of the contracts, agreements and targets. Some service providers publish supplier league tables based on their survey results, stimulating competition between suppliers.

For those significant supplier relationships in which the business has a direct interest, both the business (in conjunction with the procurement department) and IT will have established their objectives for the relationship, and defined the benefits they expect to realize. This forms a major part of the business case for entering into the relationship.

These benefits must be linked and complementary, and must be measured and managed. Where the business is seeking improvements in customer service, IT supplier relationships contributing to those customer services must be able to demonstrate improved service in their own domain, and how much this has contributed to improved customer service.

For benefits assessments to remain valid during the life of the contract, changes in circumstances that have occurred since the original benefits case was prepared must be taken into account. A supplier may have been selected on its ability to deliver a 5% saving of annual operational cost compared with other options, but after two years has delivered no savings. However, where this is due to changes to contract, or general industry costs that would have also affected the other options, it is likely that a relative cost saving is still being realized. A maintained benefits case shows that saving.

Benefits assessments often receive lower priority than cost-saving initiatives, and are given less priority in performance reports than issues and problem summaries, but it is important to the long-term relationship that achievements are recognized. A benefits report must make objective assessments against the original objectives, but may also include morale-boosting anecdotal evidence of achievements and added value.

Tip

It is important for both organizations, and for the longevity of the relationship, that the benefits being derived from the relationship are regularly reviewed and reported.

An assessment of the success of a supplier relationship, from a business perspective, is likely to be substantially based on financial performance. Even where a service is performing well, it may not be meeting one or both parties' financial targets. It is important that both parties continue to benefit financially from the relationship. A contract that squeezes the margins of a supplier too tightly may lead to under-investment by the supplier, resulting in a gradual degradation of service, or even threaten the viability of supplier. In either case this may result in adverse business impacts to the organization.

The key to the successful long-term Financial Management of the contract is a joint effort directed towards maintaining the financial equilibrium, rather than a confrontational relationship delivering short-term benefits to only one party.

Building relationships takes time and effort. As a result, the organization may only be able to build long-term relationships with a few key suppliers. The experience, culture and commitment of those involved in running a supplier relationship are at least as important as having a good contract and governance regime. The right people with the right attitudes in the relationship team can make a poor contract work, but a good contract does not ensure that a poor relationship team delivers.

A considerable amount of time and money is normally invested in negotiating major supplier deals, with more again at risk for both parties if the relationship is not successful. Both organizations must ensure that they invest suitably in the human resources allocated to managing the relationship. The personality, behaviours and culture of the relationship representatives all influence the relationship. For a partnering relationship, all those involved need to be able to respect and work closely and productively with their opposite numbers.

4.7.5.5 Contract renewal and/or termination

Contract reviews must be undertaken on a regular basis to ensure the contract is continuing to meet business needs. Contract reviews assess the contract operation holistically and at a more senior level than the service reviews that are undertaken at an operational level. These reviews should consider:

- How well the contract is working and its relevance for the future
- Whether changes are needed: services, products, contracts, agreements, targets
- What is the future outlook for the relationship – growth, shrinkage, change, termination, transfer, etc?
- Commercial performance of the contract, reviews against benchmarks or market assessments, suitability of the pricing structure and charging arrangements
- Guidance on future contract direction and ensuring best practice management processes are established
- Supplier and contract governance.

For high-value, lengthy or complex supply arrangements, the period of contract negotiation and agreement can be lengthy, costly and may involve a protracted period of negotiation. It can be a natural inclination to wish to avoid further changes to a contract for as long as possible. However, for the business to derive full value from the supplier relationship, the contract must be able to be regularly and quickly amended to allow the business to benefit from service developments.

Benchmarking provides an assessment against the marketplace. The supplier may be committed by the contract to maintaining charges against a market rate. To maintain the same margin, the supplier is obliged to improve its operational efficiency in line with its competitors. Collectively, these methods help provide an assessment of an improving or deteriorating efficiency.

The point of responsibility within the organization for deciding to change a supplier relationship is likely to depend on the type of relationship. The service provider

may have identified a need to change supplier, based on the existing supplier's performance, but for a contractual relationship the decision needs to be taken in conjunction with the organization's procurement and legal departments.

The organization should take careful steps to:

- Perform a thorough impact and Risk Analysis of a change of supplier on the organization and its business, especially during a period of transition. This could be particularly significant in the case of a strategic relationship.
- Make a commercial assessment of the exit costs. This may include contractual termination costs if supplier liability is not clear, but the largest costs are likely to be associated with a transition project. For any significant-sized relationship, this typically includes a period of dual-supply as services are migrated. Any change associated with a change in supplier will increase costs, either immediately as fixed costs, or over time where borne by the supplier and reflected back in service charges.
- Take legal advice on termination terms, applicable notice period and mechanisms, and any other consequences, particularly if the contract is to be terminated early.
- Reassess the market to identify potential benefits in changing supplier.

A prudent organization undertakes most of these steps at the time the original contract is established, to ensure the right provisions and clauses are included, but this review activity needs to be reassessed when a change of supplier is being considered.

4.7.6 Triggers, inputs, outputs and interfaces

There are many events that could trigger Supplier Management activity. These include:

- New or changed corporate governance guidelines
- New or changed business and IT strategies, policies or plans
- New or changed business needs or new or changed services
- New or changed requirements within agreements, such as SLRs, SLAs, OLAs or contracts
- Review and revision of designs and strategies
- Periodic activities such as reviewing, revising or reporting, including review and revision of Supplier Management policies, reports and plans

- Requests from other areas, particularly SLM and Security Management, for assistance with supplier issues
- Requirements for new contracts, contract renewal or contract termination
- Re-categorization of suppliers and/or contracts.

The key interfaces that Supplier Management has with other processes are:

- ITSM: with regard to the management of continuity service suppliers.
- SLM: assistance with the determining of targets, requirements and responsibilities and their inclusion within underpinning agreements and contracts to ensure that they support all SLR and SLA targets. Also the investigation of SLA and SLR breaches caused by poor supplier performance.
- ISM: in the management of suppliers and their access to services and systems, and their responsibilities with regard to conformance to ISM policies and requirements.
- Financial Management: to provide adequate funds to finance Supplier Management requirements and contracts and to provide advice and guidance on purchase and procurement matters.
- Service Portfolio Management: to ensure that all supporting services and their details and relationships are accurately reflected within the Service Portfolio.

4.7.6.1 Inputs

- **Business information:** from the organization's business strategy, plans and financial plans, and information on their current and future requirements
- **Supplier and contracts strategy:** this covers the sourcing policy of the service provider and the types of suppliers and contracts used. It is produced by the Service Strategy processes
- **Supplier plans and strategies:** details of the business plans and strategies of suppliers, together with details of their technology developments and plans and statements and information on their current financial status and projected business viability
- **Supplier contracts, agreements and targets:** of both existing and new contracts and agreements from suppliers
- **Supplier and contract performance information:** of both existing and new contracts and suppliers
- **IT information:** from the IT strategy and plans and current budgets

- **Performance issues:** the Incident and Problem Management processes, with incidents and problems relating to poor contract or supplier performance
- **Financial information:** from Financial Management, the cost of supplier service(s) and service provision, the cost of contracts and the resultant business benefit and the financial plans and budgets, together with the costs associated with service and supplier failure
- **Service information:** from the SLM process, with details of the services from the Service Portfolio and the Service Catalogue, service level targets within SLAs and SLRs, and possibly from the monitoring of SLAs, service reviews and breaches of the SLAs. Also customer satisfaction data on service quality
- **CMS:** containing information on the relationships between the business, the services, the supporting services and the technology.

4.7.6.2 Outputs

The outputs of Supplier Management are used within all other parts of the process, by many other processes and by other parts of the organization. Often this information is supplied as electronic reports or displays on shared areas or as pages on intranet servers to ensure the most up-to-date information is always used. The information provided is as follows:

- **The Supplier and Contracts Database (SCD):** holds the information needed by all sub-processes within Supplier Management – for example, the data monitored and collected as part of Supplier Management. This is then invariably used as an input to all other parts of the Supplier Management process.
- **Supplier and contract performance information and reports:** used as input to supplier and contract review meetings to manage the quality of service provided by suppliers and partners. This should include information on shared risk where appropriate.
- **Supplier and contract review meeting minutes:** produced to record the minutes and actions of all review meetings with suppliers.
- **Supplier Service Improvement Plans (SIPs):** used to record all improvement actions and plans agreed between service providers and their suppliers, wherever they are needed, and should be used to manage the progress of agreed improvement actions, including risk reduction measures.
- **Supplier survey reports:** often many people within a service provider organization have dealings with suppliers. Feedback from these individuals should be collated to ensure that consistency in the quality of

service provided by suppliers is provided in all areas. These can be published as league tables to encourage competition between suppliers.

4.7.7 Key Performance Indicators

Many KPIs and metrics can be used to assess the effectiveness and efficiency of the Supplier Management process and activities. These metrics need to be developed from the service, customer and business perspective, such as:

- Business protected from poor supplier performance or disruption:
 - Increase in the number of suppliers meeting the targets within the contract
 - Reduction in the number of breaches of contractual targets.
- Supporting services and their targets align with business needs and targets:
 - Increase in the number of service and contractual reviews held with suppliers
 - Increase in the number of supplier and contractual targets aligned with SLA and SLR targets.
- Availability of services is not compromised by supplier performance:
 - Reduction in the number of service breaches caused by suppliers
 - Reduction in the number of threatened service breaches caused by suppliers.
- Clear ownership and awareness of supplier and contractual issues:
 - Increase in the number of suppliers with nominated supplier managers
 - Increase in the number of contracts with nominated contract managers.

4.7.8 Information Management

All the information required by Supplier Management should be contained within the SCD. This should include all information relating to suppliers and contracts, as well as all the information relating to the operation of the supporting services provided by suppliers. Information relating to these supporting services should also be contained within the Service Portfolio, together with the relationships to all other services and components. This information should be integrated and maintained in alignment with all other IT information management systems, particularly the Service Portfolio and the CMS.

4.7.9 Challenges, Critical Success Factors and risks

Supplier Management faces many challenges, which could include some of the following:

- Continually changing business and IT needs and managing significant change in parallel with delivering existing service
- Working with an imposed non-ideal contract, a contract that has poor targets or terms and conditions, or poor or non-existent definition of service or supplier performance targets
- Legacy issues, especially with services recently outsourced
- Insufficient expertise retained within the organization
- Being tied into long-term contracts, with no possibility of improvement, which have punitive penalty charges for early exit
- Situations where the supplier depends on the organization in fulfilling the service delivery (e.g. for a data feed) can lead to issues over accountability for poor service performance
- Disputes over charges
- Interference by either party in the running of the other's operation
- Being caught in a daily fire-fighting mode, losing the proactive approach
- Communication – not interacting often enough or quick enough or focusing on the right issues
- Personality conflicts
- One party using the contract to the detriment of the other party, resulting in win-lose changes rather than joint win-win changes
- Losing the strategic perspective, focusing on operational issues, causing a lack of focus on strategic relationship objectives and issues.

Key elements that can help to avoid the above issues are:

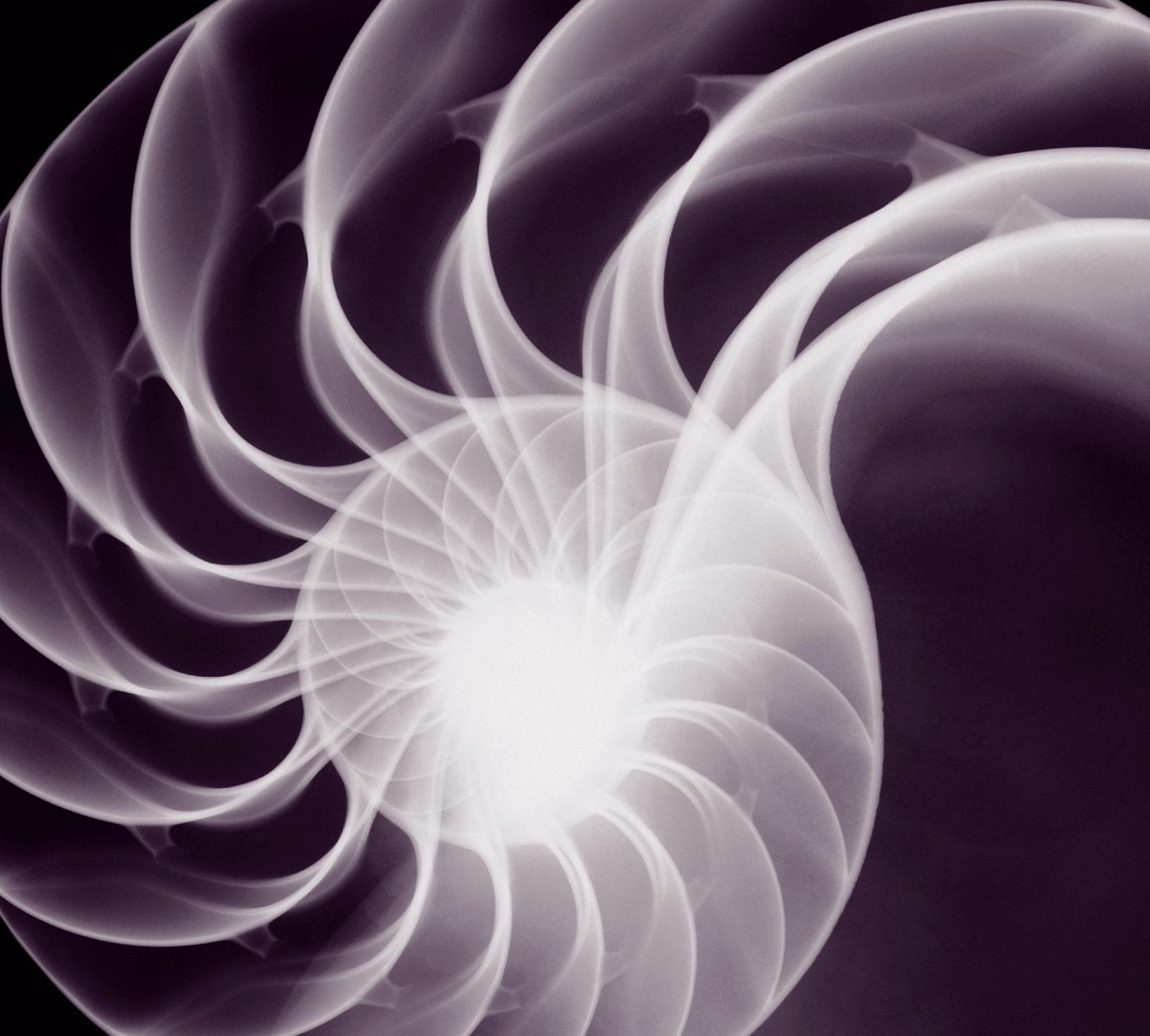
- Clearly written, well-defined and well-managed contract
- Mutually beneficial relationship
- Clearly defined (and communicated) roles and responsibilities on both sides
- Good interfaces and communications between the parties
- Well-defined Service Management processes on both sides
- Selecting suppliers who have achieved certification against internationally recognized certifications, such as ISO 9001, ISO/IEC 20000, etc.

The main CSFs for the Supplier Management process are:

- Business protected from poor supplier performance or disruption
- Supporting services and their targets align with business needs and targets
- Availability of services is not compromised by supplier performance
- Clear ownership and awareness of supplier and contractual issues.

The major areas of risk associated with Supplier Management include:

- Lack of commitment from the business and senior management to the Supplier Management process and procedures
- Lack of appropriate information on future business and IT policies, plans and strategies
- Lack of resources and/or budget for the ISM process
- Legacy of badly written and agreed contracts that don't underpin or support business needs or SLA and SLR targets
- Suppliers agree to targets and service levels within contracts that are impossible to meet, or suppliers fail or are incapable of meeting the terms and conditions of the contract
- Supplier personnel or organizational culture are not aligned to that of the service provider or the business
- Suppliers are not cooperative and are not willing to partake in and support the required Supplier Management process
- Suppliers are taken over and relationships, personnel and contracts are changed
- The demands of corporate supplier and contract procedures are excessive and bureaucratic
- Poor corporate financial processes, such as procurement and purchasing, do not support good Supplier Management.



Service Design
technology-related
activities

5

5 Service Design technology-related activities

This chapter considers the technology-related activities of requirement engineering and the development of technology architectures. The technology architectures cover aspects of Service Design in the following areas:

- Infrastructure Management
- Environmental Management
- Data and Information Management
- Application Management.

5.1 REQUIREMENTS ENGINEERING

Requirements engineering is the approach by which sufficient rigour is introduced into the process of understanding and documenting the business and user's requirements, and ensuring traceability of changes to each requirement. This process comprises the stages of elicitation, analysis (which feeds back into the elicitation) and validation. All these contribute to the production of a rigorous, complete requirements document. The core of this document is a repository of individual requirements that is developed and managed. Often these requirements are instigated by IT but ultimately they need to be documented and agreed with the business.

There are many guidelines on requirements engineering, including the Recommended Practice for Software Requirements Specifications (IEEE 830), The Software Engineering Body of Knowledge (SWEBOK), CMMI and the V-Model, which is described in detail in the Service Transition publication.

5.1.1 Different requirement types

A fundamental assumption here is that the analysis of the current and required business processes results in functional requirements met through IT services (comprising applications, data, infrastructure, environment and support skills).

It is important to note that there are commonly said to be three major types of requirements for any system – functional requirements, management and operational requirements, and usability requirements.

- Functional requirements are those specifically required to support a particular business function.
- Management and operational requirements (sometimes referred to as non-functional requirements) address the need for a responsive, available and

secure service, and deal with such issues as ease of deployment, operability, management needs and security.

- Usability requirements are those that address the 'look and feel' needs of the user and result in features of the service that facilitate its ease of use. This requirement type is often seen as part of management and operational requirements, but for the purposes of this section it will be addressed separately.

5.1.1.1 Functional requirements

Functional requirements describe the things a service is intended to do, and can be expressed as tasks or functions that the component is required to perform. One approach for specifying functional requirements is through such methods as a system context diagram or a use case model. Other approaches show how the inputs are to be transformed into the outputs (data flow or object diagrams) and textual descriptions.

A system context diagram, for instance, captures all information exchanges between, on the one hand, the IT service and its environment and, on the other, sources or destinations of data used by the service. These information exchanges and data sources represent constraints on the service under development.

A use case model defines a goal-oriented set of interactions between external actors and the service under consideration. Actors are parties outside the service that interact with the service. An actor may reflect a class of user's roles that users can play, or other services and their requirements. The main purpose of use case modelling is to establish the boundary of the proposed system and fully state the functional capabilities to be delivered to the users. Use cases are also helpful for establishing communication between business and application developers. They provide a basis for sizing and feed the definition of usability requirements. Use cases define all scenarios that an application has to support and can therefore easily be expanded into test cases. Since use cases describe a service's functionality on a level that's understandable for both business and IT, they can serve as a vehicle to specify the functional elements of an SLA, such as the actual business deliverables from the service.

One level 'below' the use case and the context diagram, many other modelling techniques can be applied. These models depict the static and dynamic characteristics of the

services under development. A conceptual data model (whether called object or data) describes the different 'objects' in the service, their mutual relationships and their internal structure. Dynamics of the service can be described using state models (e.g. state transition diagrams) that show the various states of the entities or objects, together with events that may cause state changes. Interactions between the different application components can be described using interaction diagrams (e.g. object interaction diagrams). Alongside a mature requirements modelling process, CASE tools can help in getting and keeping these models consistent, correct and complete.

5.1.1.2 Management and operational requirements

Management and operational requirements (or non-functional requirements) are used to define requirements and constraints on the IT service. The requirements serve as a basis for early systems and service sizing and estimates of cost, and can support the assessment of the viability of the proposed IT service. Management and operational requirements should also encourage developers to take a broader view of project goals.

Categories of management and operational requirements include:

- **Manageability:** Does it run? Does it fail? How does it fail?
- **Efficiency:** How many resources does it consume?
- **Availability and reliability:** How reliable does it need to be?
- **Capacity and performance:** What level of capacity do we need?
- **Security:** What classification of security is required?
- **Installation:** How much effort does it take to install the application? Is it using automated install procedures?
- **Continuity:** What level of resilience and recovery is required?
- **Controllability:** Can it be monitored, managed and adjusted?
- **Maintainability:** How well can the application be adjusted, corrected, maintained and changed for future requirements?
- **Operability:** Do the applications disturb other applications in their functionalities?
- **Measurability and reportability:** Can we measure and report on all of the required aspects of the application?

The management and operational requirements can be used to prescribe the quality attributes of the application being built. These quality attributes can be used to design test plans for testing the applications on the compliance to management and operational requirements.

5.1.1.3 Usability requirements

The primary purpose of usability requirements is to ensure that the service meets the expectations of its users with regard to its ease of use. To achieve this:

- Establish performance standards for usability evaluations
- Define test scenarios for usability test plans and usability testing.

Like the management and operational requirements, usability requirements can also be used as the quality attributes of design test plans for testing the applications on their compliance to usability requirements.

5.1.2 Requirements for support – the user view

Users have formally defined roles and activities as user representatives in requirements definition and acceptance testing. They should be actively involved in identifying all aspects of service requirements, including the three categories above, and also in:

- User training procedures and facilities
- Support activities and Service Desk procedures.

5.1.3 Requirements investigation techniques

There is a range of techniques that may be used to investigate business situations and elicit service requirements. Sometimes the customers and the business are not completely sure of what their requirements actually are and will need some assistance and prompting from the designer or requirements gatherer. This must be completed in a sensitive way to ensure that it is not seen as IT dictating business requirements again. The two most commonly used techniques are interviewing and workshops, but these are usually supplemented by other techniques, such as observation and scenarios.

5.1.3.1 Interviews

The interview is a key tool and can be vital in achieving a number of objectives, such as:

- Making initial contact with key stakeholders and establishing a basis for progress
- Building and developing rapport with different users and managers

- Acquiring information about the business situation, including issues and problems.

There are three areas that are considered during interviews:

- Current business processes that need to be fulfilled in any new business systems and services
- Problems with the current operations that need to be addressed
- New features required from the new business system or service and any supporting IT service.

The interviewing process is improved when the interviewer has prepared thoroughly as this saves time by avoiding unnecessary explanations and demonstrates interest and professionalism. The classic questioning structure of 'Why, What, Who, When, Where, How' provides an excellent framework for preparing for interviews.

It is equally important to formally close the interview by:

- Summarizing the points covered and the actions agreed
- Explaining what happens next, both following the interview and beyond
- Asking the interviewee how any further contact should be made.

It is always a good idea to write up the notes of the interview as soon as possible – ideally straight away and usually by the next day.

The advantages of interviewing are:

- Builds a relationship with the users
- Can yield important information
- Opportunity to understand different viewpoints and attitudes across the user group
- Opportunity to investigate new areas that arise
- Collection of examples of documents and reports
- Appreciation of political factors
- Study of the environment in which the new service will operate.

The disadvantages of interviewing are:

- Expensive in elapsed time
- No opportunity for conflict resolution.

5.1.3.2 Workshops

Workshops provide a forum in which issues can be discussed, conflicts resolved and requirements elicited. Workshops are especially valuable when time and budgets

are tightly constrained, several viewpoints need to be canvassed and an iterative and incremental view of service development is being taken.

The advantages of the workshop are:

- Gain a broad view of the area under investigation – having a group of stakeholders in one room will allow a more complete understanding of the issues and problems
- Increase speed and productivity – it is much quicker to have one meeting with a group of people than interviewing them one by one
- Obtain buy-in and acceptance for the IT service
- Gain a consensus view – if all the stakeholders are involved, the chance of them taking ownership of the results is improved.

There are some disadvantages, including:

- Can be time-consuming to organize – for example, it is not always easy to get all the necessary people together at the same time
- It can be difficult to get all of the participants with the required level of authority
- It can be difficult to get a mix of business and operational people to understand the different requirements.

The success or failure of a workshop session depends, in large part, on the preparatory work by the facilitator and the business sponsor for the workshop. They should spend time before the event planning the following areas:

- The objective of the workshop – this has to be an objective that can be achieved within the time constraints of the workshop.
- Who will be invited to participate in the workshop – it is important that all stakeholders interested in the objective should be invited to attend or be represented.
- The structure of the workshop and the techniques to be used. These need to be geared towards achieving the defined objective, e.g. requirements gathering or prioritization, and should take the needs of the participants into account.
- Arranging a suitable venue – this may be within the organization, but it is better to use a 'neutral' venue out of the office.

During the workshop, a facilitator needs to ensure that the issues are discussed, views are aired and progress is made towards achieving the stated objective. A record needs to be kept of the key points emerging from the discussion.

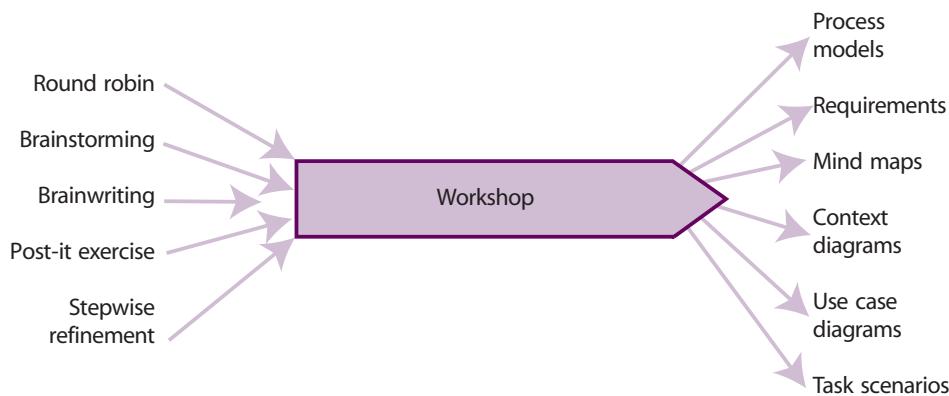


Figure 5.1 Requirements workshop techniques

At the end of the workshop, the facilitator needs to summarize the key points and actions. Each action should be assigned to an owner.

There are two main categories of technique required for a requirements workshop – techniques for discovery and techniques for documentation, as shown in Figure 5.1.

5.1.3.3 Observation

Observing the workplace is very useful in obtaining information about the business environment and the work practices. This has two advantages:

- A much better understanding of the problems and difficulties faced by the business users
- It will help devise workable solutions that are more likely to be acceptable to the business.

Conversely, being observed can be rather unnerving, and the old saying 'you change when being observed' needs to be factored into your approach and findings.

Formal observation involves watching a specific task being performed. There is a danger of being shown just the 'front-story' without any of the everyday variances, but it is still a useful tool.

5.1.3.4 Protocol Analysis

Protocol Analysis is simply getting the users to perform a task, and for them to describe each step as they perform it.

5.1.3.5 Shadowing

Shadowing involves following a user for a period such as a day to find out about a particular job. It is a powerful way to understand a particular user role. Asking for explanations of how the work is done, or the workflow, clarifies some of the already assumed aspects.

5.1.3.6 Scenario Analysis

Scenario Analysis is essentially telling the story of a task or transaction. Its value is that it helps a user who is uncertain what is needed from a new service to realize it more clearly. Scenarios are also useful when analysing or redesigning business processes. A scenario will trace the course of a transaction from an initial business trigger through each of the steps needed to achieve a successful outcome.

Scenarios provide a framework for discovering alternative paths that may be followed to complete the transaction. This is extremely useful in requirements elicitation and analysis because real-life situations, including the exceptional circumstances, are debated.

Scenarios offer significant advantages:

- They force the user to include every step, so there are no taken-for-granted elements and the problem of tacit knowledge is addressed
- By helping the user to visualize all contingencies, they help to cope with the uncertainty about future systems and services
- A workshop group refining a scenario will identify those paths that do not suit the corporate culture
- They provide a tool for preparing test scripts.

The disadvantages of scenarios are that they can be time-consuming to develop, and some scenarios can become very complex. Where this is the case, it is easier to analyse if each of the main alternative paths is considered as a separate scenario.

A popular approach to documenting scenario descriptions is to develop use case descriptions to support use case diagrams. However, there are also a number of graphical methods of documenting a scenario, such as storyboards, activity diagrams, task models and decision tree diagrams.

5.1.3.7 Prototyping

Prototyping is an important technique for eliciting, analysing, demonstrating and validating requirements. It is difficult for users to envisage the new service before it is actually built. Prototypes offer a way of showing the user how the new service might work and the ways in which it can be used. If a user is unclear what they need the service to do for them, utilizing a prototype often releases blocks to thinking and can produce a new wave of requirements. Incremental and iterative approaches to service development, such as the Dynamic Systems Development Method (DSDM), use evolutionary prototyping as an integral part of their development lifecycle.

There is a range of approaches to building prototypes. They may be built using an application development environment so that they mirror the service; images of the screens and navigations may be built using presentation software; or they may simply be 'mock-ups' on paper.

There are two basic methods of prototyping:

- The throw-away mock-up, which is only used to demonstrate the look and feel
- The incremental implementation, where the prototype is developed into the final system.

It is important to select consciously which is to be used, otherwise there is a danger that a poor-quality mock-up becomes the basis for the real system, causing problems later on.

There is a strong link between scenarios and prototyping because scenarios can be used as the basis for developing prototypes. In addition to confirming the users' requirements, prototyping can often help the users to identify new requirements.

Prototypes are successfully used to:

- Clarify any uncertainty on the part of the service developers and confirm to the user that what they have asked for has been understood
- Open the user up to new requirements as they understand what the service will be able to do to support them
- Show users the 'look and feel' of the proposed service and elicit usability requirements
- Validate the requirements and identify any errors.

Potential problems include:

- Endless iteration
- A view that if the prototype works, the full service can be ready tomorrow.

5.1.3.8 Other techniques

Other techniques that could be used, include:

- **Questionnaires:** can be useful to get a limited amount of information from a lot of people when interviewing them all would not be practical or cost-effective.
- **Special purpose records:** technique involves the users in keeping a record about a specific issue or task. For example, they could keep a simple five-bar gate record about how often they need to transfer telephone calls – this could provide information about the problems with this business process.
- **Activity sampling:** is a rather more quantitative form of observation and can be used when it is necessary to know how people spend their time – for example, how much time is spent on invoicing? How much time is spent on reconciling payments? How much time is spent on sorting out queries?

5.1.4 Problems with requirements engineering

Requirements, seen by users as the uncomplicated bit of a new service development, are actually the most problematic aspect, and yet the time allocated is far less than for the other phases.

Tight timescales and tight budgets – both the result of constraints on the business – place pressures on the development team to deliver a service. The trouble is that without the due time to understand and define the requirements properly, the service that is delivered on time may not be the service that the business thought it was asking for.

Studies carried out into IT project failures tell a common story. Many of the projects and unsatisfactory IT services suggest the following conclusions:

- A large proportion of errors (over 80%) are introduced at the requirements phase
- Very few faults (fewer than 10%) are introduced at design and development – developers are developing things right, but frequently not developing the right things
- Most of the project time is allocated to the development and testing phases of the project
- Less than 12% of the project time is allocated to requirements.

These findings are particularly significant because the cost of correcting errors in requirements increases dramatically the later into the development lifecycle they are found.

One of the main problems with requirements engineering is the lack of detailed skill and overall understanding of the area when people use it. If accurately performed, the work can integrate requirements from numerous areas in a few questions.

Other typical problems with requirements have been identified as:

- Lack of relevance to the objectives of the service
- Lack of clarity in the wording
- Ambiguity
- Duplication between requirements
- Conflicts between requirements
- Requirements expressed in such a way that it is difficult to assess whether or not they have been achieved
- Requirements that assume a solution rather than stating what is to be delivered by the service
- Uncertainty amongst users about what they need from the new service
- Users omitting to identify requirements
- Inconsistent levels of detail
- An assumption that user and IT staff have knowledge that they do not possess and therefore failing to ensure that there is a common understanding
- Requirements creep – the gradual addition of seemingly small requirements without taking the extra effort into account in the project plan.

Another problem is an apparent inability on the part of the users to articulate clearly what it is they wish the service to do for them. Very often they are deterred from doing so because the nature of the requirement is explained in a straightforward statement.

5.1.4.1 Resolving requirements engineering problems

Defining actors

There are some participants that must take part in the requirements process. They represent three broad stakeholder groups:

- The business
- The user community
- The service development team.

The user community should be represented by the domain expert (or subject-matter expert) and end-users.

Dealing with tacit knowledge

When developing a new service, the users will pass on to us their explicit knowledge, i.e. knowledge of procedures and data that is at the front of their minds and that they can easily articulate. A major problem when eliciting requirements is that of tacit knowledge, i.e. those other aspects of the work that a user is unable to articulate or explain.

Some common elements that cause problems and misunderstandings are:

- Skills – explaining how to carry out actions using words alone is extremely difficult.
- Taken-for-granted information – even experienced and expert business users may fail to mention information or clarify terminology, and the analyst may not realize that further questioning is required.
- Front-story/back-story – this issue concerns a tendency to frame a description of current working practices, or a workplace, in order to give a more positive view than is actually the case.
- Future systems knowledge – if the study is for a new service development, with no existing expertise or knowledge in the organization, how can the prospective users know what they want?
- The difficulty of an outsider assuming a common language for discourse, and common norms of communication. (If they do not have this, then the scope for misrepresentation of the situation can grow considerably.)
- Intuitive understanding, usually born of considerable experience. Decision makers are often thought to follow a logical, linear path of enquiry while making their decisions. In reality though, as improved decision-making skills and knowledge are acquired, the linear path is often abandoned in favour of intuitive pattern recognition.
- Organizational culture – without an understanding of the culture of an organization, the requirements exercise may be flawed.

Communities of practice are discrete groups of workers – maybe related by task, by department, by geographical location or some other factor – that have their own sets of norms and practices, distinct from other groups within the organization and the organization as a whole.

Table 5.1 Requirements engineering – tacit and explicit knowledge

	Tacit	Explicit
Individual	Skills, values, taken-for-granted, intuitiveness	Tasks, job descriptions, targets, volumes and frequencies
Corporate	Norms, back-story, culture, communities of practice	Procedures, style guides, processes, knowledge sharing

Example levels of tacit and explicit knowledge:

Table 5.2 Requirements engineering; examples of tacit and explicit knowledge (Maiden and Rugg, 1995)

Technique	Explicit knowledge	Tacit knowledge	Skills	Future requirements
Interviewing	✓✓	✓	X	✓
Shadowing	✓✓	✓✓	✓✓	X
Workshops	✓✓	✓✓	X	✓✓
Prototyping	✓✓	✓✓	✓✓	✓✓
Scenario analysis	✓✓	✓✓	X	✓✓
Protocol analysis	✓✓	✓✓	✓✓	X

5.1.5 Documenting requirements

The requirements document is at the heart of the process and can take a number of forms. Typically the document will include a catalogue of requirements, with each individual requirement documented using a standard template. One or more models showing specific aspects, such as the processing or data requirements, may supplement this catalogue.

Before they are formally entered into the catalogue, requirements are subject to careful scrutiny. This scrutiny may involve organizing the requirements into groupings and checking that each requirement is 'well-formed'.

Once the document is considered to be complete, it must be reviewed by business representatives and confirmed to be a true statement of the requirements, at this point in time. During this stage the reviewers examine the requirements and question whether they are well-defined, clear and complete.

As we uncover the requirements from our various users, we need to document them. This is best done in two distinct phases – building the requirements list and, later, developing an organized requirements catalogue. The list tends to be an informal document and can be presented as four columns, as shown in Table 5.3.

Table 5.3 Requirements list

Requirements	Source	Comments	Detail level
--------------	--------	----------	--------------

Each requirement in the list must be checked to see whether or not it is well formed and SMART (Specific, Measurable, Achievable, Realistic and Timely).

When checking the individual and totality of requirements, the following checklist can be used:

- Are the requirements, as captured, unambiguous?
- Is the meaning clear?
- Is the requirement aligned to the service development and business objectives, or is it irrelevant?
- Is the requirement reasonable, or would it be expensive and time-consuming to satisfy?
- Do any requirements conflict with one another such that only one may be implemented?
- Do they imply a solution rather than state a requirement?
- Are they atomic, or are they really several requirements grouped into one entry?
- Do several requirements overlap or duplicate each other?

There are several potential outcomes from the exercise:

- Accept the requirement as it stands
- Re-word the requirement to remove jargon and ambiguity
- Merge duplicated/overlapping requirements
- Take unclear and ambiguous requirements back to the users for clarification.

5.1.5.1 The requirements catalogue

The Requirements Catalogue is the central repository of the users' requirements, and all the requirements should be documented here, following the analysis of the list defined above. The Requirements Catalogue should form part of the overall Service Pipeline within the overall Service Portfolio. Each requirement that has been analysed is documented using a standard template, such as that shown in Table 5.4.

The key entries in the template are as follows:

- **Requirement ID** – this is a unique ID that never changes and is used for traceability – for example, to reference the requirement in design documents, test specifications or implemented code. This ensures that all requirements have been met and that all implemented functions are based on requirements.
- **Source** – the business area or users who requested the requirement or the document where the requirement was raised. Recording the source of a requirement helps ensure that questions can be answered or the need can be re-assessed in the future if necessary.

- **Owner** – the user who accepts ownership of the individual requirement will agree that it is worded and documented correctly, and will sign it off at acceptance testing when satisfied.
- **Priority** – the level of importance and need for a requirement. Normally approaches such as MoSCoW are used, where the following interpretation of the mnemonic applies:
 - **Must have** – a key requirement without which the service has no value.
 - **Should have** – an important requirement that must be delivered but, where time is short, could be delayed for a future delivery. This should be a short-term delay, but the service would still have value without them.
 - **Could have** – a requirement that would it be beneficial to include if it does not cost too much or take too long to deliver, but it is not central to the service.
 - **Won't have** (but want next time) – a requirement that will be needed in the future but is not required for this delivery. In a future service release, this requirement may be upgraded to a 'must have'.

The following should be clearly agreed during this prioritization activity:

- Requirement priorities can and do change over the life of a service development project.
- 'Should have' requirements need to be carefully considered because, if they are not delivered within the initial design stage, they may be impossible to implement later.

Table 5.4 Requirements template

IT service	Author	Date		
Requirement ID	Requirement Name			
Source	Owner	Priority		
Functional Requirement Description				
Management and Operational and Usability Requirements	Description			
Justification				
Related Documents				
Related Requirements				
Comments				
Resolution				
Version No	Change History	Date		
		Change request		

- Requirements are invariably more difficult and more expensive to meet later in the Service Lifecycle.
- It is not just the functional requirements that can be ‘must haves’ – some of the management and operational requirements should be ‘must haves’.
- Requirement description – a succinct description of the requirement. A useful approach is to describe the requirement using the following structure:
 - Actor (or user role)
 - Verb phrase
 - Object (noun or noun phrase).
- Where the requirement incorporates complex business rules or data validation, decision table or decision tree may be more useful to define complex business rules, whilst data validation rules may be defined in a repository. If a supplementary technique is used to specify or model the requirement, there should be a cross-reference to the related document.
- Business process – a simple phrase to group together requirements that support a specific activity, such as sales, inventory, customer service, and so on.
- Justification – not all the requirements that are requested will be met. This may be due to time and budget constraints, or may be because the requirement is dropped in favour of a conflicting requirement. Often the requirement is not met because it adds little value to the business. The justification sets out the reasons for requesting the requirement.
- Related requirements – requirements may be related to each other for several reasons. Sometimes there is a link between the functionality required by the requirements or a high-level requirement is clarified by a series of more detailed requirements.
- Change history – the entries in this section provide a record of all the changes that have affected the requirement. This is required for Configuration Management and traceability purposes.

5.1.5.2 Full requirements documentation

An effective requirements document should comprise the following elements:

- A glossary of terms, to define each organizational term used within the requirements document. This will help manage the problem of local jargon and will clarify synonyms and homonyms for anyone using the document
- A scoping model, such as a system context diagram
- The Requirements Catalogue, ideally maintained as part of an overall Service Portfolio

- Supporting models, such as business process models, data flow diagrams or interaction diagrams.

Managing changes to the documentation

Changes may come about because:

- The scope of the new service has altered through budget constraints
- The service must comply with new regulation or legislation
- Changes in business priorities have been announced
- Stakeholders have understood a requirement better after some detailed analysis – for example, using scenarios or prototyping – and amended the original requirement accordingly.

There are a number of specialist support tools on the market to support requirements processes. These are sometimes called CARE (Computer Aided Requirements Engineering) or CASE (Computer Aided Software Engineering). Features include:

- Maintaining cross-references between requirements
- Storing requirements documentation
- Managing changes to the requirements documentation
- Managing versions of the requirements documentation
- Producing formatted requirements specification documents from the database
- Ensuring documents delivered by any solution project are suitable to enable support.

5.1.6 Requirements and outsourcing

The aim is to select standard packaged solutions wherever possible to meet service requirements. However, whether IT requirements are to be purchased off-the-shelf, developed in-house or outsourced, all the activities up to the production of a specification of business requirements are done in-house. Many IT service development contracts assume it is possible to know what the requirements are at the start, and that it is possible to produce a specification that unambiguously expresses the requirements. For all but the simplest services this is rarely true. Requirements analysis is an iterative process – the requirements will change during the period the application and service are being developed. It will require user involvement throughout the development process, as in the DSDM and other ‘agile’ approaches.

5.1.6.1 Typical requirements outsourcing scenarios

Typical approaches to contract for the development of IT systems to be delivered in support of an IT service are as follows:

- Low-level requirements specification – the boundary between ‘customer’ and provider is drawn between the detailed requirements specification and any design activities. All the requirements that have an impact on the user have been specified in detail, giving the provider a very clear and precise implementation target. However, there is increased specification effort, and the added value of the provider is restricted to the less difficult aspects of development.
- High-level requirements specification – the customer/provider boundary is between the high-level requirements and all other phases. The provider contract covers everything below the line. The customer is responsible for testing the delivered service against the business requirements. As it is easier to specify high-level requirements, there is reduced effort to develop contract inputs. However, there may be significant problems of increased cost and risk for both customer and provider, together with increased room for mistakes, instability of requirements and increased difficulty in knowing what information systems you want.

5.2 DATA AND INFORMATION MANAGEMENT

Data is one of the critical asset types that need to be managed in order to develop, deliver and support IT services effectively. Data/Information Management is how an organization plans, collects, creates, organizes, uses, controls, disseminates and disposes of its data/information, both structured records and unstructured data. It also ensures that the value of that data/information is identified and exploited, both in support of its internal operations and in adding value to its customer-facing business processes.

A number of terms are common in this area, including ‘Data Management’, ‘Information Management’ and ‘Information Resource Management’. For the purposes of this publication, the term ‘Data Management’ is used as shorthand for all of the three above.

The role of Data Management described is not just about managing raw data: it’s about managing all the contextual

metadata – additional ‘data about the data’ – that goes with it, and when added to the raw data gives ‘information’ or ‘data in context’.

Data, as the basis for the organization’s information, has all the necessary attributes to be treated as an asset (or resource). For example, it is essential for ‘the achievement of business objectives and the successful daily workings of an organization’. In addition, it can be ‘obtained and preserved by an organization, but only at a financial cost’. Finally it can, along with other resources/assets, be used to ‘further the achievement of the aims of an organization’.

Key factors for successful Data Management are as follows:

- All users have ready access through a variety of channels to the information they need to do their jobs.
- Data assets are fully exploited, through data sharing within the organization and with other bodies.
- The quality of the organization’s data is maintained at an acceptable level, and the information used in the business is accurate, reliable and consistent.
- Legal requirements for maintaining the privacy, security, confidentiality and integrity of data are observed.
- The organization achieves a high level of efficiency and effectiveness in its data and information-handling activities.
- An enterprise data model to define the most important entities and their relationships – this helps to avoid redundancies and to avoid the deterioration of the architecture as it is changed over the years.

5.2.1 Managing data assets

If data isn’t managed effectively:

- People maintain and collect data that isn’t needed
- The organization may have historic information that is no longer used
- The organization may hold a lot of data that is inaccessible to potential users
- Information may be disseminated to more people than it should be, or not to those people to whom it should be
- The organization may use inefficient and out-of-date methods to collect, analyse, store and retrieve the data
- The organization may fail to collect data that it needs, reducing data quality and data integrity is lost, e.g. between related data sources.

In addition, whether or not information is derived from good-quality data is a difficult question to answer, because

there are no measurements in place against which to compare it. For example, poor data quality often arises because of poor checks on input and/or updating procedures. Once inaccurate or incomplete data have been stored in the IT system, any reports produced using these data will reflect these inaccuracies or gaps. There may also be a lack of consistency between internally-generated management information from the operational systems, and from other internal, locally-used systems, created because the central data is not trusted.

One way of improving the quality of data is to use a Data Management process that establishes policy and standards, provides expertise and makes it easier to handle the data aspects of new services. This should then allow full Data/Information Asset Management to:

- Add value to the services delivered to customers
- Reduce risks in the business
- Reduce the costs of business processes
- Stimulate innovation in internal business processes.

5.2.2 Scope of Data Management

There are four areas of management included within the scope of Data/Information Management:

- **Management of data resources:** the governance of information in the organization must ensure that all these resources are known and that responsibilities have been assigned for their management, including ownership of data and metadata. This process is normally referred to as data administration and includes responsibility for:
 - Defining information needs
 - Constructing a data inventory and an enterprise data model
 - Identifying data duplication and deficiencies
 - Maintaining a catalogue/index of data/information content
 - Measuring the cost and value of the organization's data.
- **Management of data/information technology:** the management of the IT that underpins the organization's information systems; this includes processes such as database design and database administration. This aspect is normally handled by specialists within the IT function – see the Service Operation publication for more details.
- **Management of information processes:** business processes will lead to IT services involving one or other of the data resources of the organization. The processes of creating, collecting, accessing, modifying,

storing, deleting and archiving data – i.e. the data lifecycle – must be properly controlled, often jointly with the applications management process.

- **Management of data standards and policies:** the organization will need to define standards and policies for its Data Management as an element of an IT strategy. Policies will govern the procedures and responsibilities for Data Management in the organization; and technical policies, architectures and standards that will apply to the IT infrastructure that supports the organization's information systems.

The best practices scope of the Data Management process includes managing non-structured data that is not held in conventional database systems – for example, using formats such as text, image and audio. It is also responsible for ensuring process quality at all stages of the data lifecycle, from requirements to retirement. The main focus in this publication will be on its role in the requirements, design and development phases of the asset and Service Lifecycle.

The team supporting the Data Management process may also provide a business information support service. In this case they are able to answer questions about the meaning, format and availability of data internal to the organization, because they manage the metadata. They also are able to understand and explain what external data might be needed in order to carry out necessary business processes and will take the necessary action to source this.

Critically, when creating or redesigning processes and supporting IT services, it is good practice to consider re-using data and metadata across different areas of the organization. The ability to do this may be supported by a corporate data model – sometimes known as a common information model – to help support re-use, often a major objective for data management.

5.2.3 Data Management and the Service Lifecycle

It is recommended that a lifecycle approach be adopted in understanding the use of data in business processes. General issues include:

- What data is currently held and how can it be classified?
- What data needs to be collected or created by the business processes?
- How will the data be stored and maintained?
- How will the data be accessed, by whom and in what ways?

- How will the data be disposed of, and under whose authority?
- How will the quality of the data be maintained (accuracy, consistency, currency, etc.)?
- How can the data be made more accessible/available?

5.2.4 Supporting the Service Lifecycle

During requirements and initial design, Data Management can assist design and development teams with service-specific data modelling and give advice on the use of various techniques to model data.

During detailed ('physical') design and development, the Data Management function can provide technical expertise on database management systems and on how to convert initial 'logical' models of data into physical, product specific, implementations.

Many new services have failed because poor data quality has not been addressed during the development of the service, or because a particular development created its own data and metadata, without consultation with other service owners, or with Data Management.

5.2.5 Valuing data

Data is an asset and has value. Clearly in some organizations this is more obvious than in others. Organizations that are providers of data to other organizations – Yell, Dun and Bradstreet, and Reuters – can value data as an 'output' in terms of the price that they are charging external organizations to receive it. It's also possible to think of value in terms of what the internal data would be worth to another organization.

It's more common to value data in terms of what it's worth to the owner organization. There are a number of suggested ways of doing this:

- **Valuing data by availability:** one approach often used is to consider which business processes would not be possible if a particular piece of data were unavailable, and how much that non-availability of data would cost the business.
- **Valuing lost data:** another approach that's often used is to think about the costs of obtaining some data if it were to be destroyed.
- **Valuing data by considering the data lifecycle:** this involves thinking about how data is created or obtained in the first place, how it is made available to people to use, and how data is retired, either through archiving or physical destruction. It may be that some data is provided from an external source and then held internally, or it may be that data has to be

created by the organization's internal systems. In these two cases, the lifecycle is different and the processes that take place for data capture will be entirely separate. In both cases the costs of redoing these stages can be evaluated. The more highly valued the data, the more the effort that needs to be expended on ensuring its integrity, availability and confidentiality.

5.2.6 Classifying data

Data can be initially classified as operational, tactical or strategic:

- **Operational data:** necessary for the ongoing functioning of an organization and can be regarded as the lowest, most specific, level.
- **Tactical data:** usually needed by second-line management – or higher – and typically concerned with summarized data and historical data, typically year-to-year data or quarterly data. Often the data that's used here appears in management information systems that require summary data from a number of operational systems in order to deal with an accounting requirement, for example.
- **Strategic data:** often concerned with longer-term trends and with comparison with the outside world, so providing the necessary data for a strategic support system involves bringing together the operational and tactical data from many different areas with relevant external data. Much more data is required from external sources.

An alternative method is to use a security classification of data and documents. This is normally adopted as a corporate policy within an organization.

An orthogonal classification distinguishes between organization-wide data, functional-area data and service-specific data.

- Organization-wide data needs to be centrally managed.
- The next level of data is functional-area data that should be shared across a complete business function. This involves sharing data 'instances' – for example, individual customer records – and also ensuring that consistent metadata across that functional area, such as standard address formats, are being used.
- The final level is IT service-specific, where the data and metadata are valid for one IT service and do not need to be shared with other services.

5.2.7 Setting data standards

One of the critical aspects of data administration is to ensure that standards for metadata are in place – for example, what metadata is to be kept for different underlying ‘data types’. Different details are kept about structured tabular data than for other areas. ‘Ownership’ is a critical item of this metadata, some sort of unique identifier is another, a description in business meaningful terms another, and a format might be another. The custodian or steward, someone in the IT department who takes responsibility for the day-to-day management of the data, is also recorded.

Another benefit of a Data Management process would be in the field of reference data. Certain types of data, such as postcodes or names of countries, may be needed across a variety of systems and need to be consistent. It is part of the responsibility of data administration to manage reference data on behalf of the whole business, and to make sure that the same reference data is used by all systems in the organization.

Standards for naming must be in place; so, for example, if a new type of data is requested in a new service, then there is a need to use names that meet these standards. An example standard might be ‘all capitals, no underlining and no abbreviations’.

5.2.8 Data ownership

Data administration can assist the service developer by making sure responsibilities for data ownership are taken seriously by the business and by the IT department. One of the most successful ways of doing this is to get the business and the IT department to sign up to a data charter – a set of procedural standards and guidance for the careful management of data in the organization, by adherence to corporately defined standards.

Responsibilities of a data owner are often defined here and may include:

- Agreeing a business description and a purpose for the data
- Defining who can create, amend, read and delete occurrences of the data
- Authorizing changes in the way data is captured or derived
- Approving any format, domain and value ranges
- Approving the relevant level of security, including making sure that legal requirements and internal policies about data security are adhered to.

5.2.9 Data migration

Data migration is an issue where a new service is replacing a number of (possibly just one) existing services, and it’s necessary to carry across, into the new service, good-quality data from the existing systems and services. There are two types of data migration of interest to projects here: one is the data migration into data warehouses etc., for business intelligence/analytics purposes; the other is data migration to a new transactional, operational service. In both cases it will be beneficial if data migration standards, procedures and processes are laid down by Data Management. Data migration tools may have already been purchased on behalf of the organization by the Data Management team. Without this support, it’s very easy to underestimate the amount of effort that’s required, particularly if data consolidation and cleaning has to take place between multiple source systems, and the quality of the existing services’ data is known to be questionable.

5.2.10 Data storage

One area where technology has moved on very rapidly is in the area of storage of data. There is a need to consider different storage media – for example, optical storage – and be aware of the size and cost implications associated with this. The main reason for understanding the developments in this area is that they make possible many types of data management areas that were considered too expensive before. For example, to store real-time video, which uses an enormous bandwidth, has, until the last two to three years, been regarded as too expensive. The same is true of the scanning of large numbers of paper documents, particularly where those documents are not text-based but contain detailed diagrams or pictures. Understanding technology developments with regard to electronic storage of data is critical to understanding the opportunities for the business to exploit the information resource effectively by making the best use of new technology.

5.2.11 Data capture

It is also very important to work with Data Management on effective measures for data capture. The aim here is to capture data as quickly and accurately as possible. There is a need to ensure that the data capture processes require the minimum amount of keying, and exploit the advantages that graphical user interfaces provide in terms of minimizing the number of keystrokes needed, also decreasing the opportunity for errors during data capture. It is reasonable to expect that the Data Management process has standards for, and can provide expertise on,

effective methods of data capture in various environments, including 'non-structured' data capture using mechanisms such as scanning.

5.2.12 Data retrieval and usage

Once the data has been captured and stored, the next aspect to consider is the retrieval of information from the data. Services to allow easy access to structured data via query tools of various levels of sophistication are needed by all organizations, and generate their own specific architectural demands.

The whole area of searching within scanned text and other non-structured data such as video, still images or sound is a major area of expansion. Techniques such as automatic indexing, and the use of search engines to give efficient access via keywords to relevant parts of a document, are essential technologies that have been widely implemented, particularly on the internet. Expertise in the use of data or content within websites should exist within the Data Management as well as Content Management – standards and procedures that are vital for websites.

5.2.13 Data integrity and related issues

When defining requirements for IT services, it is vital that management and operational requirements related to data are considered. In particular, the following areas must be addressed:

- Recovery of lost or corrupted data
- Controlled access to data
- Implementation of policies on archiving of data, including compliance with regulatory retention periods
- Periodic data integrity checks.

Data integrity is concerned with ensuring that the data is of high quality and uncorrupted. It is also about preventing uncontrolled data duplication, and hence avoiding any confusion about what is the valid version of the data. There are several approaches that may assist with this. Various technology devices such as 'database locking' are used to prevent multiple, inconsistent, updating of data. In addition, prevention of illegal updating may be achieved through access control mechanisms.

5.3 APPLICATION MANAGEMENT

An application is defined here as the software program(s) that perform those specific functions that directly support the execution of business processes and/or procedures.

Applications, along with data and infrastructure components such as hardware, the operating system and middleware, make up the technology components that are part of an IT service. The application itself is only one component, albeit an important one of the service. Therefore it is important that the application delivered matches the agreed requirements of the business. However, too many organizations spend too much time focusing on the functional requirements of the new service and application, and insufficient time is spent designing the management and operational requirements (non-functional requirements) of the service. This means that when the service becomes operational, it meets all of the functionality required, but totally fails to meet the expectation of the business and the customers in terms of its quality and performance, and therefore becomes unusable.

Two alternative approaches are necessary to fully implement Application Management. One approach employs an extended Service Development Lifecycle (SDLC) to support the development of an IT service. SDLC is a systematic approach to problem solving and is composed of the following steps:

- Feasibility study
- Analysis
- Design
- Testing
- Implementation
- Evaluation
- Maintenance.

The other approach takes a global view of all services to ensure the ongoing maintainability and manageability of the applications:

- All applications are described in a consistent manner, via an Application Portfolio that is managed and maintained to enable alignment with dynamic business needs.
- Consistency of approach to development is enforced through a limited number of application frameworks and design patterns and through a 're-use' first philosophy.
- Common software components, usually to meet management and operational requirements, are created or acquired at an 'organizational' level and used by individual systems as they are designed and built.

Table 5.5 Application Portfolio attributes example

Application name	IT operations owner	New development cost
Application identifier	IT development owner	Annual operational costs
Application description	Support contacts	Annual support cost
Business process supported	Database technologies	Annual maintenance costs
IT services supported	Dependent applications	Outsourced components
Executive sponsor	IT systems supported	Outsource partners
Geographies supported	User interfaces	Production metrics
Business criticality	IT Architecture, including Network topology	OLA link
SLA link	Application technologies used	Support metrics
Business owner	Number of users	

5.3.1 The Application Portfolio

This is simply a full record of all applications within the organization and is dynamic in its content.

5.3.2 Linking Application and Service Portfolios

Some organizations maintain a separate Application Portfolio with separate attributes, while in other organizations the Application Portfolio is stored within the CMS, together with the appropriate relationships. Other organizations combine the Application Portfolio together with the Service Portfolio. It is for each organization to decide the most appropriate strategy for its own needs. What is clear is that there should be very close relationships and links between the applications and the services they support and the infrastructure components used.

5.3.3 Application frameworks

The concept of an application framework is a very powerful one. The application framework covers all management and operational aspects and actually provides solutions for all the management and operational requirements that surround an application.

Implied in the use of application frameworks is the concept of standardization. If an organization uses and has to maintain an application framework for every single application, there will not be many benefits of the use of an application framework.

An organization that wants to develop and maintain application frameworks, and to ensure the application frameworks comply with the needs of the application developers, must invest in doing so. It is essential that applications framework architectures are not developed in

isolation, but are closely related and integrated with all other framework and architectural activities. The Service, Infrastructure, Environment and Data Architectures must all be closely integrated with the **Application Architecture** and framework.

Architecture, application frameworks and standards

Architecture-related activities have to be planned and managed separately from individual system-based software projects. It is also important that architecture-related activities be performed for the benefit of more than just one application. Application developers should focus on a single application, while application framework developers should focus on more than one application, and on the common features of those applications in particular.

A common practice is to distinguish between various types of applications. For instance, not every application can be built on top of a Microsoft® Windows operating system platform, connected to a UNIX server, using HTML, Java applets, JavaBeans and a relational database. The various types of applications can be regarded as application families. All applications in the same family are based on the same application framework.

Utilizing the concept of an application framework, the first step of the application design phase is to identify the appropriate application framework. If the application framework is mature, a large number of the design decisions are given. If it is not mature, and all management and operational requirements cannot be met on top of an existing application framework, the preferred strategy is to collect and analyse the requirements that cannot be dealt with in the current version of the application framework. Based on the application requirements, new requirements can be defined for the

application framework. Next, the application framework can be modified so that it can cope with the application requirements. In fact, the whole family of applications that corresponds to the application framework can then use the newly added or changed framework features.

Developing and maintaining an application framework is a demanding task and, like all other design activities, should be performed by competent and experienced people. Alternatively, application frameworks can be acquired from third parties.

5.3.4 The need for CASE tools and repositories

One important aspect of that overall alignment is the need to align applications with their underlying support structures. Application development environments traditionally have their own Computer Assisted/Aided Software Engineering (CASE) tools that offer the means to specify requirements, draw design diagrams (according to particular modelling standards), or even generate complete applications, or nearly complete application skeletons, almost ready to be deployed. These environments also provide a central location for storing and managing all the elements that are created during application development, generally called a repository. Repository functionality includes version control and consistency checking across various models. The current approach is to use metacase-tools to model domain-specific languages and use these to make the CASE-work more aligned to the needs of the business.

5.3.5 Design of specific applications

The requirements phase of the lifecycle was addressed earlier in the requirements engineering section. The design phase is one of the most important phases within the application lifecycle. It ensures that an application is conceived with operability and Application Management in mind. This phase takes the outputs from the requirements phase and turns them into the specification that will be used to develop the application.

The goal for designs should be satisfying the organization's requirements. Design includes the design of the application itself, and the design of the infrastructure and environment within which the application operates. Architectural considerations are the most important aspect of this phase, since they can impact on the structure and content of both application and operational model. Architectural considerations for the application (design of the Application Architecture) and architectural considerations for the environment (design of the IT

Architecture) are strongly related and need to be aligned. Application Architecture and design should not be considered in isolation but should form an overall integrated component of service architecture and design.

Generally, in the design phase, the same models will be produced as have been delivered in the requirements phase, but during design many more details are added. New models include the architecture models, where the way in which the different functional components are mapped to the physical components (e.g. desktops, servers, databases and network) needs to be defined. The mapping, together with the estimated load of the system, should allow for the sizing of the infrastructure required.

Another important aspect of the architecture model is the embedding of the application in the existing environment. Which pieces of the existing infrastructure will be used to support the required new functions? Can existing servers or networks be used? With what impact? Are required functions available in existing applications that can be utilized? Do packages exist that offer the functionality needed or should the functions be built from scratch?

The design phase takes all requirements into consideration and starts assembling them into an initial design for the solution. Doing this not only gives developers a basis to begin working: it is also likely to bring up questions that need to be asked of the customers/users. If possible, application frameworks should be applied as a starting point.

It is not always possible to foresee every aspect of a solution's design ahead of time. As a solution is developed, new things will be learned about how to do things and also how not to.

The key is to create a flexible design, so that making a change does not send developers all the way back to the beginning of the design phase. There are a number of approaches that can minimize the chance of this happening, including:

- Designing for management and operational requirements
- Managing trade-offs
- Using application-independent design guidelines; using application frameworks
- Employing a structured design process/manageability checklist.

Design for management and operational requirements means giving management and operational requirements a level of importance similar to that for the functional requirements, and including them as a mandatory part of

the design phase. This includes a number of management and operational requirements such as availability, capacity, maintainability, reliability and security. It is now inconceivable in modern application development projects that user interface design (usability requirements) would be omitted as a key design activity. However, many organizations ignore or forget manageability. Details of the necessary management and operational requirements are contained within the SDP and SAC in Appendices A and B.

5.3.6 Managing trade-offs

Managing trade-off decisions focuses on balancing the relationship among resources, the project schedule, and those features that need to be included in the application for the sake of quality.

When development teams try to complete this balancing, it is often at the expense of the management and operational requirements. One way to avoid that is to include management and operational requirements in the application-independent design guidelines – for example, in the form of an application framework. Operability and manageability effectively become standard components of all design processes – for example, in the form of an application framework – and get embedded into the working practices and culture of the development organization.

5.3.7 Typical design outputs

The following are examples of the outputs from an applications design forming part of the overall Service Design:

- Input and output design, including forms and reports
- A usable user interface (human computer interaction) design
- A suitable data/object model
- A process flow or workflow model
- Detailed specifications for update and read-only processes
- Mechanisms for achieving audit controls, security, confidentiality and privacy
- A technology specific ‘physical’ design
- Scripts for testing the systems design
- Interfaces and dependencies on other applications.

There are guidelines and frameworks that can be adopted to determine and define design outputs within Applications Management, such as Capability Maturity Model Integration (CMMI).

5.3.8 Design patterns

A design pattern is a general, repeatable solution to a commonly occurring problem in software design. Object-oriented design patterns typically show relationships and interactions between classes or objects, without specifying the final application classes or objects that are involved. Design patterns describe both a problem and a solution for common issues encountered during application development.

An important design principle used as the basis for a large number of the design patterns found in recent literature is that of separation of concern. Separation of concerns will lead to applications divided into components, with a strong cohesion and minimal coupling between components. The advantage of such an application is that modification can be made to individual components with little or no impact on other components.

In typical application development projects, more than 70% of the effort is spent on designing and developing generic functions and on satisfying the management and operational requirements. That is because each individual application needs to provide a solution for such generic features as printing, error handling and security.

Among others, the Object Management Group (OMG, www.omg.com) defined a large number of services that are needed in every application. OMG’s Object Management Architecture (OMA) clearly distinguishes between functional and management and operational aspects of an application. It builds on the concept of providing a run-time environment that offers all sorts of facilities to an application.

In this concept, the application covers the functional aspects, and the environment covers all management and operational aspects. Application developers should, by definition, focus on the functional aspects of an application, while others can focus on the creation of the environment that provides the necessary management and operational services. This means that the application developers focus on the requirements of the business, while the architecture developers or application framework developers focus on the requirements of the application developers.

5.3.9 Developing individual applications

Once the design phase is completed, the application development team will take the designs that have been produced and move on to developing the application. Both the application and the related environment are

made ready for deployment. Application components are coded or acquired, integrated and tested.

To ensure that the application is developed with management at the core, the development team needs to focus on ensuring that the developing phase continues to correctly address the management and operational aspects of the design (e.g. responsiveness, availability, security).

The development phase guidance covers the following topics:

- Consistent coding conventions
- Application-independent building guidelines
- Operability testing
- Management checklist for the building phase
- Organization of the build team roles.

5.3.10 Consistent coding conventions

The main reason for using a consistent set of design and coding conventions is to standardize the structure and coding style of an application so that everyone can easily read, understand and manage the application development process. Good design and coding conventions result in precise, readable and unambiguous source code that is consistent with the organizational coding and management standards and is as intuitive to follow as possible. Adding application operability into this convention ensures that all applications are built in a way that ensures that they can be fully managed all the way through their lifecycles.

A coding convention itself can be a significant aid to managing the application, as consistency allows the management tools to interact with the application in a known way. It is better to introduce a minimum set of conventions that everyone will follow rather than to create an overly complex set that encompasses every facet but is not followed or used consistently across the organization.

5.3.11 Templates and code generation

A number of development tools provide a variety of templates for creating common application components. Rather than creating all the pieces of an application from scratch, developers can customize an existing template. They can also re-use custom components in multiple applications by creating their own templates. Other development tools will generate large pieces of code (skeletons) based on the design models and coding conventions. The code could include hooks at the code

pieces that need to be added.

In this respect, templates and application frameworks should be considered IT assets. These assets not only guide the developing of applications, but also incorporate the lessons learned or intellectual capital from previous application development efforts. The more that standard components are designed into the solution, the faster applications can be developed, against lower costs in the long term (not ignoring the fact that development of templates, code generators and application frameworks requires significant investment).

5.3.12 Embedded application instrumentation

The development phase deals with incorporating instrumentation into the fabric of the application. Developers need a consistent way to provide instrumentation for application drivers/middleware components (e.g. database drivers) and applications that is efficient and easy to implement. To keep application developers from reinventing the wheel with every new application they develop, the computer industry provides methods and technologies to simplify and facilitate the instrumentation process.

These include:

- Application Response Measurement (ARMS)
- IBM Application Management Specification (AMS)
- Common Information Model (CIM) and Web-Based Enterprise Management (WBEM) from the Distributed Management Task Force (DMTF)
- Desktop Management Instrumentation (DMI)
- Microsoft Windows® Management Instrumentation (WMI)
- Java Management Extension (JMX).

Each of these technologies provides a consistent and richly descriptive model of the configuration, status and operational aspects of applications and services. These are provided through programming Application Program Interfaces (APIs) that the developer incorporates into an application, normally through the use of standard programming templates.

It is important to ensure that all applications are built to conform to some level of compliance for the application instrumentation. Ways to do this could include:

- Provide access to management data through the instrumentation API

- Publish management data to other management systems, again through the instrumentation API
- Provide applications event handling
- Provide a diagnostic hook.

5.3.13 Diagnostic hooks

Diagnostic hooks are of greatest value during testing and when an error has been discovered in the production service. Diagnostic hooks mainly provide the information necessary to solve problems and application errors rapidly and restore service. They can also be used to provide measurement and management information of applications.

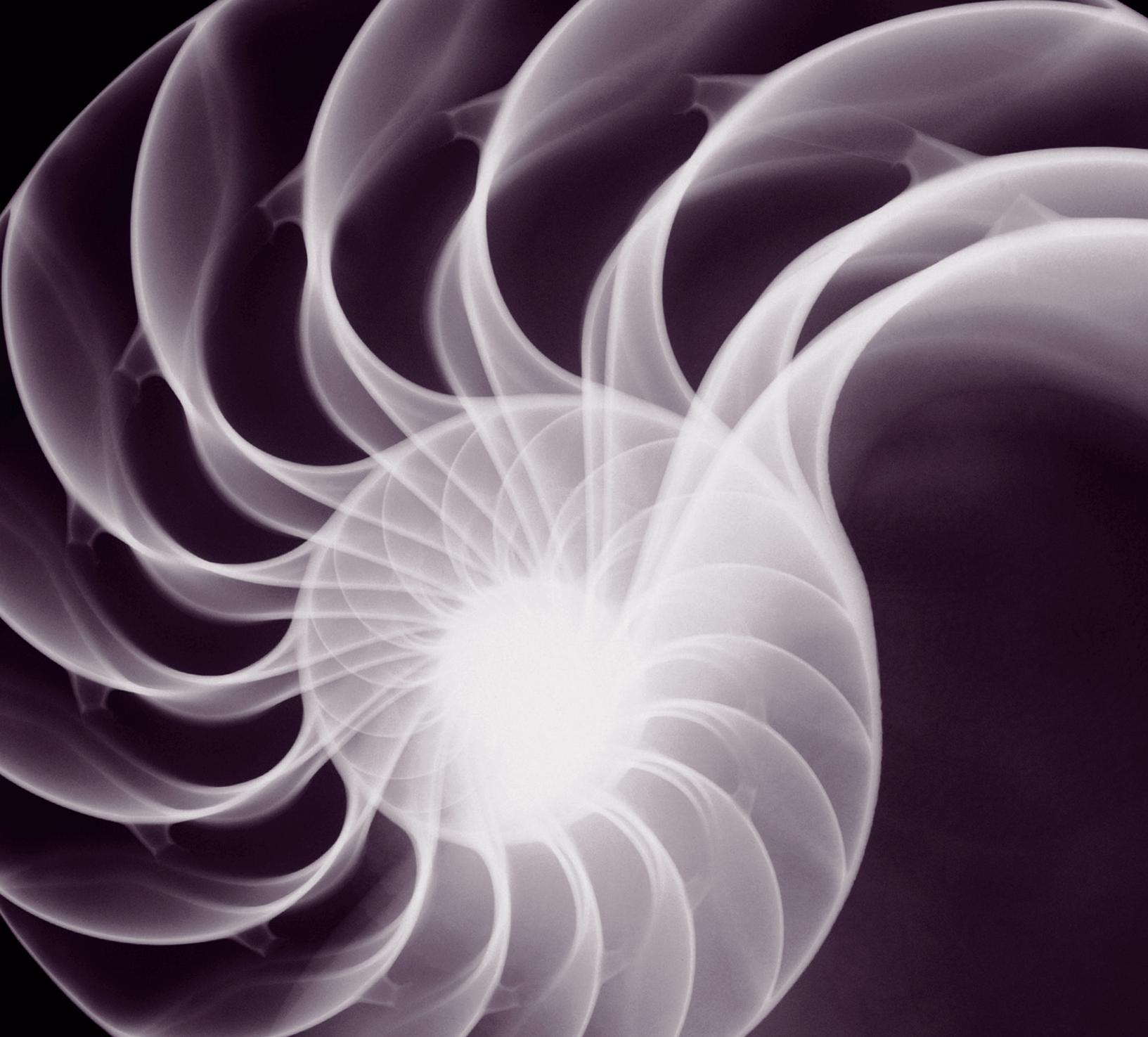
The three main categories are:

- System-level information provided by the OS and hardware
- Software-level information provided by the application infrastructure components such as database, web server or messaging systems
- Custom information provided by the applications
- Information on component and service performance.

5.3.14 Major service outputs from development

The major outputs from the development phase are:

- Scripts to be run before or after deployment
- Scripts to start or stop the application
- Scripts to check hardware and software configurations of target environments before deployment or installation
- Specification of metrics and events that can be retrieved from the application and that indicate the performance status of the application
- Customized scripts initiated by Service Operation staff to manage the application (including the handling of application upgrades)
- Specification of access control information for the system resources used by an application
- Specification of the details required to track an application's major transactions
- SLA targets and requirements
- Operational requirements and documentation
- Support requirements
- Application recovery and backups
- Other IT SM requirements and targets.



Organizing for Service Design

6

6 Organizing for Service Design

For Service Design to be successful, it is essential to define the roles and responsibilities within the organization of the various activities.

When designing a service or a process, it is imperative that all the roles are clearly defined. A trademark of high-performing organizations is the ability to make the right decisions quickly and execute them effectively. Whether the decision involves a strategic choice or a critical operation, being clear on who has input, who decides and who takes action will enable the company to move forward rapidly.

The RACI model will be beneficial in enabling decisions to be made with pace and confidence. RACI is an acronym for the four main roles of:

- **Responsible** – the person or people responsible for getting the job done
- **Accountable** – only one person can be accountable for each task
- **Consulted** – the people who are consulted and whose opinions are sought
- **Informed** – the people who are kept up-to-date on progress.

Occasionally an expanded version of RACI is used called RACI-VS, with two further roles as follows:

- **Verifies** – the person or group that checks whether the acceptance criteria have been met
- **Signs off** – the person who approves the V decision and authorizes the product hand-off. This could be the A person.

A third variation of the RACI model is RASCI, where the S represents Supportive. This role provides additional resources to conduct the work, or plays a supportive role

in implementation, for example. This could be beneficial for IT service implementation.

The RACI chart in Table 6.1 shows the structure and power of RACI modelling with the activities down the left-hand side including the actions that need to be taken and decisions that must be made. Across the top, the chart lists the functional roles responsible for carrying out the initiative or playing a part in decision making.

Whether RACI or some other tool or model is used, the important thing is to not just leave the assignment of responsibilities to chance or leave it to the last minute to decide. Conflicts can be avoided and decisions can be made quickly if the roles are allocated in advance.

To build a RACI chart the following steps are required:

- Identify the activities/processes
- Identify/define the functional roles
- Conduct meetings and assign the RACI codes
- Identify any gaps or overlaps – for example, where there are two Rs or no Rs (see analysis below)
- Distribute the chart and incorporate feedback
- Ensure that the allocations are being followed.

6.1 FUNCTIONAL ROLES ANALYSIS

- **Many As:** Are duties segregated properly? Should someone else be accountable for some of these activities? Is this causing a bottleneck in some areas that will delay decisions?
- **Many Rs:** Is this too much for one function?
- **No empty spaces:** Does this role need to be involved in so many tasks?
- Also, does the type or degree of participation fit this role's qualifications?

Table 6.1 Example RACI matrix

	Director Service Management	Service Level Manager	Problem Manager	Security Manager	Procurement Manager
Activity 1	AR	C	I	I	C
Activity 2	A	R	C	C	C
Activity 3	I	A	R	I	C
Activity 4	I	A	R	I	
Activity 5	I	I	A	C	I

6.2 ACTIVITY ANALYSIS

- More than one A: only one role can be accountable.
- No As: at least one A must be assigned to each activity.
- More than one R: too many roles responsible often means that no one takes responsibility. Responsibility may be shared, but only if roles are clear.
- No Rs: at least one person must be responsible.
- Many Cs: Is there a requirement to consult with so many roles? What are the benefits and can the extra time be justified?
- No Cs and Is: Are the communication channels open to enable people and departments to talk to each other and keep each other up-to-date?

6.3 SKILLS AND ATTRIBUTES

The specific roles within ITIL Service Management all require specific skills, attributes and competences from the people involved to enable them to work effectively and efficiently. However, whatever the role, it is imperative that the person carrying out that role has the following attributes:

- Awareness of the business priorities, objectives and business drivers
- Awareness of the role IT plays in enabling the business objectives to be met
- Customer service skills
- Awareness of what IT can deliver to the business, including latest capabilities
- The competence, knowledge and information necessary to complete their role
- The ability to use, understand and interpret the best practice, policies and procedures to ensure adherence.

The following are examples of attributes required in many of the roles, dependent on the organization and the specific role:

- **Management skills** – both from a person management perspective and from the overall control of process
- **Meeting skills** – to organize, chair, document and ensure actions are followed up
- **Communications** – an important element of all roles is raising awareness of the processes in place to ensure buy-in and conformance. An ability to communicate at all levels within the organization will be imperative
- **Articulate** – both written, for reports etc., and verbal

- **Negotiation** – required for several aspects, such as procurement and contracts
- **Analytical** – to analyse metrics produced from the activity.

More information about the skills and competences of these roles can be found within the Skills Framework for the Information Age (SFIA – www.sfia.org.uk).

6.4 ROLES AND RESPONSIBILITIES

The following sections document the roles and responsibilities of the various roles within Service Design. In some organizations this could be a full-time individual and in others it could be several people, or it could be a part-time role. In smaller organizations many of these roles may be performed by a single person. This will depend on the size and volatility of the organization. The roles or job titles often vary between organizations. However, what is important is that the roles, responsibilities, processes, dependencies and interfaces are clearly defined and scoped for each individual organization. (See Appendix C for an example process document template.)

The following are illustrations of the main activities within each of the Service Design roles.

6.4.1 Process owner

A process owner is responsible for ensuring that their process is being performed according to the agreed and documented process and is meeting the aims of the process definition. This includes such tasks as:

- Documenting and publicizing the process
- Defining the Key Performance Indicators (KPIs) to evaluate the effectiveness and efficiency of the process
- Reviewing KPIs and taking action required following the analysis
- Assisting with and being ultimately responsible for the process design
- Improving the effectiveness and efficiency of the process
- Reviewing any proposed enhancements to the process
- Providing input to the ongoing Service Improvement Plan
- Addressing any issues with the running of the process
- Ensuring all relevant staff have the required training in the process and are aware of their role in the process
- Ensures that the process, roles, responsibilities and documentation are regularly reviewed and audited
- Interfaces with line management, ensuring that the process receives the necessary staff resources. (Line

management and process owners have complementary tasks – they need to work together to ensure efficient and effective processes. Often it is the task of line management to ensure the required training of staff.)

6.4.2 Service Design Manager

The key role and responsibilities of the Service Design Manager are covered throughout this publication and they are responsible for the overall coordination and deployment of quality solution designs for services and processes. Responsibilities of the role over and above those of line management of all people involved in Service Design roles include:

- Taking the overall Service Strategies and ensuring they are reflected in the Service Design practice and the Service Designs that are produced to meet and fulfil the documented business requirements
- Designing the functional aspects of the services as well as the infrastructure, environment applications and data management
- Producing quality, secure and resilient designs for new or improved services, technology architecture, processes or measurement systems that meet all the agreed current and future IT requirements of the organization
- Producing and maintaining all design documentation, including designs, plans, architectures and policies
- Producing and maintaining all necessary SDPs
- Measuring the effectiveness and efficiency of the Service Design process.

6.4.3 IT Planner

An IT Planner is responsible for the production and coordination of IT plans. The main objectives of the role are as follows:

- Develop IT plans that meet and continue to meet the IT requirements of the business.
- Coordinate, measure and review the implementation progress of all IT strategies and plans.
- Produce and maintain the overall set of IT standards, policies, plans and strategies, encompassing all aspects of IT required to support an organization's business strategy. IT planning includes participation in the creation of SLAs and the planning of all aspects of infrastructure – internal and external, public or private, internet and intranet – necessary to ensure that the provision of IT services satisfies business.
- Assume responsibility for all aspects of IT standards, policy and strategy implementation for IT as a whole

and for significant projects or major new strategic applications.

- Recommend policy for the effective use of IT throughout the organization and work with IT Designers to ensure that overall plans and strategies are developed in conjunction with IT design for all areas of IT.
- Review IT costs against budgets and new developments, initiating proposals to change IT plans and strategies where appropriate, in conjunction with Financial Management.
- Assume full responsibility for the management, planning and coordination of IT systems and services, including investigation, analysis, specification, design, development, testing, maintenance, upgrade, transition and operation. It is essential that while performing these activities, the business, IT Management and all the Service Management processes are kept up-to-date with the progress of projects.
- Obtain and evaluate proposals from suppliers of equipment, software, transmission services and other services, ensuring that all business and IT requirements are satisfied.
- Identify internal and external influencing factors, forecast future needs and set plans for the effective use of IT within the organization.
- Sponsor and monitor research, development and long-term planning for the provision and use of IT architectures, products and services
- Review IT performance with all other areas and initiate any improvements in organization to ensure that service levels and targets continue to be met in all areas.
- Take ultimate responsibility for prioritizing and scheduling the implementation of new or changed services within IT.
- Work with senior management and other senior specialists and planners in formulating plans and making procurement decisions applicable to all areas of IT.
- Recognize the key business drivers and those areas of business need that are not adequately supported by current and planned IT services, developing the plans and IT response to the business requirements.
- Identify suitable applications, services and products, together with their environments, to meet business needs within the required planning timeframe.
- Develop the initial plans for the implementation of authorized new IT services, applications and infrastructure support, identifying budgetary, technical

and staffing constraints, and clearly listing costs and expected benefits.

- Monitor the existing IT plans in relation to business needs and IT strategy to determine opportunities for improving business processes through the use of new technology, and to identify unforeseen risks to the achievement of forecast business benefit.
- Investigate major options for providing IT services effectively and efficiently and recommend new innovative solutions, based on new approaches to processes, provision, recruitment and retention, and global supply contracts.
- Produce feasibility studies, business models, IT models, business cases, SoRs and ITTs for recommended new IT systems, identifying the business impact, the probability of satisfying business needs, the anticipated business benefits and the risks and consequences of failure.
- Oversee and coordinate the programme of planned IT project implementations and changes, taking appropriate action to identify and overcome problems and resolve conflict.
- Conduct Post Implementation Reviews (PIRs) in conjunction with Change Management of those information systems introduced in pursuit of the plans, to assess the extent to which expected business benefits were realized.
- Liaise with Strategy, Transition and Operations teams and processes to plan for their immediate and future needs.
- Provide authoritative advice and guidance on relevant national and international standards, regulations, protocols and tariffs.
- Document all work using required standards, methods and tools.
- Ensure that all IT planning processes, roles, responsibilities and documentation are regularly reviewed and audited for efficiency, effectiveness and compliance.
- Maintain a good overall knowledge of all IT product capabilities and the technical frameworks in which they operate.
- Where required, assess changes for their conformance to the design strategies, including attendance at CAB meetings if appropriate.

6.4.4 IT Designer/Architect

An IT Designer/Architect is responsible for the overall coordination and design of the required technology. Often Designers and Architects within large organizations would

specialize in one of the five aspects of design (see section 3). However, an integrated approach to design should always be adopted, therefore Designers and Architects need to work together within a formal method and framework to ensure consistent and compatible designs are produced. In smaller organizations, some or all of the roles are usually combined, and this is less of an issue, although a formal approach should still be used.

Whenever designs are produced, they should always adopt an integrated approach, covering all areas, and should be accepted and signed off by all areas. All designers need to understand how architectures, strategies, designs and plans fit together and all the main aspects of design.

The Designer/Architect should produce a detailed process map that documents all the processes and their high-level interfaces. This ensures that the overall structure is not unnecessarily complex, that the process's central interfaces are part of the design, and provides an overview to everyone on how the customer and all other stakeholders interact with the processes.

To perform the role of Designer or Architect, it is necessary for staff to have good knowledge and practical experience of design philosophies and planning, including Programme, Project and Service Management, methods and principles. The main objectives of the IT Designer/Architect are as follows:

- Produce and review the designs of all new or changed services, SLAs, OLAs and contracts.
- Produce a process map of all of the processes and their high-level interfaces, to ensure integration, consistency and continuity across all processes.
- Design secure and resilient technology architectures that meet all the current and anticipated future IT requirements of the organization.
- Ensure that the design of all processes, roles, responsibilities and documentation is regularly reviewed and audited for efficiency, effectiveness and compliance.
- Design an appropriate and suitable Service Portfolio, supporting all activities within the complete Service Lifecycle.
- Design measurement systems and techniques to support the continual improvement of service provision and all supporting processes.
- Produce and keep up-to-date all IT design, architectural, policy and specification documentation.
- Produce and maintain all aspects of IT specification, including the overall designs, architectures, topologies and configurations of the infrastructure, environment, applications and data, and the design documentation

- of all IT systems. This should include not just the technology, but also the management systems, processes, information flows and external services.
- Recommend proactive, innovative IT solutions for the improvement of IT design and operation whenever and wherever possible.
 - Translate logical designs into physical designs, taking account of business requirements, target environments, processes, performance requirements, existing systems and services, and any potential safety-related aspects.
 - Create and maintain IT design policies, philosophies and criteria, covering all areas including connectivity, capacity, interfaces, security, resilience, recovery, access and remote access, and ensuring that all new services meet their service levels and targets.
 - Work with Capacity Management and review IT traffic volumes and requirements, identifying trends in traffic flows and levels of service.
 - Propose design enhancements to IT infrastructure, capacity changes, continuity, backup and recovery arrangements, as required, and be aware of operational requirements, especially in terms of service levels, availability, response times, security and repair times. All these activities are performed in liaison with all of the Service Management processes.
 - Review IT costs against external service providers, new developments and new services, initiating proposals to change IT design where appropriate cost reductions and benefits can be achieved, in consultation with Financial Management.
 - Provide advice and guidance to management on the design and planning phases of IT systems, to ensure that requirements (particularly capacity, recovery, performance and security needs) are reflected in the overall specifications.
 - Provide advice and guidance to all areas of IT and Business Management, analysts, planners, designers and developers on all aspects of IT design and technology.
 - Interface with designers and planners from external suppliers and service providers, ensuring all external IT services are designed to meet their agreed service levels and targets.
 - Play a major role in the selection of any new IT infrastructure or technology solutions.

- Assume technical responsibility for IT standards, policy and design for all significant projects or major application areas, assisting with the Impact Assessment and evaluation of major new IT design options.
- Provide technical advice and guidance on relevant national and international standards, regulations, protocols and tariffs.
- Take full responsibility for the design aspects of all stages of the lifecycle of IT systems, including investigation, analysis, specification, design, development, construction, testing, maintenance, upgrade, transition, operation and improvement.
- Work with IT colleagues where appropriate, producing or updating IT and corporate design documentation and models.
- Update or provide input to cost-benefit analyses, risk analyses, business cases, SoRs and ITTs and development plans, to take account of design decisions.
- Obtain and assist with the evaluation and selection of proposals and solutions from suppliers of equipment, software and other IT service and product providers.
- Construct, interpret and monitor test plans to verify correct operation of completed systems against their design objectives.
- Document all work using required standards, methods and tools.
- Maintain a good technical knowledge of all IT product capabilities and the technical frameworks in which they operate.
- Where required, assess changes for their conformance to the design principles, including attendance at CAB meetings if appropriate.

Note: Often Designers and Architects within large organisations would specialise in one of the five aspects of design (see sections 3 and 4 for more detail). However, an integrated approach to design should always be adopted, therefore Designers and Architects need to work together within a formal method and framework to ensure consistent and compatible designs are produced. In smaller organisations, some or all of the roles are usually combined, and this is less of an issue, although a formal approach should still be used. Whenever designs are produced, they should always adopt a holistic approach, covering all areas, and should be accepted and signed off by all areas. All Designers need to understand how architectures, strategies, designs and plans fit together.

6.4.5 Service Catalogue Manager

The Service Catalogue Manager has responsibility for producing and maintaining the Service Catalogue. This includes responsibilities such as:

- Ensuring that all operational services and all services being prepared for operational running are recorded within the Service Catalogue
- Ensuring that all the information within the Service Catalogue is accurate and up-to-date
- Ensuring that all the information within the Service Catalogue is consistent with the information within the Service Portfolio
- Ensuring that the information within the Service Catalogue is adequately protected and backed up.

6.4.6 Service Level Manager

The Service Level Manager has responsibility for ensuring that the aims of Service Level Management are met. This includes responsibilities such as:

- Keeping aware of changing business needs
- Ensuring that the current and future service requirements of customers are identified, understood and documented in SLA and SLR documents
- Negotiating and agreeing levels of service to be delivered with the customer (either internal or external); formally documenting these levels of service in SLAs
- Negotiating and agreeing OLAs and, in some cases, other SLAs and agreements that underpin the SLAs with the customers of the service
- Assisting with the production and maintenance of an accurate Service Portfolio, Service Catalogue, Application Portfolio and the corresponding maintenance procedures
- Ensuring that targets agreed within underpinning contracts are aligned with SLA and SLR targets
- Ensuring that service reports are produced for each customer service and that breaches of SLA targets are highlighted, investigated and actions taken to prevent their recurrence
- Ensuring that service performance reviews are scheduled, carried out with customers regularly and are documented with agreed actions progressed
- Ensuring that improvement initiatives identified in service reviews are acted on and progress reports are provided to customers

- Reviewing service scope, SLAs, OLAs and other agreements on a regular basis, ideally at least annually
- Ensuring that all changes are assessed for their impact on service levels, including SLAs, OLAs and underpinning contracts, including attendance at CAB meetings if appropriate
- Identifying all key stakeholders and customers
- Developing relationships and communication with stakeholders, customers and key users
- Defining and agreeing complaints and their recording, management, escalation, where necessary, and resolution
- Definition recording and communication of all complaints
- Measuring, recording, analysing and improving customer satisfaction.

6.4.7 Availability Manager

An Availability Manager has responsibility for ensuring that the aims of Availability Management are met. This includes responsibilities such as:

- Ensuring that all existing services deliver the levels of availability agreed with the business in SLAs
- Ensuring that all new services are designed to deliver the levels of availability required by the business, and validation of the final design to meet the minimum levels of availability as agreed by the business for IT services
- Assisting with the investigation and diagnosis of all incidents and problems that cause availability issues or unavailability of services or components
- Participating in the IT infrastructure design, including specifying the availability requirements for hardware and software
- Specifying the requirements for new or enhanced event management systems for automatic monitoring of availability of IT components
- Specifying the reliability, maintainability and serviceability requirements for components supplied by internal and external suppliers
- Being responsible for monitoring actual IT availability achieved against SLA targets, and providing a range of IT availability reporting to ensure that agreed levels of availability, reliability and maintainability are measured and monitored on an ongoing basis
- Proactively improving service availability wherever possible, and optimizing the availability of the IT infrastructure to deliver cost-effective improvements that deliver tangible benefits to the business

- Creating, maintaining and regularly reviewing an AMIS and a forward-looking Availability Plan, aimed at improving the overall availability of IT services and infrastructure components, to ensure that existing and future business availability requirements can be met
- Ensuring that the Availability Management process, its associated techniques and methods are regularly reviewed and audited, and that all of these are subject to continual improvement and remain fit for purpose
- Creating availability and recovery design criteria to be applied to new or enhanced infrastructure design
- Working with Financial Management, ensuring the levels of IT availability required are cost-justified
- Maintaining and completing an availability testing schedule for all availability mechanisms
- Ensuring that all availability tests and plans are tested after every major business change
- Assisting Security and **IT Service** Continuity Management with the assessment and management of risk
- Assessing changes for their impact on all aspects of availability, including overall service availability and the Availability Plan
- Attending CAB meetings when appropriate.

6.4.8 IT Service Continuity Manager

The **IT Service** Continuity Manager is responsible for ensuring that the aims of **IT Service** Continuity Management are met. This includes such tasks and responsibilities as:

- Performing Business Impact Analyses for all existing and new services
- Implementing and maintaining the ITSCM process, in accordance with the overall requirements of the organization's Business Continuity Management process, and representing the IT services function within the Business Continuity Management process
- Ensuring that all ITSCM plans, risks and activities underpin and align with all BCM plans, risks and activities, and are capable of meeting the agreed and documented targets under any circumstances
- Performing risk assessment and risk management to prevent disasters where cost-justifiable and where practical
- Developing and maintaining the organization's continuity strategy
- Assessing potential service continuity issues and invoking the Service Continuity Plan if necessary

- Managing the Service Continuity Plan while it is in operation, including fail-over to a secondary location and restoration to the primary location
- Performing post mortem reviews of service continuity tests and invocations, and instigating corrective actions where required
- Developing and managing the ITSCM plans to ensure that, at all times, the recovery objectives of the business can be achieved
- Ensuring that all IT service areas are prepared and able to respond to an invocation of the continuity plans
- Maintaining a comprehensive IT testing schedule, including testing all continuity plans in line with business requirements and after every major business change
- Undertaking quality reviews of all procedures and ensuring that these are incorporated into the testing schedule
- Communicating and maintaining awareness of ITSCM objectives within the business areas supported and IT service areas
- Undertaking regular reviews, at least annually, of the Continuity Plans with the business areas to ensure that they accurately reflect the business needs
- Negotiating and managing contracts with providers of third-party recovery services
- Assessing changes for their impact on Service Continuity and Continuity Plans
- Attending CAB meetings when appropriate.

6.4.9 Capacity Manager

A Capacity Manager has responsibility for ensuring that the aims of Capacity Management are met. This includes such tasks as:

- Ensuring that there is adequate IT capacity to meet required levels of service, and that senior IT management is correctly advised on how to match capacity and demand and to ensure that use of existing capacity is optimized
- Identifying, with the Service Level Manager, capacity requirements through discussions with the business users
- Understanding the current usage of the infrastructure and IT services, and the maximum capacity of each component
- Performing sizing on all proposed new services and systems, possibly using modelling techniques, to ascertain capacity requirements
- Forecasting future capacity requirements based on business plans, usage trends, sizing of new services, etc.

- Production, regular review and revision of the Capacity Plan, in line with the organization's business planning cycle, identifying current usage and forecast requirements during the period covered by the plan
- Ensuring that appropriate levels of monitoring of resources and system performance are set
- Analysis of usage and performance data, and reporting on performance against targets contained in SLAs
- Raising incidents and problems when breaches of capacity or performance thresholds are detected, and assisting with the investigation and diagnosis of capacity-related incidents and problems
- Identifying and initiating any tuning to be carried out to optimize and improve capacity or performance
- Identifying and implementing initiatives to improve resource usage – for example, demand management techniques
- Assessing new technology and its relevance to the organization in terms of performance and cost
- Being familiar with potential future demand for IT services and assessing this on performance service levels
- Ensuring that all changes are assessed for their impact on capacity and performance and attending CAB meetings when appropriate
- Producing regular management reports that include current usage of resources, trends and forecasts
- Sizing all proposed new services and systems to determine the computer and network resources required, to determine hardware utilization, performance service levels and cost implications
- Assessing new techniques and hardware and software products for use by Capacity Management that might improve the efficiency and effectiveness of the process
- Performance testing of new services and systems
- Reports on service and component performance against targets contained in SLAs
- Maintaining a knowledge of future demand for IT services and predicting the effects of demand on performance service levels
- Determining performance service levels that are maintainable and cost-justified
- Recommending tuning of services and systems, and making recommendations to IT management on the design and use of systems to help ensure optimum use of all hardware and operating system software resources
- Acting as a focal point for all capacity and performance issues.

6.4.10 Security Manager

The Security Manager is responsible for ensuring that the aims of Information Security Management are met. This includes such tasks and responsibilities as:

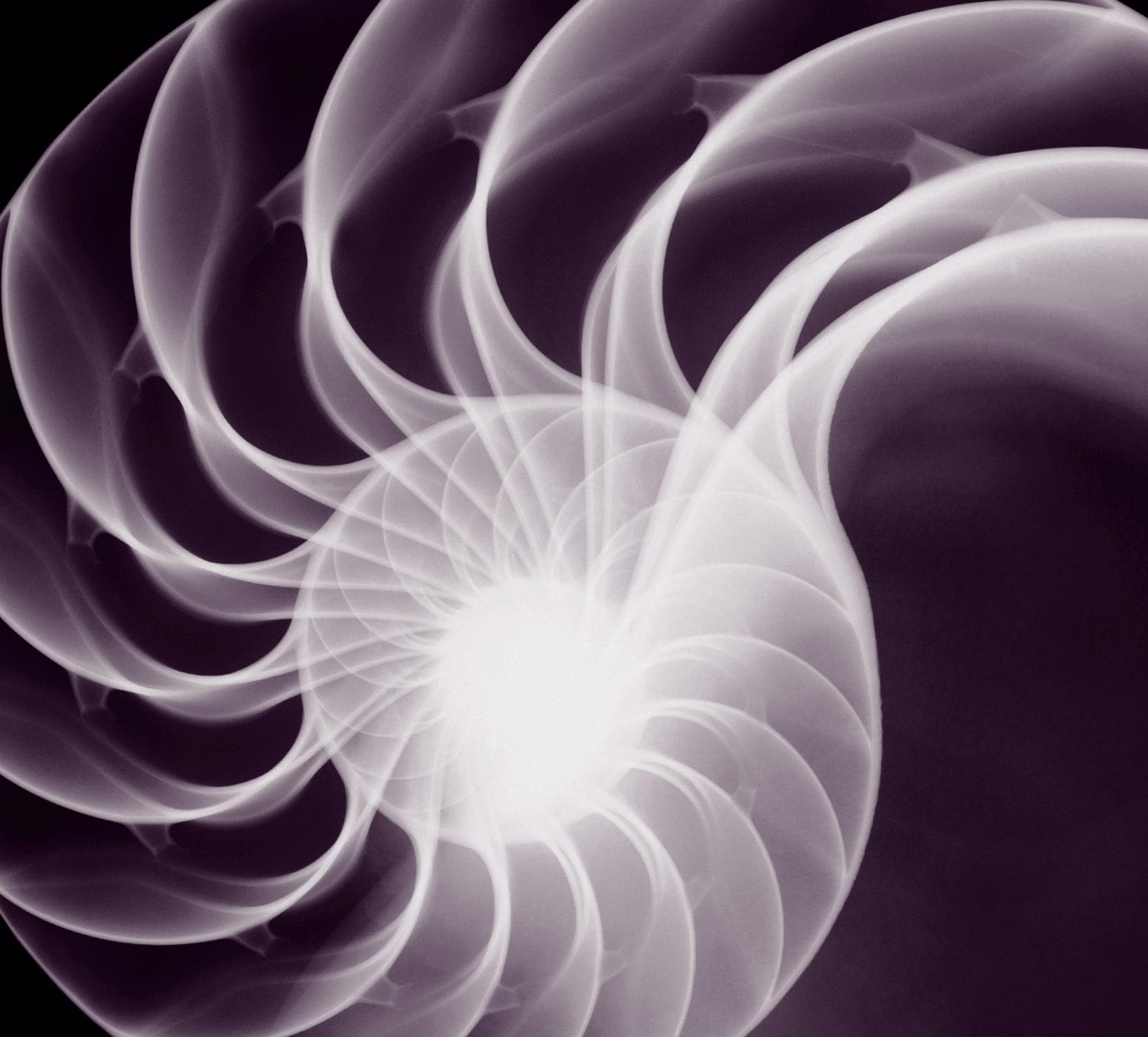
- Developing and maintaining the Information Security Policy and a supporting set of specific policies, ensuring appropriate authorization, commitment and endorsement from senior IT and business management
- Communicating and publicizing the Information Security Policy to all appropriate parties
- Ensuring that the Information Security Policy is enforced and adhered to
- Identifying and classifying IT and information assets (Configuration Items) and the level of control and protection required
- Assisting with Business Impact Analyses
- Performing Security Risk Analysis and risk management in conjunction with Availability and **IT Service Continuity Management**
- Designing security controls and developing security plans
- Developing and documenting procedures for operating and maintaining security controls
- Monitoring and managing all security breaches and handling security incidents, taking remedial action to prevent recurrence wherever possible
- Reporting, analysing and reducing the impact and volumes of all security incidents in conjunction with Problem Management
- Promoting education and awareness of security
- Maintaining a set of security controls and documentation, and regularly reviewing and auditing all security controls and procedures
- Ensuring all changes are assessed for impact on all security aspects, including the Information Security Policy and security controls, and attending CAB meetings when appropriate
- Performing security tests
- Participating in any security reviews arising from security breaches and instigating remedial actions
- Ensuring that the confidentiality, integrity and availability of the services are maintained at the levels agreed in the SLAs and that they conform to all relevant statutory requirements
- Ensuring that all access to services by external partners and suppliers is subject to contractual agreements and responsibilities
- Acting as a focal point for all security issues.

6.4.11 Supplier Manager

The Supplier Manager has responsibility for ensuring that the aims of Supplier Management are met. This includes tasks such as:

- Providing assistance in the development and review of SLAs, contracts, agreements or any other documents for third-party suppliers
- Ensuring that value for money is obtained from all IT suppliers and contracts
- Ensuring that all IT supplier processes are consistent and interface to all corporate supplier strategies, processes and standard terms and conditions
- Maintaining and reviewing a Supplier and Contracts Database (SCD)
- Review and Risk Analysis of all suppliers and contracts on a regular basis
- Ensuring that any underpinning contracts, agreements or SLAs developed are aligned with those of the business
- Ensuring that all supporting services are scoped and documented and that interfaces and dependencies between suppliers, supporting services and supplier processes are agreed and documented
- Ensuring that all roles and relationships between lead and any sub-contracted suppliers are documented, maintained and subject to contractual agreement
- Reviewing lead suppliers' processes to ensure that any sub-contracted suppliers are meeting their contractual obligations
- Performing contract or SLA reviews at least annually, and ensuring that all contracts are consistent with organizational requirements and standard terms and conditions wherever possible
- Updating contracts or SLAs when required, ensuring that the Change Management process is followed
- Maintaining a process for dealing with contractual disputes, and ensuring that any disputes are dealt with in an efficient and effective manner
- Maintaining a process for dealing with the expected end, early end or transfer of a service

- Monitoring, reporting and regularly reviewing supplier performance against targets, identifying improvement actions as appropriate and ensuring these actions are implemented
- Ensuring changes are assessed for their impact on suppliers, supporting services and contracts and attending CAB meetings when appropriate
- Coordinating and supporting all individual IT supplier and contract managers, ensuring that each supplier/contract has a nominated owner within the service provider organization.



Technology considerations

7

7 Technology considerations

It is generally recognized that the use of Service Management tools is essential for the success of all but the very smallest process implementations. However, it is important that the tool being used supports the processes – not the other way around. As a general rule, don't modify processes to fit the tool. However, with the use of tools to support processes, there is a need to be pragmatic and recognize that there may not be a tool that supports the designed process totally, so an element of process re-design may be necessary. Don't limit the requirements to functionality: consider the product's ability to perform, enlarge the size of the databases, recover from failure and maintain data integrity. Does the product conform to international standards? Is it efficient enough to enable you to meet your Service Management Requirements?

Often organizations believe that by purchasing or developing a tool all their problems will be solved, and it is easy to forget that we are still dependent on the process, the function and, most importantly, the people. Remember:

'a fool with a tool is still a fool'

7.1 SERVICE DESIGN TOOLS

There are many tools and techniques that can be used to assist with the design of services and their associated components. These tools and techniques enable:

- Hardware design
- Software design
- Environmental design
- Process design
- Data design.

The tools and techniques are many and varied, including both proprietary and non-proprietary, and are useful in:

- Speeding up the design process
- Ensuring that standards and conventions are followed
- Offering prototyping, modelling and simulation facilities
- Enabling 'What if?' scenarios to be examined
- Enabling interfaces and dependencies to be checked and correlated
- Validating designs before they are developed and implemented to ensure that they satisfy and fulfil their intended requirements.

Developing Service Designs can be simplified by the use of tools that provide graphical views of the service and its constituent components, from the business processes, through the service and SLA to the infrastructure, environment, data and applications, processes, OLAs, teams, contracts and suppliers. Some Configuration Management tools provide such facilities, and are sometimes referred to as an element of Business Service Management (BSM) tools. They can contain or be linked to 'auto-discovery' tools and mechanisms and allow the relationships between all of these elements to be graphically represented, providing the ability to drill down within each component and obtain detailed information if needed.

If these types of tool also contain financial information, and are then linked to a 'Metrics Tree' providing KPIs and metrics of the various aspects of the service, then the service can be monitored and managed through all stages of its lifecycle. Sharing this single, centralized set of service information allows everybody in the service provider organization and the business to access a single, consistent, 'real-world' view of the service and its performance, and provides a solid base for the development of good relationships and partnerships between the service provider and its customers.

These types of tools not only facilitate the design processes, but also greatly support and assist all stages in the Service Lifecycle, including:

- Management of all stages of the Service Lifecycle
- All aspects of the service and its performance
- Service achievement, SLA, OLA, contractual and supplier measurement, reporting and management
- Consolidated metrics and Metrics Trees, with views from management dashboards down to detailed component information, performance and fault analysis and identification
- Consistent and consolidated views across all processes, systems, technologies and groups
- Relationships and integration of the business and its processes with IT services, systems and processes
- A comprehensive set of search and reporting facilities, enabling accurate information and analysis for informed decision-making
- Management of service costs
- Management of relationships, interfaces and inter-dependencies

- Management of the Service Portfolio and Service Catalogue
- A Configuration Management System (CMS)
- A Service Knowledge Management System (SKMS).

The following generic activities will be needed to implement such an approach:

- Establish the generic lifecycle for IT Assets (Requirements, Design and Develop, Build, Test, Deploy, Operate and Optimize, Dispose) and define the principal processes, policies, activities and technologies within each stage of the lifecycle for each type of asset
- Formalize the relationships between different types of IT asset, and the relationship between IT asset acquisition and management and other IT disciplines
- Define all roles and responsibilities involved in IT asset activities
- Establish measures for understanding the (Total) Cost of Ownership of an IT service
- Establish policies for the re-use of IT assets across services, e.g. at the corporate level
- Define a strategy for the acquisition and management of IT assets, including how it should be aligned with other IT and business strategies.

For the applications asset type, additionally:

- Define a strategy for the acquisition and management of IT assets, including how it should be aligned with other IT and business strategies
- Document the role played by applications in the delivery of IT services to the business
- Ensure the generic IT asset lifecycle model is adapted to an applications lifecycle, tailored to different application types
- Set standards for the use of different approaches to developing applications, and recognize the role of development methodologies, including those based on 're-use' (see the section on Design and Development for further discussion)
- Ensure that procedures are in place to consider all requirement types (such as operability, service performance, maintainability, security) in the early stages of application development
- Set standards for deciding on the optimal delivery of applications to the organization, such as the use of Application Service Providers, customized developments, COTS and package customization.

For the data/information asset type, additionally:

- Establish how the general principles of IT asset acquisition and management can help to manage the data/information resources of an organization.

Ensure that data designs are undertaken in the light of:

- The importance of standardized and re-usable metadata
- The need for data quality
- The value of data to an organization
- The need for data administration and database administration skills
- Understanding the 'corporate' (or common/cooperative) subject area and individual service ('system') views of data
- The need to manage data of non-traditional data types such as text, scanned images, video and audio
- Awareness of the major storage, security and legal issues for data
- Specify how the generic IT assets lifecycle model can be adapted to the data asset type.

For the IT infrastructure and environmental asset type, additionally:

- Establish standards for acquisition and management of the IT infrastructure and environmental equipment (including hardware, power, O/S software, dbms software, middleware and networks) and ensure they provide a stable yet adaptable foundation that underpins the provision of IT services to the business
- Establish how the generic IT assets lifecycle model should be adapted to a specific IT infrastructure lifecycle
- Establish activities to optimize the usage of IT infrastructure assets through their re-use
- Specify the need for tools and describe how their overall use and integration assists in the management of an effective IT infrastructure and related services.

For the skills (people, competencies), additionally:

- Formalize how the competencies of individuals responsible for the IT assets and related services can be regarded as an asset within the organization and are managed as such
- Specify how the IT asset lifecycle applies to people assets, particularly in terms of measurable competencies, such as skill, knowledge, understanding, qualifications, experience, attitude and behaviour

- Ensure the documentation of the competencies currently in place and specify how these can be re-used or enhanced
- Ensure organization standards are compatible with existing standard competency frameworks for the IT sector, such as SFIA+ (Skills For The Information Age) skills and competences are incorporated into roles and responsibilities.

In addition, in order to establish effective interfaces and dependencies:

- Define the interfaces that IT asset acquisition and management has with IT-enabled Business Change, IT Project Management and IT Security
- Formalize the interfaces that IT asset acquisition and management have with functions and processes outside IT
- Finally formalize measurement and reporting in this area by:
 - Identifying suitable metrics and the reports on IT assets for distribution throughout the organization as appropriate
 - Formalizing quality control and measurement in the acquisition and management of IT assets.

7.2 SERVICE MANAGEMENT TOOLS

Tools will enable the Service Design processes to work more effectively. Tools will increase efficiency and effectiveness, and provide a wealth of management information, leading to the identification of weak areas. The longer-term benefits to be gained from the use of tools are cost savings and increased productivity, which in turn can lead to an increase in the quality of the IT service provision.

The use of tools will enable the centralization of key processes and the automation and integration of core Service Management processes. The raw data collected by the tools can be analysed, resulting in the identification of 'trends'. Preventative measures can then be implemented, again improving the quality of the IT service provision.

Some points that organizations should consider when evaluating Service Management tools include:

- Data structure, data handling and integration
- Integration of multi-vendor infrastructure components, and the need to absorb new components in the future – these will place particular demands on the data-handling and modelling capabilities of the tool
- Conformity to international open standards
- Flexibility in implementation, usage and data sharing

- Usability – the ease of use permitted by the user interface
- Support for monitoring service levels
- Distributed clients with a centralized shared database (e.g. client server)
- Conversion requirements for previously tracked data
- Data backup, control and security
- Support options provided by the tool vendor
- Scalability at increasing of capacity (the number of users, volume of data and so on).

Consideration must be given to the exact requirements for the tool. What are the mandatory requirements and what are the desired requirements? Generally the tool should support the processes, not the other way round, so minimize modification of the processes to fit the tool. Where possible, it is better to purchase a fully integrated tool (although not at the expense of efficiency and effectiveness) to underpin many (if not all) Service Management processes. If this is not possible, consideration must be given to the interfaces between the various tools.

It is essential to have a Statement of Requirements (SoR) for use during the selection process – this statement can be used as a 'tick list'. The tool requirements should be categorized using the MoSCoW analysis:

- M – MUST have this
- S – SHOULD have this if at all possible
- C – COULD have this if it does not affect anything else
- W – WON'T have this time but WOULD like in the future.

The tool must be adequately flexible to support your required access rights. You must be able to determine who is permitted to access what data and for what purpose, e.g. read access to customers.

In the early stages, consideration must also be given to the platform on which the tool will be expected to operate – this may be on existing hardware and software or a new purchase. There may be restrictions laid down by IT strategy – for example, all new products may have to reside on specific servers. This might restrict which products could be included in the evaluation process. Make sure that the procurement fits within existing approved budgets.

There are many Service Management tools available. Details can be found on the internet, Service Management publications, from asking other organizations, from asking consultants or attending seminars and conferences to see what products are available.

During the early stages of the selection process, think about vendor and tool credibility. Are they still going to be supporting the purchase in a few months' or a year's time? Consider the past record of the supplier as well as that of the tool. Telephone the supplier's Service Desk to see how easy it is to get through, and ask some test questions to assess their technical competence. Ask the vendor to arrange a visit to a reference site to see what the experience is with the tool in practice – if possible without the vendor or supplier present. Make sure that the organization has similar requirements of the tool. See the tool in operation and speak to the users about their experiences, both initially and ongoing.

Assess the training needs of the organization and evaluate the capability of the supplier to provide the appropriate training. Also the ongoing training and tool update (upgrades and changes in user requirements) will need to be assessed to ascertain the support and training costs. In particular, consider training costs, training location, time required, how soon after training the tool will be in use, and during the implementation project ensure that sufficient training is provided – think about how the new tool will impact both IT and customer. Also ensure that interfaces with other tools and telephony are functioning correctly. It is wise to identify whether the planned combination has been used (or tried) elsewhere and with what results. Consider periods of parallel running alongside existing solutions before finally going live.

When evaluating tools, a 100% fit to requirements should not be expected and will almost certainly not be found. The '80/20 rule' should be brought into effect instead. A tool is deemed to be fit for its purpose if it meets 80% or more of the business's operational requirements. Those operational requirements should be categorized as discussed earlier.

Any product should be rejected as unsuitable if not all of the mandatory requirements ('must haves') are met. In some circumstances, it will be impossible to find an existing software product that will either meet all of the mandatory requirements or provide an 80% match. In this situation, the product offering the best functional design should be selected and the unsuitable elements re-written. This enhancement process should be done by the vendor if at all possible. In some cases, part of the enhancement costs may be met by the purchaser. Some products have been designed to include user hooks – this provides accessibility to site-written code at key procedural points, without the need for the package to be modified.

It doesn't end when the product has been selected. In many ways this could be considered as only the

beginning. The tool now has to be implemented. Once the hardware platform has been prepared and the software loaded, data population needs to be considered. What, where from, how and when? Timing is important to the testing, implementation and the go-live processes. Resources must be available to ensure success. In other words, don't schedule implementation during a known busy period, such as year-end processing. Today 'software as a service' products are available where hardware and software are not required. These products give network-based access to and management of commercially available software. These types of products will still require planning and implementation, but this should simplify the process as no dedicated hardware is required.

Consideration should also be given to managed service providers and Application Service Providers who may be able to provide the same functionality.

Whatever tool or type of tool is chosen, the fulfilment of the requirements can be differentiated between:

- **Out-of-the box** – the requirement is fulfilled
- **Configuration** – the tool can be configured with x days of effort to fulfil the requirement and this will be preserved over product upgrades
- **Customization** – the tool must be reprogrammed with x days of effort to fulfil the requirement, and this may have to be repeated on every product upgrade.

Extensive customization of any product is always best avoided because of the high costs incurred at product upgrade. Vendors may be unwilling to support old releases, and purchasers may be unable to resource the necessary re-application of any bespoke customization. Customization may also release the vendor from much of their support obligations – this would be disastrous if, as a result, your Service Management system is unavailable for any length of time. Further costs would be incurred in providing the bespoke training that would be required. It would be impossible to take advantage of any cheap scheduled training courses being run by the software supplier.

The process of tool evaluation is shown in Figure 7.1.

Figure 7.1 shows the standard approach of identifying requirements before identifying products, but pragmatically there may be some element of overlap, where exploration of tools on the market opens one's eyes to new options that change the requirements. These stages are targeted primarily at the evaluation of packaged software products, but a similar approach could also be used when evaluating custom-built software. Produce a clear Statement of Requirements (SoR) that identifies the

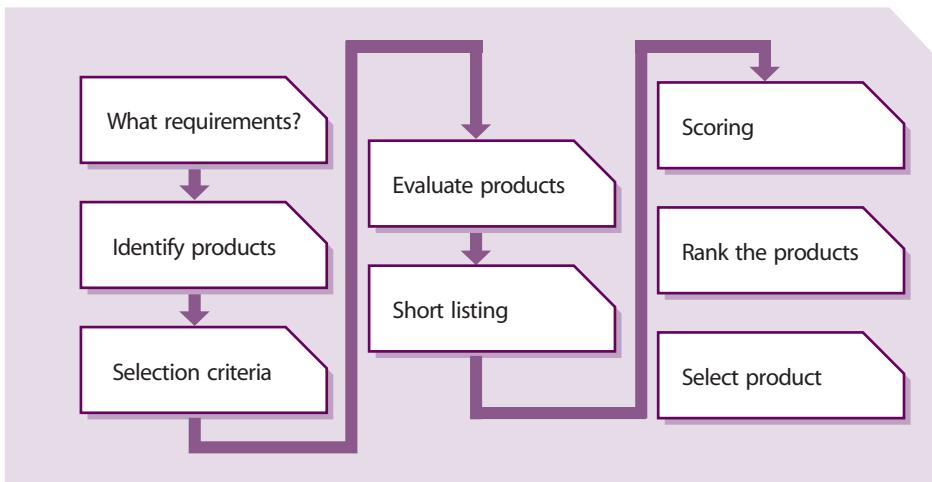


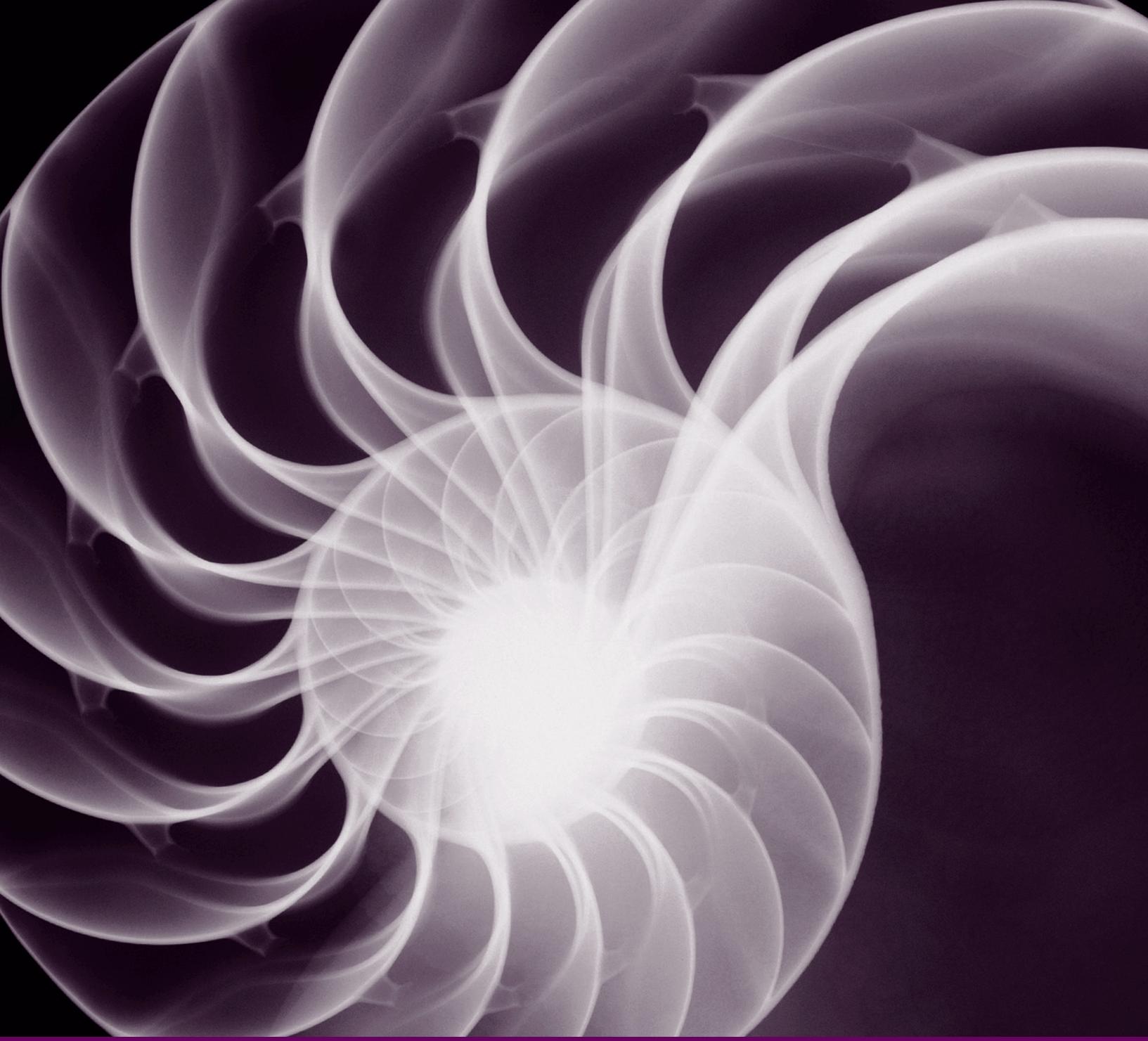
Figure 7.1 Service Management tool evaluation process

business requirements together with the mandatory facilities and those features that it would be 'nice to have'. Also identify the site policies and standards to which the product must conform. Such standards may include it running under particular system software, or on specific hardware.

Remember the considerations about the supplier's suitability, and carry out a formal evaluation of the products under consideration.

If well-developed and appropriate tools are used to support the processes, the results achieved will be far greater and often the overall costs of service provision will be less. Selecting the right tool means paying attention to a number of issues:

- An 80% fit to all functional and technical requirements
- A meeting of ALL mandatory requirements
- Little (if any) product customization required
- Adherence of tool and supplier to Service Management best practice
- A sound data structure and handling
- Integration with other Service Management and Operational Management tools
- Support of open standards and interfaces
- Business-driven not technology-driven
- Administration and maintenance costs within budget
- Acceptable levels of maintenance and release policies
- Security and integrity
- Availability of training and consultancy services
- Good report generation
- Scalability and growth.



8

Implementing Service Design

8 Implementing Service Design

This section of the publication considers the task of implementing the Service Design processes and tackles issues such as:

- Where do we start?
- How do we improve?
- How do we know we are making progress?

The activities of implementing and improving Service Design need to be focused on the needs and desires of the customer and the business. Therefore these activities should be driven and prioritized by:

- Business needs and business impacts
- Risks to the services and processes.

The activities will be influenced significantly by the requirements outlined in the SLRs and by the agreements made in the SLAs.

8.1 BUSINESS IMPACT ANALYSIS

A valuable source of input when trying to ascertain the business needs, impacts and risks is the Business Impact Analysis (BIA). The BIA is an essential element of the overall business continuity process (see section 4.7) and will dictate the strategy for risk reduction and disaster recovery. Its normal purpose is to identify the effect a disaster would have on the business. It will show which parts of the organization will be most affected by a major incident and what effect it will have on the company as a whole. It therefore enables the recognition of the most critical business functions to the company's survival and where this criticality differs depending on the time of the day, week, month or year. Additionally experience has shown that the results from the BIA can be an extremely useful input for a number of other areas as well, and will give a far greater understanding of the service than would otherwise be the case.

The BIA could be divided into two areas:

- One by business management, which has to investigate the impact of the loss (or partial loss) of a business process or a business function. This includes the knowledge of manual workarounds and their costs.
- A second role located in Service Management is essential to break down the effects of service loss to the business. This element of the BIA shows the

impact of service disruption to the business. The services can be managed and influenced by Service Management. Other aspects also covered in 'Business BIA' cannot be influenced by Service Management.

As part of the design phase of a new or changed service, a BIA should be conducted to help define the business continuity strategy and to enable a greater understanding about the function and importance of the service. This will enable the organization to define:

- Which are the critical services, what constitutes a major incident on these services, and the subsequent impact and disruption caused to the business – important in deciding when and how to implement changes
- Acceptable levels and times of service outage levels – again important in the consideration of change and implementation schedules
- Critical business and service periods – important periods to avoid
- The cost of loss of service – important for Financial Management
- The potential security implications of a loss of service – important considerations in the management of risk.

8.2 SERVICE LEVEL REQUIREMENTS

As part of the Service Level Management process (see Chapter 4), the Service Level Requirements for all services will be ascertained and the ability to deliver against these requirements will be assessed and finally agreed in a formal SLA. For new services, the requirements must be ascertained at the start of the development process, not after completion. Building the service with Service Level Requirements uppermost in mind is essential from a Service Design perspective.

8.3 RISKS TO THE SERVICES AND PROCESSES

When implementing the Service Design and ITSM processes, business-as-usual practices must not be adversely affected. This aspect must be considered during the production and selection of the preferred solution to ensure that disruption to operational services is minimized.

This assessment of risk should then be considered in detail in the Service Transition activities as part of the implementation process.

8.4 IMPLEMENTING SERVICE DESIGN

The process, policy and architecture for the design of IT services outlined in this publication will need to be documented and utilized to ensure the appropriate innovative IT services can be designed and implemented to meet current and future agreed business requirements.

The **IT Service Management** processes outlined in Chapter 4 of this publication and in the other publications in this series will also need to be implemented to ensure service delivery that matches the requirements of the business.

The question often asked is ‘Which process shall I implement first?’ The real answer is all of them, as the true value of implementing all of the Service Management processes is far greater than the sum of the individual processes. All the processes are interrelated, and in some cases are totally dependent on others. What is ultimately required is a single, integrated set of processes, providing management and control of a set of IT services throughout their entire lifecycle.

While recognising that, to get the complete benefit of implementing IT service Management, all of the processes need to be addressed, it is also recognized that it is unlikely that organizations can do everything at once. It is therefore recommended that the areas of greatest need be addressed first. A detailed assessment needs to be undertaken to ascertain the strengths and weaknesses of IT service provision. This should be undertaken by performing customer satisfaction surveys, talking to customers, talking to IT staff and analysing the processes in action. From this assessment, short-, medium- and long-term strategies can be developed.

It may be that ‘quick wins’ need to be implemented in the short term to improve the current situation, but these improved processes may have to be discarded or amended as part of the medium- or long-term strategies. If ‘quick wins’ are implemented, it is important that they are not done at the expense of the long-term objectives, so these must be considered at all times. However, every organization will have to start somewhere, and the starting point will be wherever the organization is now in terms of IT Service Management maturity.

Implementation priorities should be set against the goals of a SIP. For example, if availability of IT services is a critical issue, focus on those processes aimed at maximizing availability (e.g. Incident Management,

Problem Management, Change Management and Availability Management). Throughout the implementation process, key players must be involved in the decision-making process. These will include receivers as well as providers of the service. There can be a tendency, when analysing the areas of greatest need, to go straight for tools to improve the situation. Workshops or focus groups will be beneficial in understanding the requirements and the most suitable process for implementation that will include people, processes, products and partners.

The first thing to do is to establish a formal process and method of implementation and improvement of Service Design, with the appropriate governance in place. This formal process should be based around the six-stage process illustrated in Figure 8.1. More information can also be found on this process in the Continual Service Improvement publication.

It is important that when implementing or improving processes a structured Project Management method is used. The improvement process can be summarized as, first, understanding the vision by ascertaining the high-level business objectives. The ‘vision-setting’ should set and align business and IT strategies. Second, assessing the current situation to identify strengths that can be built on and weaknesses that need to be addressed. So ‘Where are we now?’ is an analysis of the current position in terms of the business, organization, people and process. Third, ‘Where do we want to be?’ is a development of the principles defined in the vision-setting, agreeing the priorities for improvement, and fourth, detailing the SIP to achieve higher-quality service provision. Next, measurements and metrics need to be put in place to show that the milestones have been achieved and that the business objectives and business priorities have been met. Finally the process should ensure that the momentum for quality improvement is maintained.

The following are key elements for successful alignment of IT with business objectives:

- Vision and leadership in setting and maintaining strategic direction, clear goals, and measurement of goal realization in terms of strategic direction
- Acceptance of innovation and new ways of working
- Thorough understanding of the business, its stakeholders and its environment
- IT staff understanding the needs of the business
- The business understanding the potential of IT
- Information and communication available and accessible to everyone who needs it

- Separately allocated time to familiarize with the material
- Continuous tracking of technologies to identify opportunities for the business.

The implementation/improvement cycle is useful in checking the alignment between the business and IT, as shown in Figure 8.1.

8.4.1 What is the vision?

The starting point for all of these activities is the culture and environment of the service provider organization. The people and the culture have to be appropriate and acceptable to improvement and change. Therefore, before attempting anything else, the culture within the service provider needs to be reviewed to ensure that it will accept and facilitate the implementation of the required changes and improvements. The following key steps need to be completed to achieve this stage of the cycle:

- Establish a vision, aligned with the business vision and objectives
- Establish the scope of the project/programme
- Establish a set of high-level objectives
- Establish governance, sponsorship and budget
- Obtain senior management commitment
- Establish a culture focused on:
 - Quality
 - Customer and business focus
 - A learning environment
 - Continual improvement
 - Commitment to the 'improvement cycle'
 - Ownership and accountability.

8.4.2 Where are we now?

Once the vision and high-level objectives have been defined, the service provider then needs to review the current situation, in terms of what processes are in place and the maturity of the organization. The steps and activities that need to be completed here are:

- A review, assessment or a more formal audit of the current situation, using a preferred technique:
 - An internal review or audit
 - Maturity assessment
 - An external assessment or benchmark
 - An ISO/IEC 20000 audit
 - An audit against COBIT
 - A Strengths, Weaknesses, Opportunities and Threats (SWOT) analysis
 - A risk assessment and management methodology
- The review should include:
 - The culture and maturity of the service provider organization
 - The processes in place and their capability and maturity
 - The skills and competence of the people
 - The services and technology
 - The suppliers, contracts and their capability
 - The quality of service and the current measurements, metrics and KPIs
 - A report summarizing the findings and recommendations.

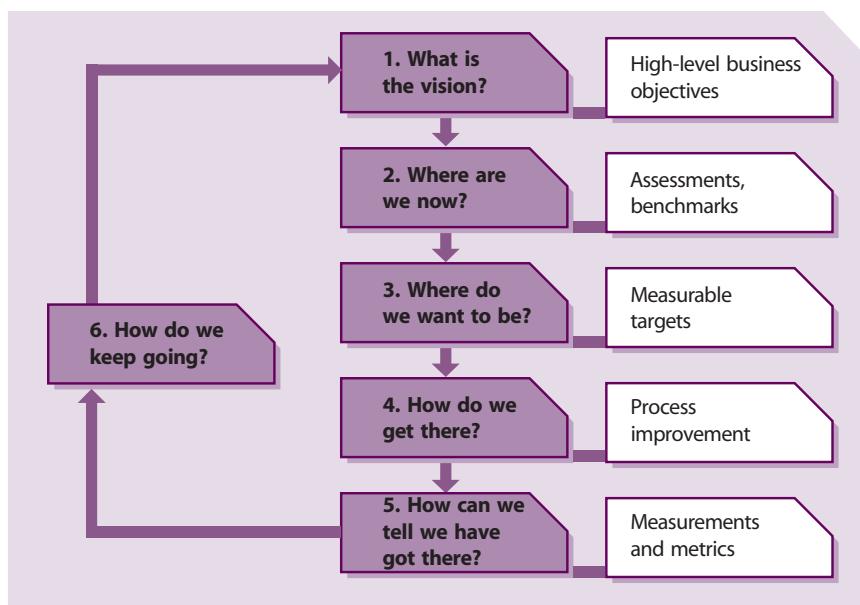


Figure 8.1 Implementation/improvement cycle

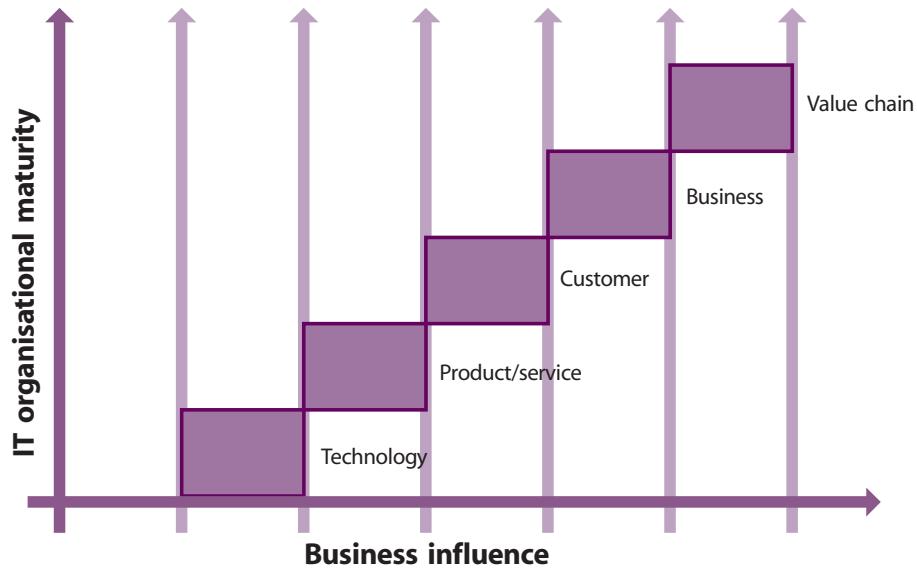


Figure 8.2 Cultural maturity assessment

The review of the culture should include assessing it in terms of the capability and maturity of the culture within the IT service provider organization, as shown in Figure 8.2.

This assessment should be based on the fact that each growth stage represents a transformation of IT organization and as such will require:

- Changes in people (skills and competences)
- Processes and ways of working
- Technology and tools (to support and enable the people and processes)
- Steering (the visions, goals and results)
- Attitude (the values and beliefs)
- The appropriate level and degree of interaction with the business, stakeholders, customers and users.

The assessment should also include a review of the capability and maturity of the Service Design processes, as shown in Figure 8.3.

This review and should include all aspects of the processes and their use including the:

- Vision: steering, objectives and plans
- Process maturity, functionality, usage, application, effectiveness and efficiency together with ownership, management and documentation
- People: the roles, responsibilities, skills and knowledge of the people
- Products, including the tools and technology used to automate the processes
- Culture: the focus, attitudes and beliefs.

The above framework can be used to provide consistency of process assessment. Assessing these two aspects will determine the current state of the organization and its Service Management capability and maturity. When starting out on the implementation or improvement of Service Design, or any set of processes, it is important to

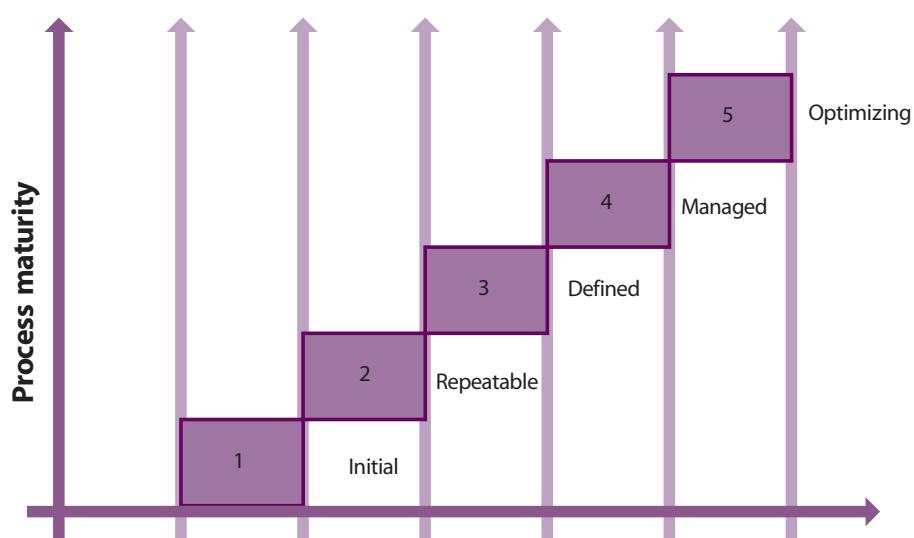


Figure 8.3 Process maturity framework

build on the strengths of the existing cultures and processes and rapidly identify and improve the weaknesses. A more detailed explanation of this framework is contained in Appendix H.

8.4.3 Where do we want to be?

Based on the current state assessment, and the vision and high-level objectives, a future desired state can be defined. This should be expressed in terms of planned outcomes, including some or all of:

- Improved IT service provision alignment with total business requirements
- Improved quality of Service Design
- Improvements in service levels and quality
- Increases in customer satisfaction
- Improvements in process performance.

8.4.4 How do we get there?

A set of improvements should then be identified to move forward from the current state to the agreed future state. A plan to implement these improvements should then be developed, incorporating Service Transition and Service Operation, and should include:

- The improvement actions
- The approach to be taken and the methods to be used
- Activities and timescales
- Risk assessment and management
- Resources and budgets
- Roles and responsibilities
- Monitoring, measurement and review.

8.4.5 How can we tell when we have got there?

Often organizations instigate improvement initiatives without considering or designing the measurement system from the outset. The success of the initiative cannot, therefore, be ascertained because we have no benchmark before, during or after the implementation. It is imperative that the measurements are designed before the implementation. A defined set of metrics needs to be utilized in order to ensure that the desired future state is achieved. This desired future state needs to be expressed in measurable terms such as:

- X% reduction in Service Design non-conformances
- X% increase in customer satisfaction
- X% increase in the service availability of critical services.

Thus once the improvement actions and plans have been completed, checks and reviews should be completed in order to determine:

- Did we achieve our desired new state and objectives?
- Are there any lessons learnt and could we do it better next time?
- Did we identify any other improvement actions?

8.4.6 How do we keep going?

Having improved, we now need to consolidate and move on. The organization and the culture must recognize that we can always get better, and therefore must establish an environment of continual improvement. So, once we have achieved the new desired state, we must review the vision and objectives, identify more improvement actions and repeat the six-stage process again. So this stage is all about:

- Developing a learning environment
- Establishing a desire to improve throughout the organization
- Recognizing and reinforcing the message that quality and improvement are everybody's job
- Maintaining the momentum on improvement and quality.

8.5 MEASUREMENT OF SERVICE DESIGN

The success of the Service Design and the success of the improvement to the processes around the Service Design must be measured, the data must be analysed and reported on. Where the design or process does not meet the requirements of the business as a whole, changes to the process may be required and the results of those changes must also be measured. Continuous measurement, analysis and reporting are mandatory requirements for both the Service Design process and the ITSM processes.

There are measurement methods available that enable the analysis of service improvement. The Balanced Scorecard is a method developed by Robert Kaplan and David Norton as a concept for measuring a company's activities in terms of its vision and strategies. It gives a comprehensive view of the performance of a business. The system forces managers to focus on the important performance metrics that drive success. It balances a financial perspective with customer, internal process and learning and growth perspectives. More information can be found on the Balanced Scorecard method in the Continual Service Improvement publication.

Six Sigma is a methodology developed by Bill Smith at Motorola Inc. in 1986, and was originally designed to manage process variations that cause defects, defined as unacceptable deviation from the mean or target, and to systematically work towards managing variation to eliminate those defects. Six Sigma has now grown beyond defect control and is often used to measure improvement in IT process execution. (Six Sigma is a registered service mark and trademark of Motorola Inc.)

Six Sigma (DMADV) is an improvement system used to develop new processes at Six Sigma quality levels and is defined as:

- **Define** – formally define the goals of the design activity that are consistent with customer demands and organization strategy
- **Measure** – identify Critical Success Factors, capabilities, process capability and risk assessment
- **Analyse** – develop and design alternatives, create high-level design and evaluate design capability to select the best design
- **Design** – develop detailed design, optimize design and plan for design verification
- **Verify** – set up pilot runs, implement production process and hand over to process owners.

The Six Sigma (DMAIC) process (define, measure, analyse, improve, control) is an improvement system for existing processes falling below specification and looking for incremental improvement.

8.5.1 Prerequisites for success

There are a number of prerequisites required for the Service Design and the successful introduction of new or revised processes. Often these prerequisites for success (PFSs) are elements of one process required by another. For example, fully completed and up-to-date Business Service Catalogue and Technical Service Catalogue are required before Service Level Management can design the SLA and supporting agreement structure, and before SLM can set up and agree the SLAs. Problem Management will depend on a mature Incident Management process. The PFSs can be much wider than just ITSM process interdependencies. For example, the design of availability and capacity for a new service cannot be achieved without details of the business plan for the utilization of the new service. The design of the service will be impossible without the Service Portfolio and Service Transition Pack. There are many more examples of these PFSs that need to be considered and planned before high process maturity levels can be achieved. Low maturity in one process will

mean that high levels of maturity will not be achievable in other processes.

8.5.2 Critical Success Factors and Key Performance Indicators

Critical Success Factor (CSF) is a term for an element that is necessary for an organization or project to achieve its mission. CSFs can be used as a means for identifying the important elements of success.

CSFs are the things that have to be got right in the Service Design and within each ITSM process. Key Performance Indicators (KPIs) are measures that quantify objectives and enable the measurement of performance. KPIs should be set and measured against the design and for each of the processes to ensure the CSFs are met. Together, CSFs and KPIs establish the baseline and mechanisms for tracking performance.

It is recommended that each IT organization focuses on a small sub-set of CSFs and KPIs at any one time. The required CSFs and KPIs should be set at the beginning of the Continual Service Improvement Plan (CSIP).

It is important that CSFs are agreed during the design phase of a service and of the processes, and that Key Performance Indicators (KPIs) are set, measured and reported on to indicate the quality of the Service Design and the Service Design processes. There is a requirement to be able to analyse how well the service infrastructure was designed. It is possible to arrive at a good design in a very resource-inefficient manner, and vice versa, so we need to look at the quality as well as resources required to achieve the required quality. KPIs around the success of delivery of the service indicate the effectiveness of the Service Design are applicable – for example, does the service meet the (defined) business requirements for availability, reliability, throughput, security, maintainability, serviceability, functionality etc.? KPIs around the resource estimates, however, will show us how efficient we were in the design.

These should be defined as part of QA planning and release acceptance. These KPIs could be supported by similar component metrics.

KPIs for the process of Service Design include:

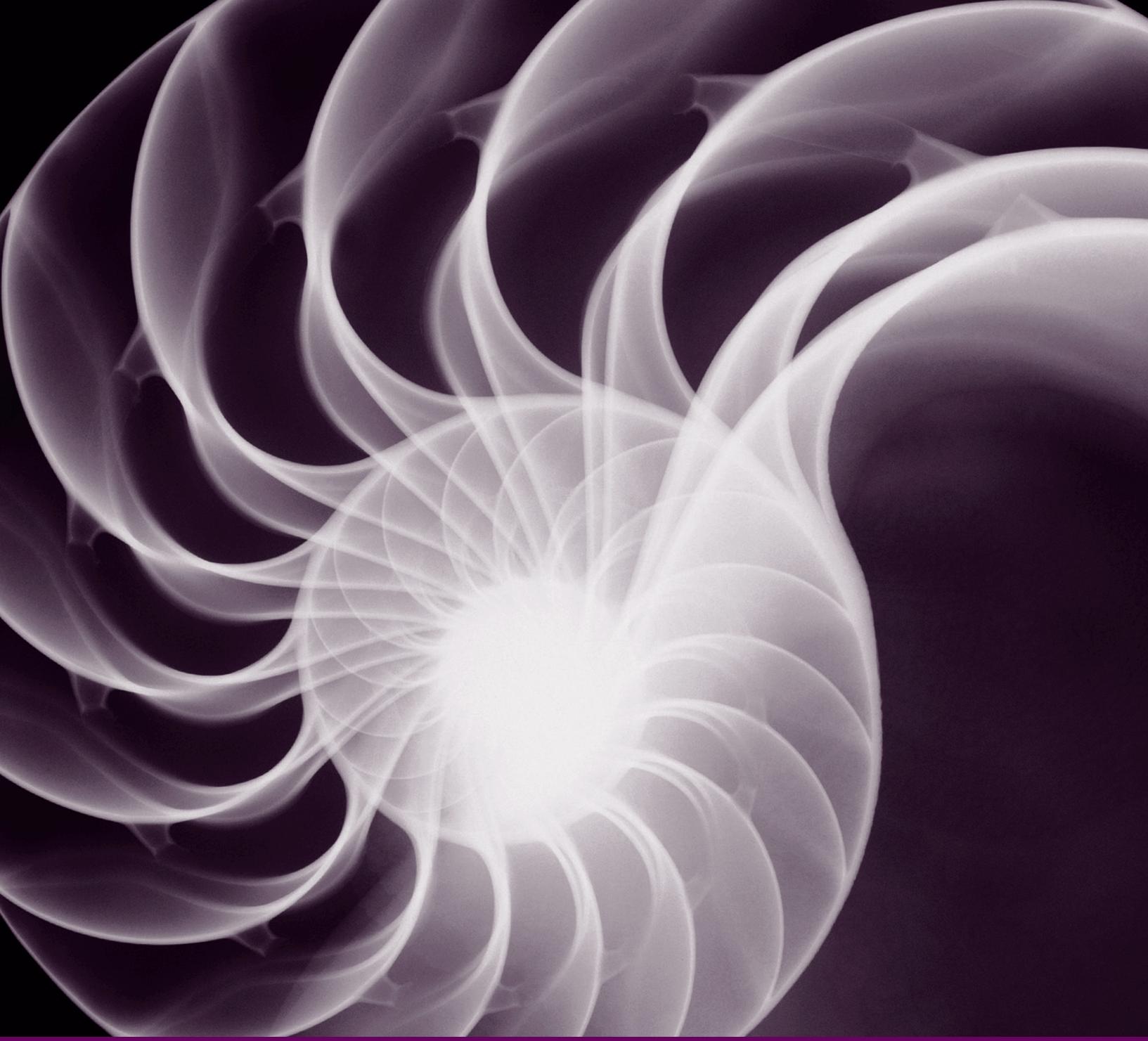
- Percentage of Service Design requirement specifications produced on time (and to budget)
- Percentage of Service Design plans produced on time
- Percentage of Service Transition packs completed on time
- Percentage of QA and acceptance criteria plans produced on time

- Accuracy of Service Design – for example, was the correct infrastructure built to support the service?
- Percentage accuracy of the cost estimate of the whole Service Design phase
- Accuracy of SLA(s), OLA(s) and contract(s) – do they really support the required level of service?

To judge service provision and ITSM process performance, clearly defined objectives with measurable targets should be set. Confirmation needs to be sought that these objectives and the milestones set in the Continual Service Improvement (CSI) stage of the lifecycle have been reached and that the desired service quality or desired improvement in quality has been achieved. It is vital when designing services or processes that KPIs are designed from the outset and collected regularly and at important milestones. For example, when designing at the completion of each significant stage of the programme, a Post Implementation Review (PIR) should be conducted to ensure the objectives have been met. The PIR will include a review of supporting documentation and the general awareness amongst staff of the refined processes.

A comparison is required of what has been achieved against the original goals set in the project. Once this has been confirmed, new improvement targets should be defined. To confirm that the milestones have been reached, KPIs need to be constantly monitored. These KPIs include customer satisfaction targets, so there will be a need to survey customers planned at various stages to confirm that changes made are improving the customer perception of the service quality. It is possible that the services have higher availability, that there are fewer incidents and that response times have improved, but at the same time the customer's perception of service quality has not improved. Clearly this is as important, and will need to be addressed by talking to customers to ascertain their concerns. Confirmation will need to be sought that CSIs put in place are addressing the customer's primary needs.

For further information on service improvement practices, please refer to the Continual Service Improvement publication.



Challenges, Critical Success Factors and risks

9

9 Challenges, Critical Success Factors and risks

9.1 CHALLENGES

With every undertaking there will be challenges or difficulties to face and to overcome. This will be especially true when attempting to design new services and processes that meet the requirements of all stakeholders within the business. Experience has shown that the following will help to overcome the challenges:

- Understanding the business requirements and the business priorities and ensuring that these are uppermost in mind when designing the processes and the services.
- Communications will be vitally important both in explaining what is happening and how individuals will be affected and in listening to the requirements and needs of the individuals. It's vitally important to communicate with people about concerns that relate to their daily job.
- Involve as many people as possible in the design. Setting up focus groups or steering groups can be very effective in getting the right solution as well as gaining wider support.
- Gaining commitment from senior management as well as from all levels of staff.

Examples of challenges that may be faced include:

- The need to ensure alignment with current architectural directions, strategy and policies. An example of this may be that the procured infrastructure may have poor monitoring and control features.
- The use of diverse and disparate technologies and applications.
- Documentation and adherence to agreed practices and processes.
- Unclear or changing requirements from the business. This may be unavoidable in some cases because business needs are likely to change. The important thing is to ensure that there is a very close relationship between the IT service provider organization and the business customer of the service, so that any changing requirements can be identified as quickly as possible.
- A lack of awareness and knowledge of service and business targets and requirements.
- Linked to the above point, it may be that certain

facilities are not built into the design. Again, it is imperative that representatives of every user of the designed service or process are involved throughout the process to reduce the chance of this happening. Details of service testing (an important element here) are contained within the Service Transition publication.

- A resistance to planning, or a lack of planning leading to unplanned initiatives and unplanned purchases.
- Inefficient use of resources causing wasted spend and investment.
- As mentioned previously, a good knowledge and appreciation of the business impacts and priorities is imperative.
- Poor relationships, communication or lack of cooperation between the IT service provider and the business may result in the design not achieving the business requirements.
- Resistance to work within the agreed strategy.
- Use of, and therefore the constraints of, old technology and legacy systems.
- Required tools are too costly or too complex to implement or maintain with the current staff skills.
- Lack of information, monitoring and measurements.
- Unreasonable targets and timescales previously agreed in the SLAs and OLAs.
- Over-commitment of available resources with an associated inability to deliver (e.g. projects always late or over budget).
- Poor Supplier Management and/or poor supplier performance.
- Lack of focus on service availability.
- Lack of awareness and adherence to the operational aspects of security policies and procedures.
- Ensuring normal daily operation or business as usual is considered as part of the design.
- Cost and budgetary constraints.
- Ascertaining the ROI and the realization of business benefit.

9.2 RISKS

There are a number of risks directly associated with the Service Design phase of the Service Lifecycle. These risks need to be identified to ensure that they are not realized. They include the following:

- If any of the PFSs for Service Design are not met, then the Service Design or Service Management process will not be successful.
- If maturity levels of one process are low, it will be impossible to achieve full maturity in other processes.
- Business requirements are not clear to IT staff.
- Business timescales are such that insufficient time is given for proper Service Design.
- Insufficient testing, resulting in poor design and therefore poor implementation.
- An incorrect balance is struck between innovation, risk and cost while seeking a competitive edge, where desired by the business.
- The fit between infrastructures, customers and partners is not sufficient to meet the overall business requirements.
- A coordinated interface is not provided between IT planners and business planners.
- The policies and strategies, especially the Service Management strategy, are not available from Service Strategy, or its content is not clearly understood.
- There are insufficient resources and budget available for Service Design activities.
- The risk of services developed in isolation using their 'own' assets and infrastructure. This can appear to be cheaper in isolation, but can be much more costly in the long term because of the financial savings of corporate buying and the extra cost of supporting different architecture.
- Insufficient time given to the design phase, or insufficient training given to the staff tasked with the design.
- Insufficient engagement or commitment with the application's functional development, leading to insufficient attention to Service Design requirements.



Afterword

Afterword

Service Design, as described in this publication, covers the design of appropriate and innovative IT services to meet current and future agreed business requirements. Service Design develops a Service Design Package and looks at selecting the appropriate Service Design model. In this publication we have also examined the various sourcing models available and given some benefits and disadvantages to each.

The publication also discusses the fundamentals of the design processes and the five aspects of the design:

- The design of the service solutions, including all of the functional requirements, resources and capabilities needed and agreed
- The design of Service Management systems and tools, especially the Service Portfolio for the management and control of services through their lifecycle
- The design of the technology architectures and management architectures and tools required to provide the services
- The design or specification of the processes needed to design, transition, operate and improve the services, the architectures and the processes themselves
- The design of the measurement systems, methods and metrics for the services, the architectures and their constituent components and the processes.

The definition of Service Design is:

'The design of appropriate and innovative IT services, including their architectures, processes, policies and documentation, to meet current and future agreed business requirements'.

The publication has explained that the better and more careful the design, the better the solution taken into live operation. It is also highly likely that the better the design, the less re-work time that will need to be undertaken during the transition and live phases.

The scope of this publication includes the design of services, as well as the design of Service Management systems and processes. Service Design is not limited to new services, but includes change necessary to increase or

maintain value to customers over the lifecycle of services.

This publication explains that pragmatism sometimes overrides the perfect solution where we know what it would be, but the amount of effort and cost does not justify the perfect solution. As always it will depend on the business needs and the business requirements. As always it is imperative that whatever is done within IT has a direct benefit to the overall business.



Appendix A: The Service Design Package

A

Appendix A: The Service Design Package

A 'Service Design Package' or 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 SDP should contain:

Table A.1 Contents of the Service Design Package

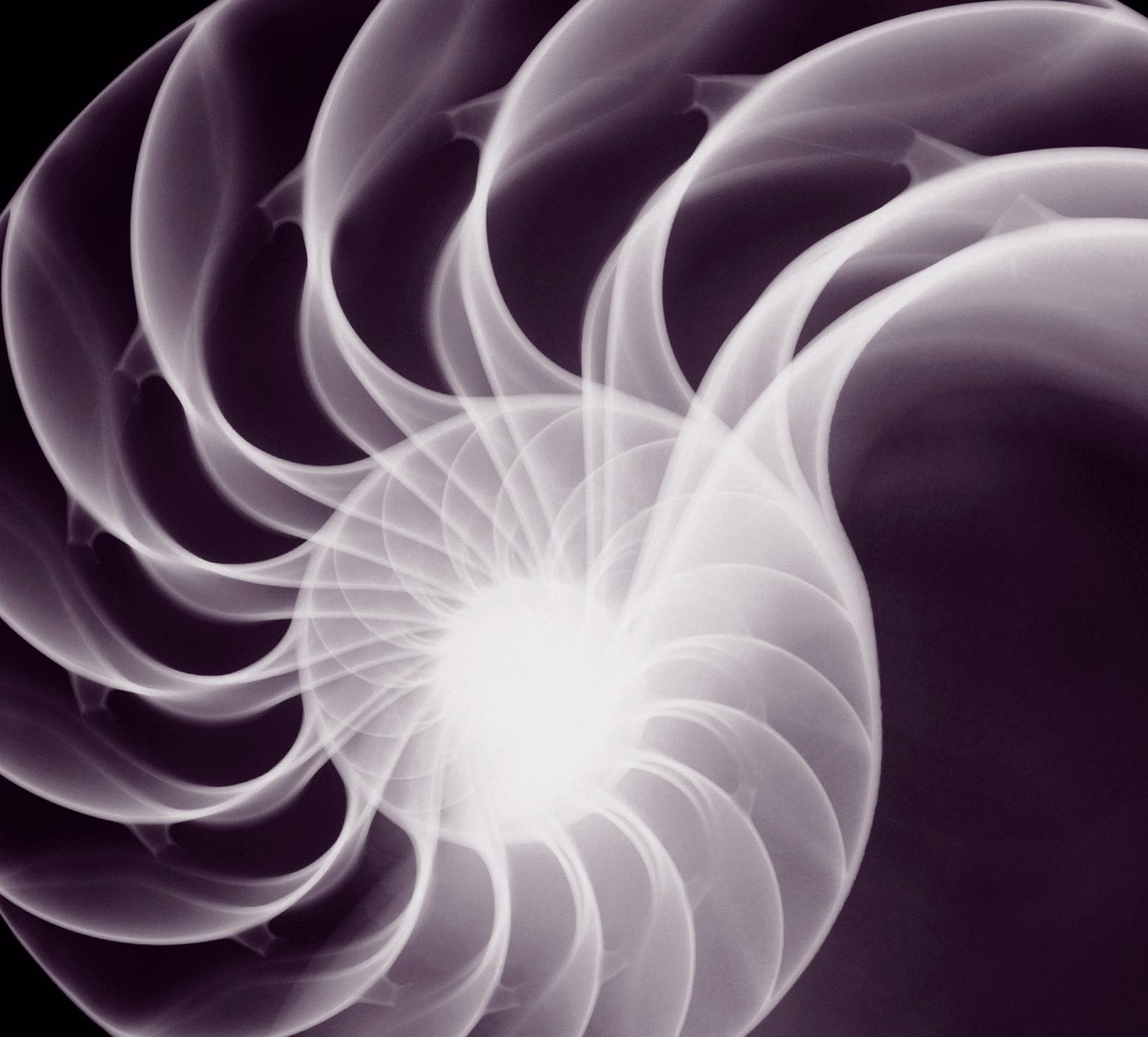
Category	Sub-category	Description of what is in the SDP
Requirements	Business requirements	The initial agreed and documented business requirements
	Service applicability	This defines how and where the service would be used. This could reference business, customer and user requirements for internal services
	Service contacts	The business contacts, customer contacts and stakeholders in the service
Service Design	Service functional requirements	The changed functionality of the new or changed service, including its planned outcomes and deliverables, in a formally agreed Statement of Requirements (SoR)
	Service Level Requirements	The SLR, revised or new 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: <ul style="list-style-type: none"> ■ The service definition and model, for transition and operation ■ All service components and infrastructure (including H/W, S/W, networks, environments, data, applications, technology, tools, documentation), including version numbers and relationships, preferably within the 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 A.1 Contents of the Service Design Package (continued)

Category	Sub-category	Description of what is in the SDP
Service Lifecycle Plan	Service Programme	<p>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:</p> <ul style="list-style-type: none"> ■ 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	<p>Overall transition strategy, objectives, policy, risk assessment and plans including:</p> <ul style="list-style-type: none"> ■ 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: <ul style="list-style-type: none"> ● 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

Table A.1 Contents of the Service Design Package (continued)

Category	Sub-category	Description of what is in the SDP
	Service Transition Plan	<ul style="list-style-type: none"> ■ Deployment policy, release policy, plans and requirements, including logistics, deployment, roll-out, staging, deployment environments, cultural change, organisational 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	<p>Overall operational strategy, objectives, policy, risk assessment and plans including:</p> <ul style="list-style-type: none"> ■ 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	<p>Development and use of Service Acceptance Criteria (SAC) for progression through each stage of the Service Lifecycle, including:</p> <ul style="list-style-type: none"> ■ All environments ■ Guarantee and pilot criteria and periods



Appendix B: Service Acceptance Criteria (example)

B

Appendix B: Service Acceptance Criteria (example)

The Service Acceptance Criteria (SAC) is a set of criteria used to ensure that the 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 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 SLA/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 CMS and appropriate relationships established for all supporting components?	Service Level, Configuration
Have all customers and 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
Have all new suppliers been identified and their associated contracts drawn up accordingly?	Contract and Supplier Management

Table B.1 Service Acceptance Criteria (continued)

Criteria	Responsibility
Have all support arrangements been reviewed and revised – SLAs, SLRs, 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 RFCS 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 S/W licences been purchased or reallocated licences used?	Configuration
Have any new H/W components been stored in the DL with details recorded in the CMS?	Configuration
Have all new S/W components been lodged in the DL 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 new service?	Project Manager



Appendix C: Process documentation templates (example)

C

Appendix C: Process documentation templates (example)

C1 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
- Roles and responsibilities:
 - Operational responsibilities
 - Process owner
 - Process members
 - Process users
 - Other roles
- Associated documentation and references
- Interfaces and dependencies to:
 - Other SM processes
 - Other IT processes
 - Business processes
- Process measurements and metrics: reviews, assessments and audits
- Deliverables and reports produced by the process:
 - Frequency
 - Content
 - Distribution
- Glossary, acronyms 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 technology 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.

D1 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
- SoR and 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 policies 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, policies and standards
- Handover, acceptance and sign-off standards and methods
- Partners, 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
- E-mail and groupware architectures, design standards and policies
- Environmental requirements, design policies and standards
- IT security design policies and standards, including fire walling, 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.

D2 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

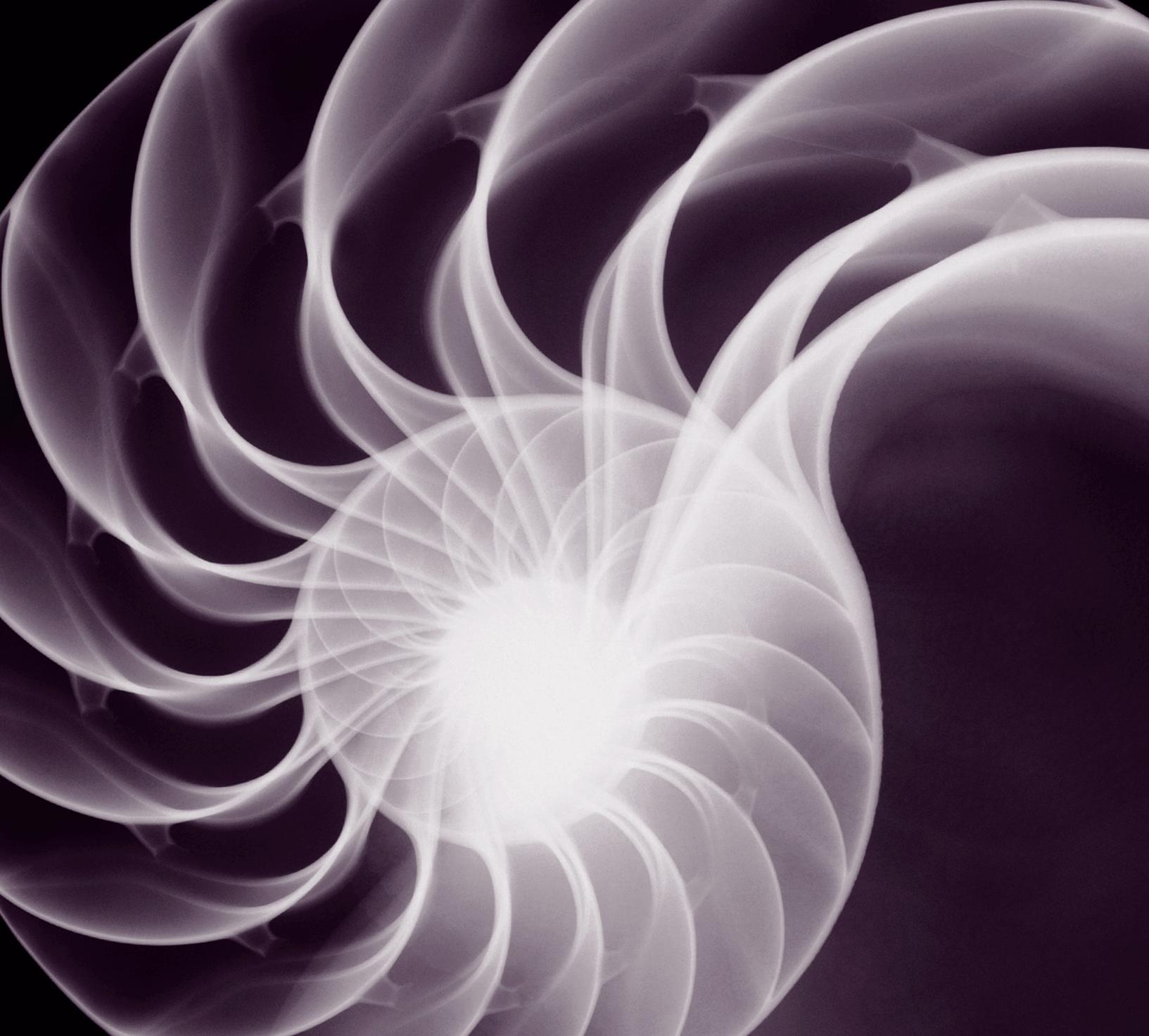
■ **Transition plans:**

- 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
- 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 with 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



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. The following tables cover the major aspects that need to be considered, with example characteristics.

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	Minimize external risks
Services	Where possible and justifiable, alternate 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
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
External	Generator for major data centres and business-critical systems

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° (\pm 3°). Provide for up to 550W/m ² . 6° variation throughout the room and a maximum of 6° per hour
Humidity control	Strict control: 50% (\pm 10%)
Air quality	Positive pressure, filtered intake low gaseous pollution (e.g. sulphur dioxide \leq 0.14 ppm), dust levels for particles > 1 micron, less than 5 x 10 ⁶ 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 \pm 5% of rating with minimal impulse, sags, surges and over/under voltage conditions
False floors	Antistatic, liftable floor tiles 600 x 600mm on pedestals, with alternate pedestals screwed to the solid floor. Minimum of 600mm clearance to solid floor. Floor loadings of up to 5kN/m ² with a recommended minimum of 3m 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. With 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 (1.5V/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° (\pm 5°), preferable
Humidity control	Strict control: 50% (\pm 10%), preferable
Air quality	Positive pressure, filtered intake low gaseous pollution (e.g. sulphur dioxide \leq 0.14 ppm), dust levels for particles > 1 micron, less than 5 x 10 ⁶ 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 \pm 5% of rating with minimal impulse, sags, surges and over/under voltage conditions
False floors	Antistatic, liftable floor tiles 600 x 600mm on pedestals, with alternate pedestals screwed to the solid floor. Minimum of 600mm clearance to solid floor. Floor loadings of up to 5kN/m ² with a recommended minimum of 3m 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. With 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 (1.5V/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 3m 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 (1.5V/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 SLA and OLA



Appendix F: Sample SLA and OLA

This appendix contains examples of SLAs and OLAs 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.

SERVICE LEVEL AGREEMENT (SLA – SAMPLE)

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 the (date) until (date). The agreement will be reviewed annually. Minor changes may be recorded on the form at the end of the agreement, providing 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 x 24 x 365, 08:00 to 18:00 – Monday to Friday).

Special conditions for exceptions (e.g. weekends, public holidays) and procedures for requesting service extensions (who 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.

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, underpinning 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 POS support service'. This strong link between the IT service and the customer's business processes is a sign of maturity in both the SLM 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 e.g. four per annum, or as a Mean Time Between Failures (MTBF) or Mean Time Between Systems Incidents (MTBSI)).

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

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.)

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 week-end extension)

Note. 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.

Note. 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.

Service performance:

Details of the expected responsiveness of the IT service (e.g. 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.

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.

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 RFCs, usually based on the category or urgency/priority of the change, should also be included and details of any known changes that will impact on the agreement, if any.

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).

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, content, 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.

OPERATIONAL LEVEL AGREEMENT (OLA – SAMPLE)

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 the (date) until (date).

The agreement will be reviewed annually. Minor changes may be recorded on the form at the end of the agreement, providing 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 support of 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 Management:

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

Configuration Management:

The responsibilities for the ownership, provision and maintenance of accurate 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.

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, SLRs 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.



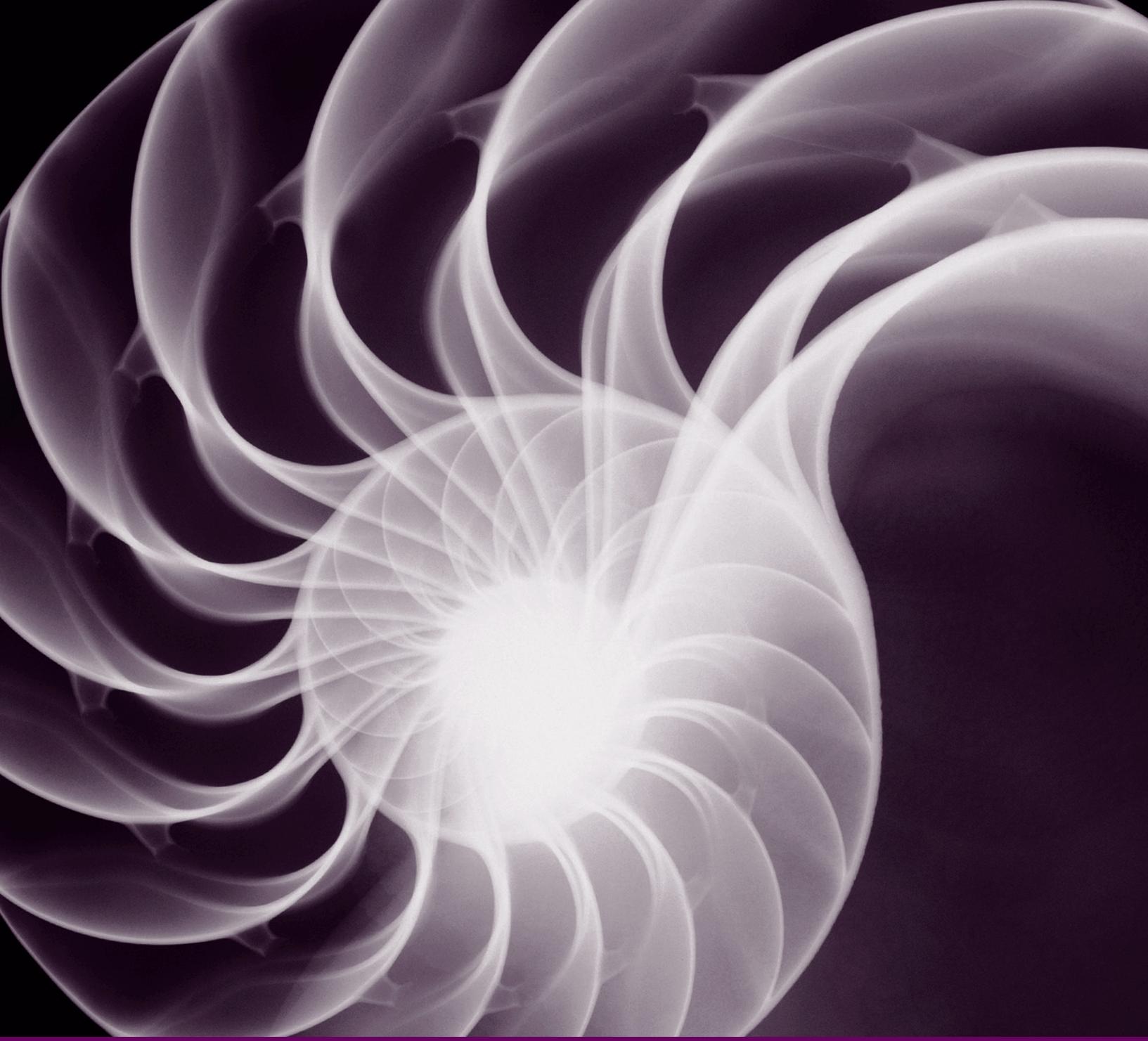
Appendix G: Example Service Catalogue

G

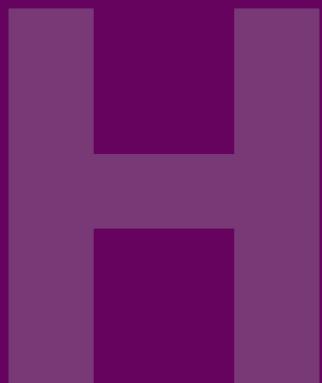
Appendix G: Example Service Catalogue

The Service Catalogue is key document containing valuable information on the complete set of services offered. It should preferably be stored as a set of 'service' CLs within a CMS, 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 Example Service Catalogue



Appendix H: The Service Management process maturity framework



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 H.1, can be used by organizations to internally review their own Service Management processes as well as 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.

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'.

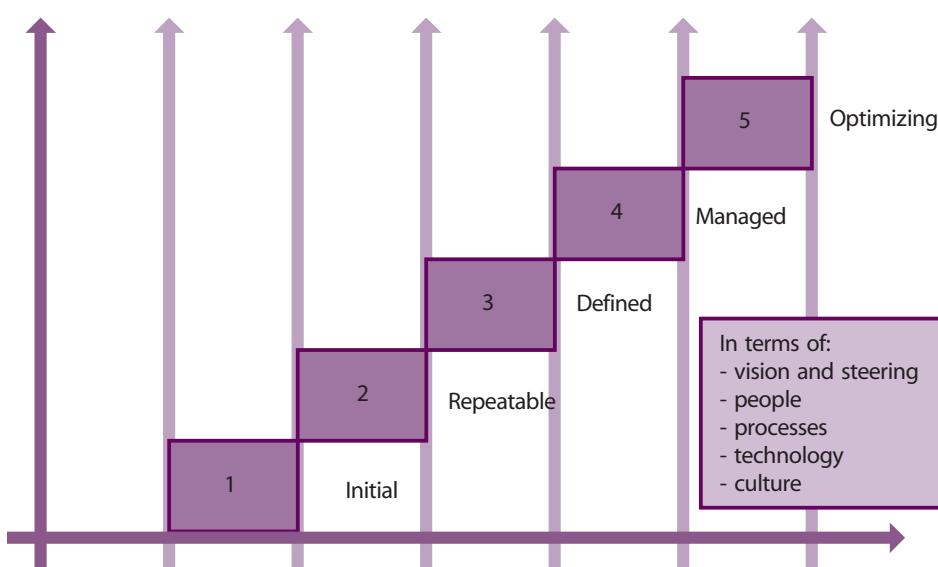


Figure H.1 Process maturity framework

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

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.

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

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.

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

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.

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

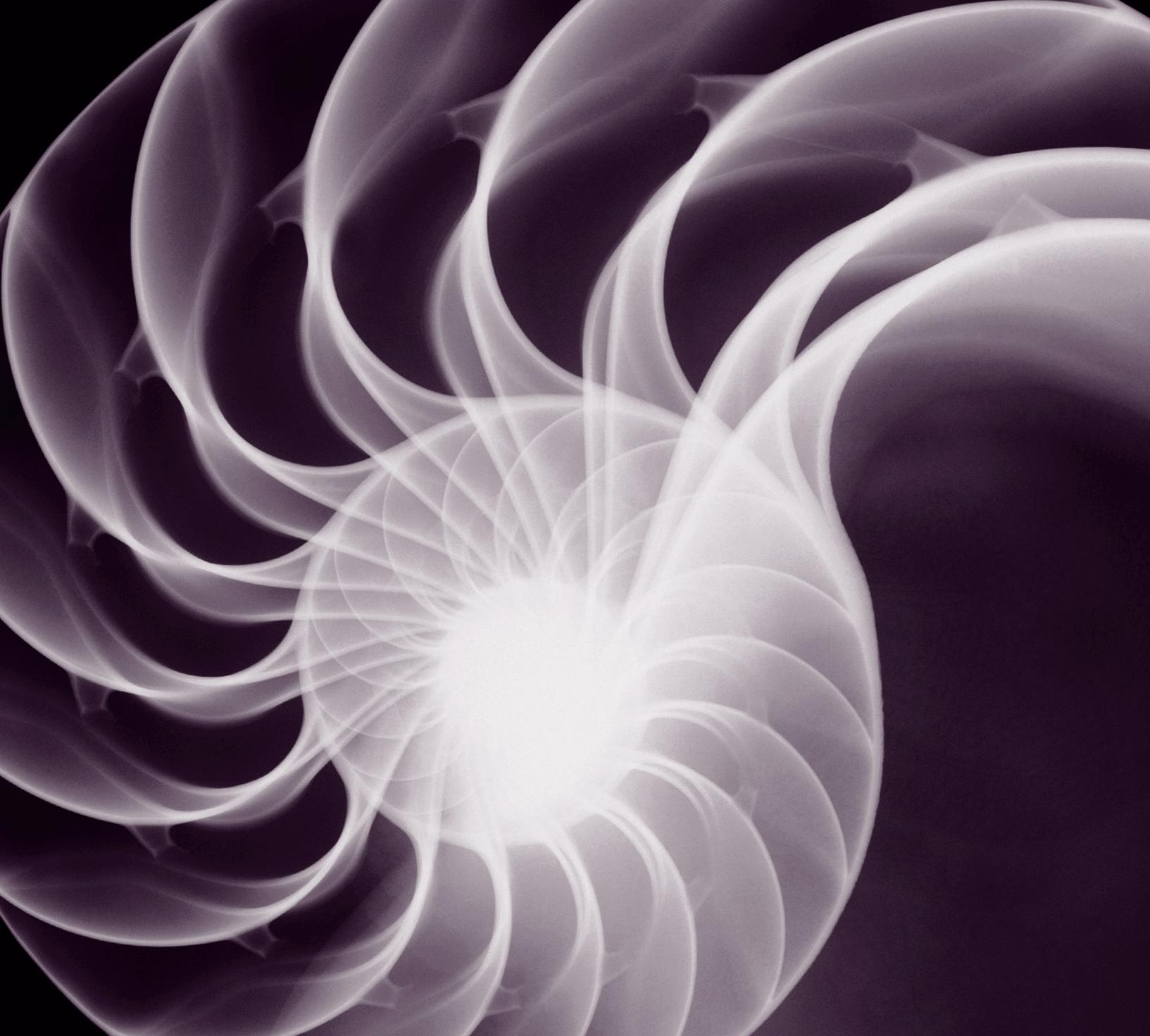
Optimizing (Level 5)

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.

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 their various maturity models including the evolving CMMI-SVC, which focuses on the delivery of services.

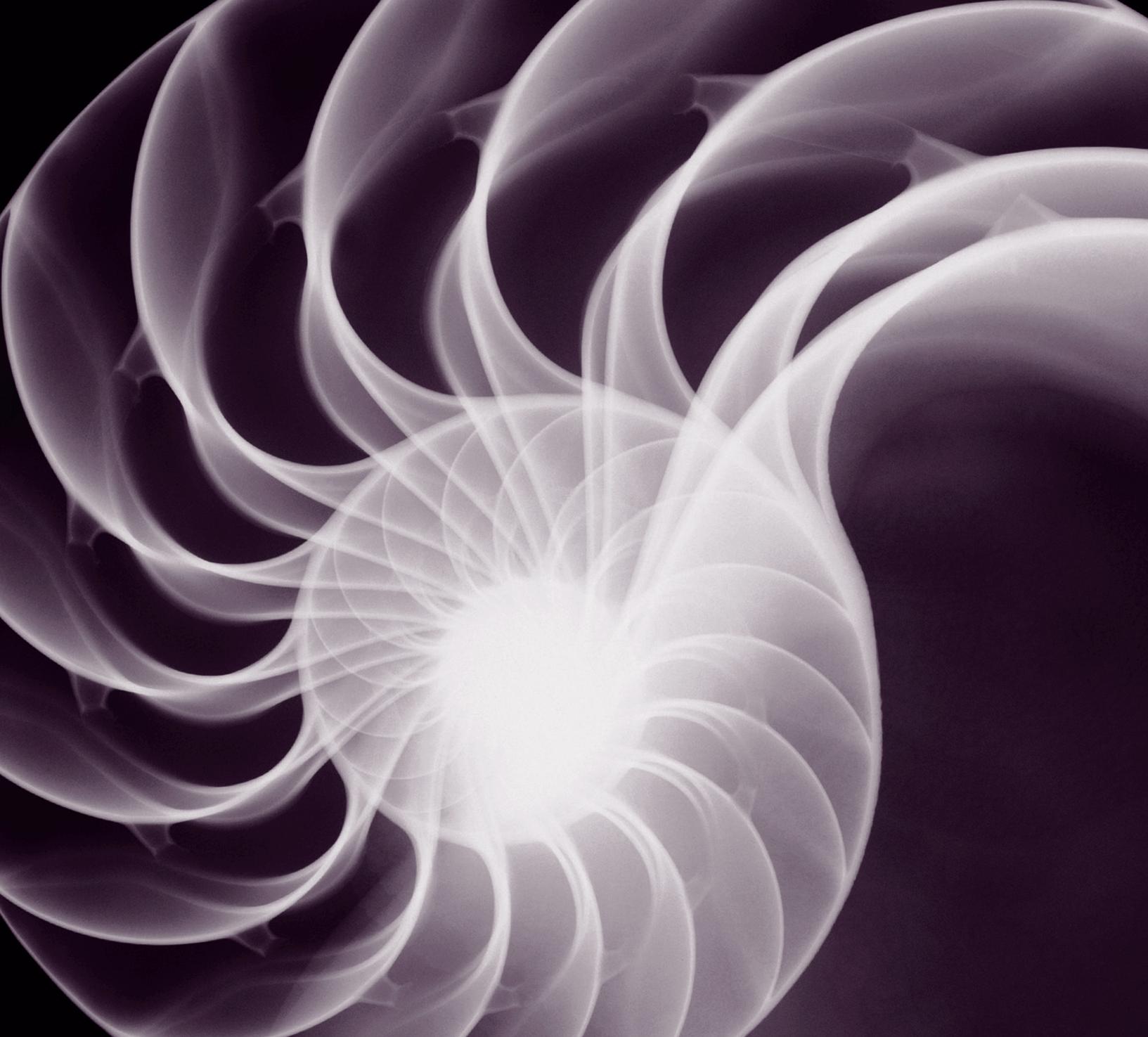


Appendix I: Example contents of a Statement of Requirement (SoR) and/or Invitation to Tender (ITT)

Appendix I: Example contents of a Statement of Requirement (SoR) and/or Invitation to Tender (ITT)

The following is an example of a minimum set of contents that should be included in an ITT or SoR:

- A description of the services, products and/or components required
- All relevant technical specifications, details and requirements
- An 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
- Details of the contents and structure of the responses required.



Appendix J: The typical contents of a Capacity Plan

J

Appendix J: The typical contents of a Capacity Plan

The typical contents of a Capacity Plan are as follows.

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.

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.

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.

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.

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.

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.

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.

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 resource usage, broken down by hardware platform. This information 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 they 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.

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.

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 process and the IT Financial Plan.

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
- Cost, both set-up and ongoing.



Appendix K: The typical contents of a recovery plan

K

Appendix K: The typical contents of a recovery plan

The typical contents of an ITSCM recovery plan are as follows.

GENERIC RECOVERY PLAN

1 DOCUMENT CONTROL

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

1.1 Document distribution

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

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

1.3 Document approval

This document must be approved by the following personnel:

Name	Title	Signature

2 SUPPORTING INFORMATION

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.

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, services or facility was last tested on:

2.3 Invocation

The following personnel are authorized to invoke this plan:

- 1
- 2

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.

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.

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.

System	Document Reference	Contact

2.7 Contact lists

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

Name	Organization/Role	Title	Contact Details

2.8 Recovery team

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

Name	Title	Contact Details

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. BCP, 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		

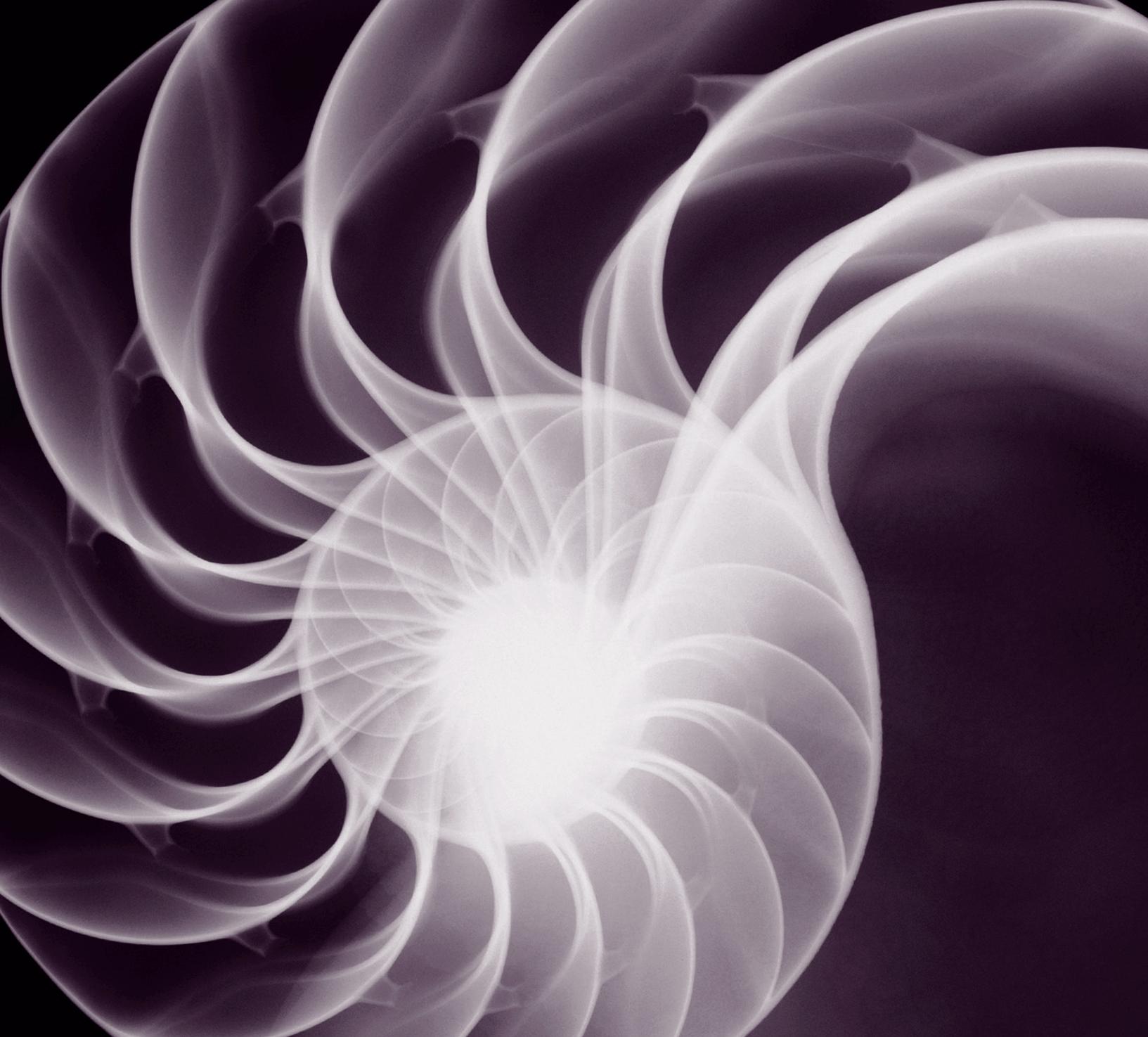
Advise customers and management of estimated recovery completion		

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.

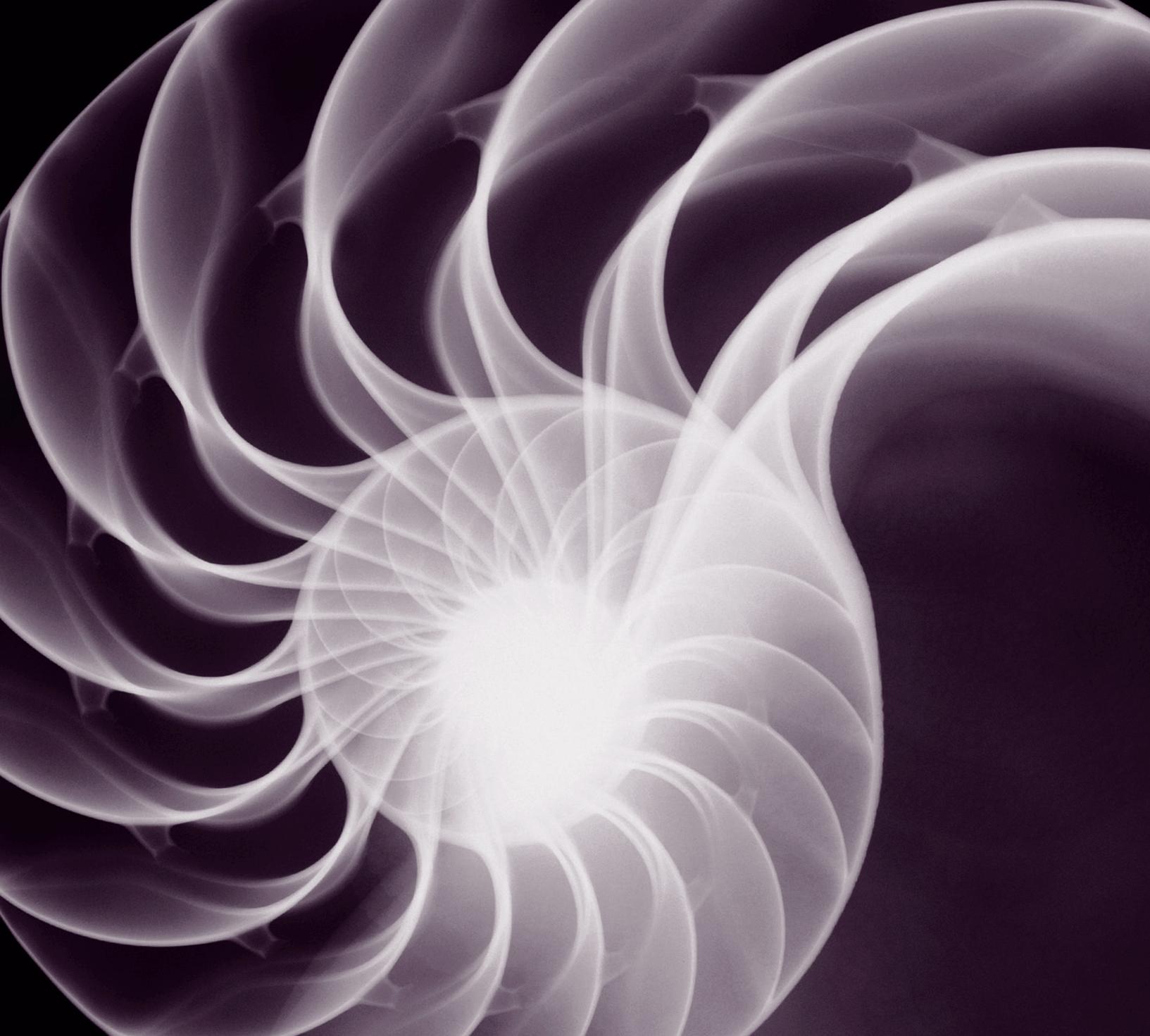
Where necessary, references should be made to supporting documentation (and its location), diagrams and other information sources. This should include the document reference number (if it exists). It is the responsibility of the plan author to ensure that this information is maintained with this plan. 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.



Further information

REFERENCES

1. Service Strategy
2. Service Transition
3. Service Operation
4. Continual Service Improvement
5. Peter Drucker
6. COBIT – ISACA
7. CMMI – CMU
8. eSCM-Service Portfolio – CMU
9. PRINCE2 – OGC
10. ISO 9000
11. ISO/IEC 20000
12. ISO 27001
13. Enterprise Architecture – Gartner
14. Plan Do Check Act – W Edwards Deming
15. Balanced Scorecard – Kaplan/Norton
16. Service Oriented Architecture – OASIS
17. Management of Risk – OGC
18. Recommended Practice for Software Requirements Specification (IEEE 830)
19. The Software Engineering Body of Knowledge (SWEBOK)
20. Object management architecture – OMG
21. Common Information Model (CIM) – DMTF
22. Web-Based Enterprise Management (WEBM) – DMTF
23. Application Management Specification – IBM
24. Windows Management Instrumentation – Microsoft
25. Desktop Management Instrumentation – Windows
26. Six Sigma – Motorola Inc
27. Dynamics of Software Development – Jim McCarthy
28. Requirements engineering; examples of tacit and explicit knowledge (Maiden & Rugg, 1995)
29. Business Analysis – Deborah Paul and Donald Yeates
30. Principles of Data Management – Keith Gordon
31. Practical Data Migration – John Morris



Glossary

Acronyms list

ACD	Automatic Call Distribution	DIKW	Data-to-Information-to-Knowledge-to-Wisdom
AM	Availability Management	ELS	Early Life Support
AMIS	Availability Management Information System	eSCM-CL	eSourcing Capability Model for Client Organizations
ASP	Application Service Provider	eSCM-SP	eSourcing Capability Model for Service Providers
BCM	Business Capacity Management	FMEA	Failure Modes and Effects Analysis
BCM	Business Continuity Management	FTA	Fault Tree Analysis
BCP	Business Continuity Plan	IRR	Internal Rate of Return
BIA	Business Impact Analysis	ISG	IT Steering Group
BRM	Business Relationship Manager	ISM	Information Security Management
BSI	British Standards Institution	ISMS	Information Security Management System
BSM	Business Service Management	ISO	International Organization for Standardization
CAB	Change Advisory Board	ISP	Internet Service Provider
CAB/EC	Change Advisory Board/Emergency Committee	IT	Information Technology
CAPEX	Capital Expenditure	ITSCM	IT Service Continuity Management
CCM	Component Capacity Management	ITSM	IT Service Management
CFIA	Component Failure Impact Analysis	itSMF	IT Service Management Forum
CI	Configuration Item	IVR	Interactive Voice Response
CMDB	Configuration Management Database	KEDB	Known Error Database
CMIS	Capacity Management Information System	KPI	Key Performance Indicator
CMM	Capability Maturity Model	LOS	Line of Service
CMMI	Capability Maturity Model Integration	M_o_R	Management of Risk
CMS	Configuration Management System	MTBF	Mean Time Between Failures
COTS	Commercial off the Shelf	MTBSI	Mean Time Between Service Incidents
CSF	Critical Success Factor	MTRS	Mean Time to Restore Service
CSI	Continual Service Improvement	MTTR	Mean Time To Repair
CSIP	Continual Service Improvement Plan	NPV	Net Present Value
CSP	Core Service Package		
CTI	Computer Telephony Integration		

OGC	Office of Government Commerce	TO	Technical Observation
OLA	Operational Level Agreement	TOR	Terms of Reference
OPEX	Operational Expenditure	TCO	Total Cost of Ownership
OPSI	Office of Public Sector Information	TCU	Total Cost of Utilization
PBA	Pattern of Business Activity	TQM	Total Quality Management
PIR	Post-Implementation Review	UC	Underpinning Contract
PFS	Prerequisite for Success	UP	User Profile
PSO	Projected Service Outage	VBF	Vital Business Function
QA	Quality Assurance	VOI	Value on Investment
QMS	Quality Management System	WIP	Work in Progress
RCA	Root Cause Analysis		
RFC	Request for Change		
ROI	Return on Investment		
RPO	Recovery Point Objective		
RTO	Recovery Time Objective		
SoC	Separation of Concerns		
SAC	Service Acceptance Criteria		
SACM	Service Asset and Configuration Management		
SCD	Supplier and Contract Database		
SCM	Service Capacity Management		
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		
SMO	Service Maintenance Objective		
SOP	Standard Operating Procedures		
SOR	Statement of requirements		
SPI	Service Provider Interface		
SPM	Service Portfolio Management		
SPO	Service Provisioning Optimization		
SPOF	Single Point of Failure		

Definitions list

The publication names included in parentheses after the name of a term identify where a reader can find more information about that term. This is either because the term is primarily used by that publication or because additional useful information about that term can be found there. Terms without a publication name associated with them may be used generally by several publications, or may not be defined in any greater detail than can be found in the glossary, i.e. we only point readers to somewhere they can expect to expand on their knowledge or to see a greater context. Terms with multiple publication names are expanded on in multiple publications.

Where the definition of a term includes another term, those related terms are highlighted in a second colour. This is designed to help the reader with their understanding by pointing them to additional definitions that are all part of the original term they were interested in. The form 'See also Term X, Term Y' is used at the end of a definition where an important related term is not used with the text of the definition itself.

Acceptance

Formal agreement that an **IT Service**, **Process**, **Plan**, or other **Deliverable** is complete, accurate, **Reliable** and meets its specified **Requirements**. Acceptance is usually preceded by **Evaluation** or **Testing** and is often required before proceeding to the next stage of a **Project** or **Process**. See also **Service Acceptance Criteria**.

Accounting

(Service Strategy) The **Process** responsible for identifying actual **Costs** of delivering **IT Services**, comparing these with budgeted costs, and managing variance from the **Budget**.

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

(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 **Service Level Agreement**, **Operational Level Agreement**.

Alert

(Service Operation) A warning that a threshold has been reached, something has changed, or a **Failure** has occurred. Alerts are often created and managed by **System Management** tools and are managed by the **Event Management Process**.

Analytical Modelling

(Service Strategy) (Service Design) (Continual Service Improvement) A technique that uses mathematical **Models** to predict the behaviour of a **Configuration Item** or **IT Service**. Analytical Models are commonly used in **Capacity Management** and **Availability Management**. See also **Modelling**.

Application

Software that provides **Functions** that are required by an **IT Service**. Each **Application** may be part of more than one **IT Service**. An Application runs on one or more **Servers** or **Clients**. See also **Application Management**, **Application Portfolio**.

Application Management

(Service Design) (Service Operation) The **Function** responsible for managing **Applications** throughout their **Lifecycle**.

Application Portfolio

(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)

(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

(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

(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**.

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

(Service Strategy) Any **Resource** or **Capability**. Assets of a **Service Provider** including anything that could contribute to the delivery of a **Service**. Assets can be one of the following types: Management, **Organization**, Process, Knowledge, People, Information, **Applications**, Infrastructure, and Financial Capital.

Asset Management

(Service Transition) Asset Management is the **Process** responsible for tracking and reporting the value and ownership of financial **Assets** throughout their **Lifecycle**. Asset Management is part of an overall **Service Asset** and **Configuration Management Process**.

Attribute

(Service Transition) A piece of information about a **Configuration Item**. Examples are: name, location, **Version** number, and **Cost**. Attributes of CIs are recorded in the Configuration Management Database (CMDB). *See also Relationship.*

Audit

Formal inspection and verification to check whether a **Standard** or set of **Guidelines** is being followed, that **Records** are accurate, or that **Efficiency** and **Effectiveness** targets are being met. An Audit may be carried out by internal or external groups. *See also Certification, Assessment.*

Automatic Call Distribution (ACD)

(Service Operation) Use of **Information Technology** to direct an incoming telephone call to the most appropriate person in the shortest possible time. ACD is sometimes called Automated Call Distribution.

Availability

(Service Design) Ability of a **Configuration Item** or **IT Service** to perform its agreed **Function** when required. Availability is determined by **Reliability**, **Maintainability**, **Serviceability**, **Performance** and **Security**. Availability is usually calculated as a percentage. This calculation is often based on **Agreed Service Time** and **Downtime**. It is **Best Practice** to calculate Availability using measurements of the **Business** output of the **IT Service**.

Availability Management

(Service Design) The **Process** responsible for defining, analysing, **Planning**, measuring and improving all aspects of the **Availability** of **IT Services**. Availability Management is responsible for ensuring that all **IT Infrastructure**, **Processes**, **Tools**, **Roles**, etc. are appropriate for the agreed **Service Level Targets** for Availability.

Availability Management Information System (AMIS)

(Service Design) A virtual repository of all **Availability Management** data, usually stored in multiple physical locations. *See also Service Knowledge Management System.*

Availability Plan

(Service Design) A **Plan** to ensure that existing and future **Availability Requirements** for **IT Services** can be provided **Cost Effectively**.

Back-out

See **Remediation**.

Backup

(Service Design) (Service Operation) Copying data to protect against loss of **Integrity** or **Availability** of the original.

Balanced Scorecard

(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

(Continual Service Improvement) A **Benchmark** used as a reference point. For example:

- An **ITSM** Baseline can be used as a starting point to measure the effect of a **Service Improvement Plan**
- A **Performance** Baseline can be used to measure changes in **Performance** over the lifetime of an **IT Service**
- A **Configuration Management** Baseline can be used to enable the **IT Infrastructure** to be restored to a known **Configuration** if a **Change** or **Release** fails.

Benchmark

(Continual Service Improvement) The recorded state of something at a specific point in time. A Benchmark can be created for a **Configuration**, a **Process**, or any other set of data. For example, a benchmark can be used in:

- **Continual Service Improvement**, to establish the current state for managing improvements
- **Capacity Management**, to document performance characteristics during normal operations.

See also Benchmarking, Baseline.

Benchmarking

(Continual Service Improvement) Comparing a Benchmark with a **Baseline** or with **Best Practice**. The term Benchmarking is also used to mean creating a series of **Benchmarks** over time, and comparing the results to measure progress or improvement.

Best Practice

Proven **Activities** or **Processes** that have been successfully used by multiple **Organizations**. **ITIL** is an example of Best Practice.

Brainstorming

(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.

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. Consists of a periodic negotiation cycle to set future **Budgets** (usually annual) and the day-to-day monitoring and adjusting of current **Budgets**.

Build

(Service Transition) The **Activity** of assembling a number of **Configuration Items** to create part of an **IT Service**. The term Build 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

(Service Strategy) An overall corporate entity or **Organization** formed of a number of **Business Units**. In the context of **ITSM**, the term Business 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 (BCM)

(Service Design) In the context of **ITSM**, Business Capacity Management is the **Activity** responsible for understanding future **Business Requirements** for use in the Capacity Plan. *See also* Service Capacity Management.

Business Case

(Service Strategy) Justification for a significant item of expenditure. Includes information about **Costs**, benefits, options, issues, **Risks**, and possible problems. *See also* Cost Benefit Analysis.

Business Continuity Management (BCM)

(Service Design) The **Business Process** responsible for managing **Risks** that could seriously affect the **Business**. BCM safeguards the interests of key stakeholders, reputation, brand and value-creating activities. The **BCM Process** involves reducing **Risks** to an acceptable level and planning for the recovery of **Business Processes** should a disruption to the **Business** occur. BCM sets the **Objectives**, **Scope** and **Requirements** for **IT Service Continuity Management**.

Business Continuity Plan (BCP)

(Service Design) A **Plan** defining the steps required to **Restore Business Processes** following a disruption. The **Plan** will also identify the triggers for **Invocation**, people to be involved, communications, etc. **IT Service Continuity Plans** form a significant part of **Business Continuity Plans**.

Business Customer

(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)

(Service Strategy) BIA is the **Activity** in **Business Continuity Management** that identifies **Vital Business Functions** and their dependencies. These dependencies may include **Suppliers**, people, other **Business Processes**, **IT Services**, etc. BIA defines the recovery requirements for **IT Services**. These requirements include **Recovery Time Objectives**, **Recovery Point Objectives** and minimum **Service Level Targets** for each **IT Service**.

Business Objective

(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

(Service Strategy) The day-to-day execution, monitoring and management of **Business Processes**.

Business Perspective

(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

(Service Strategy) The **Process** or **Function** responsible for maintaining a **Relationship** with the **Business**. **Business Relationship Management** usually includes:

- Managing personal **Relationships** with **Business managers**
- Providing input to **Service Portfolio Management**
- Ensuring that the **IT Service Provider** is satisfying the **Business** needs of the **Customers**

This **Process** has strong links with **Service Level Management**.

Business Service

An **IT Service** that directly supports a **Business Process**, as opposed to an **Infrastructure Service**, which is used internally by the **IT Service Provider** and is not usually visible to the **Business**.

The term **Business Service** is also used to mean a **Service** that is delivered to **Business Customers** by **Business Units**. For example, delivery of financial services to **Customers** of a bank, or goods to the **Customers** of a retail store. Successful delivery of **Business Services** often depends on one or more **IT Services**.

Business Service Management (BSM)

(Service Strategy) (Service Design) An approach to the management of **IT Services** that considers the **Business Processes** supported and the **Business** value provided.

This term also means the management of **Business Services** delivered to **Business Customers**.

Business Unit

(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

(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

(Service Operation) An Organization or Business Unit that handles large numbers of incoming and outgoing telephone calls. See also Service Desk.

Capability

(Service Strategy) The ability of an Organization, person, Process, Application, Configuration Item or IT Service to carry out an Activity. Capabilities are intangible Assets of an Organization. See also Resource.

Capacity

(Service Design) The maximum Throughput that a Configuration Item or IT Service can deliver whilst meeting agreed Service Level Targets. For some types of CI, Capacity may be the size or volume, for example a disk drive.

Capacity Management

(Service Design) The Process responsible for ensuring that the Capacity of IT Services and the IT Infrastructure is able to deliver agreed Service Level Targets in a Cost Effective and timely manner. Capacity Management considers all Resources required to deliver the IT Service, and plans for short-, medium- and long-term Business Requirements.

Capacity Management Information System (CMIS)

(Service Design) A virtual repository of all Capacity Management data, usually stored in multiple physical locations. See also Service Knowledge Management System.

Capacity Plan

(Service Design) A Capacity Plan is used to manage the Resources required to deliver IT Services. The Plan contains scenarios for different predictions of Business demand, and costed options to deliver the agreed Service Level Targets.

Capacity Planning

(Service Design) The Activity within Capacity Management responsible for creating a Capacity Plan.

Category

A named group of things that have something in common. Categories are used to group similar things together. For example, Cost Types are used to group similar types of Cost. Incident Categories are used to group similar types of Incident, CI Types are used to group similar types of Configuration Item.

Certification

Issuing a certificate to confirm Compliance to a Standard. Certification includes a formal Audit by an independent and Accredited body. The term Certification is also used to mean awarding a certificate to verify that a person has achieved a qualification.

Change

(Service Transition) The addition, modification or removal of anything that could have an effect on IT Services. The Scope should include all IT Services, Configuration Items, Processes, Documentation, etc.

Change Advisory Board (CAB)

(Service Transition) A group of people that advises the Change Manager in the Assessment, prioritization and scheduling of Changes. This board is usually made up of representatives from all areas within the IT Service Provider, representatives from the Business and Third Parties such as Suppliers.

Change History

(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

(Service Transition) The Process responsible for controlling the Lifecycle of all Changes. The primary objective of Change Management is to enable beneficial Changes to be made, with minimum disruption to IT Services.

Change Request

See Request for Change.

Change Schedule

(Service Transition) A Document that lists all approved Changes and their planned implementation dates. A Change Schedule is sometimes called a Forward Schedule of Change, even though it also contains information about Changes that have already been implemented.

Change Window

(Service Transition) A regular, agreed time when **Changes** or **Releases** may be implemented with minimal impact on **Services**. Change Windows are usually documented in **SLAs**.

Charging

(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.

Classification

The act of assigning a **Category** to something. Classification is used to ensure consistent management and reporting. **CIs**, **Incidents**, **Problems**, **Changes**, etc. are usually classified.

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 **Account Manager**.

The term client is also used to mean:

- A computer that is used directly by a **User**, for example a PC, Handheld Computer, or Workstation
- The part of a Client-Server **Application** that the **User** directly interfaces with. For example an e-mail Client.

Closed

(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

(Service Operation) The act of changing the **Status** of an **Incident**, **Problem**, **Change**, etc. to Closed.

COBIT

(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 the IT Governance Institute. See www.isaca.org for more information.

Cold Standby

See **Gradual Recovery**.

Commercial Off-The-Shelf (COTS)

(Service Design) 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

(Service Design) (Continual Service Improvement) The **Process** 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 **Service Capacity Management**.

Component CI

(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)

(Service Design) A technique that helps to identify the impact of **CI** failure on **IT Services**. A matrix is created with **IT Services** on one edge and **CIs** on the other. This enables the identification of critical **CIs** (that could cause the failure of multiple **IT Services**) and of 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

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

Configuration

(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 CIs.

Configuration Baseline

(Service Transition) A Baseline of a Configuration that has been formally agreed and is managed through the Change Management process. A Configuration Baseline is used as a basis for future Builds, Releases and Changes.

Configuration Control

(Service Transition) The Activity responsible for ensuring that adding, modifying or removing a CI is properly managed, for example by submitting a Request for Change or Service Request.

Configuration Identification

(Service Transition) The Activity responsible for collecting information about Configuration Items and their Relationships, and loading this information into the CMDB. Configuration Identification is also responsible for labelling the CIs themselves, so that the corresponding Configuration Records can be found.

Configuration Item (CI)

(Service Transition) Any Component that needs to be managed in order to deliver an IT Service. Information about each CI is recorded in a Configuration Record within the Configuration Management System and is maintained throughout its Lifecycle by Configuration Management. CIs are under the control of Change Management. CIs typically include IT Services, hardware, software, buildings, people, and formal documentation such as Process documentation and SLAs.

Configuration Management

(Service Transition) The Process responsible for maintaining information about Configuration Items required to deliver an IT Service, including their Relationships. This information is managed throughout the Lifecycle of the CI. Configuration Management is part of an overall Service Asset and Configuration Management Process.

Configuration Management System (CMS)

(Service Transition) A set of tools and databases that are used to manage an IT Service Provider's Configuration data. The CMS also includes information about Incidents, Problems, Known Errors, Changes and Releases; and may contain data about employees, Suppliers, locations, Business Units, Customers and Users. The CMS includes tools for collecting, storing, managing, updating, and presenting data about all Configuration Items and their Relationships. The CMS is maintained by Configuration Management and is used by all IT Service Management Processes. See also Service Knowledge Management System.

Continual Service Improvement (CSI)

(Continual Service Improvement) A stage in the Lifecycle of an IT Service and the title of one of the Core ITIL publications. Continual Service Improvement is responsible for managing improvements to IT Service Management Processes and IT Services. The Performance of the IT Service Provider is continually measured and improvements are made to Processes, IT Services and IT Infrastructure in order to increase Efficiency, Effectiveness, and Cost Effectiveness. See also Plan–Do–Check–Act.

Continuous Availability

(Service Design) An approach or design to achieve 100% Availability. A Continuously Available IT Service has no planned or unplanned Downtime.

Continuous Operation

(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 ensuring that a Process is followed. Example Controls include Policies, Procedures, Roles, RAID, door locks, etc. A control is sometimes called a Countermeasure or safeguard. Control also means to manage the utilization or behaviour of a Configuration Item, System or IT Service.

Control perspective

(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**. Example Control Perspectives include Reactive and Proactive management within **IT Operations**, or a **Lifecycle** view for an **Application Project** team.

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**, **Return on Investment**.

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 **KPI**, **Return on Investment**, **Value for Money**.

Countermeasure

Can be used to refer to any type of **Control**. The term Countermeasure is most often used when referring to measures that increase **Resilience**, **Fault Tolerance** or **Reliability** of an **IT Service**.

Crisis Management

(IT Service Continuity 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 a **Process**, **Project**, **Plan**, or **IT Service** is to succeed. **KPIs** are used to measure the achievement of each CSF. For example a CSF of 'protect **IT Services** when making Changes' could be measured by KPIs such as 'percentage reduction of unsuccessful Changes', 'percentage reduction in Changes causing Incidents', etc.

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 that defines and agrees the **Service Level Targets**. The term Customers is also sometimes informally used to mean **Users**, for example 'this is a **Customer**-focused Organization'.

Dashboard

(Service Operation) A graphical representation of overall **IT Service Performance** and **Availability**. Dashboard images may be updated in real-time, and can also be included in management reports and web pages. Dashboards can be used to support **Service Level Management**, **Event Management** or **Incident Diagnosis**.

Deliverable

Something that must be provided to meet a commitment in a **Service Level Agreement** or a **Contract**. Deliverable is also used in a more informal way to mean a planned output of any **Process**.

Demand Management

Activities that understand and influence **Customer** demand for **Services** and the provision of **Capacity** to meet these demands. At a **Strategic** level Demand Management can involve analysis of **Patterns of Business Activity** and **User Profiles**. At a tactical level it can involve use of **Differential Charging** to encourage **Customers** to use **IT Services** at less busy times. See also **Capacity Management**.

Dependency

The direct or indirect reliance of one **Process** or **Activity** on another.

Deployment

(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

(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**.

Detection

(Service Operation) A stage in the **Incident Lifecycle**. Detection results in the **Incident** becoming known to the **Service Provider**. Detection can be automatic, or can be the result of a user logging an **Incident**.

Development

(Service Design) The **Process** responsible for creating or modifying an **IT Service** or **Application**. Also used to mean the **Role** or group that carries out Development work.

Development Environment

(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 Environments** or **Live Environments**. See also **Development**.

Diagnosis

(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 **IT Service Function** at different times.

Document

Information in readable form. A Document may be paper or electronic. For example, a **Policy** statement, **Service Level Agreement**, **Incident Record**, diagram of computer room layout. See also **Record**.

Downtime

(Service Design) (Service Operation) The time when a **Configuration Item** or **IT Service** is not **Available** during its **Agreed Service Time**. The **Availability** of an **IT Service** is often calculated from **Agreed Service Time** and Downtime.

Driver

Something that influences **Strategy**, **Objectives** or **Requirements**. For example, new legislation or the actions of competitors.

Economies of scale

(Service Strategy) The reduction in average **Cost** that is possible from increasing the usage of an **IT Service** or **Asset**.

Effectiveness

(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 **KPI**.

Efficiency

(Continual Service Improvement) A measure of whether the right amount of resources 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 **KPI**.

Environment

(Service Transition) A subset of the **IT Infrastructure** that is used for a particular purpose. For example: **Live Environment**, **Test Environment**, **Build Environment**. It is possible for multiple Environments to share a **Configuration Item**, for example **Test** and **Live Environments** may use different partitions on a single mainframe computer. Also used in the term **Physical Environment** to mean the accommodation, air conditioning, power system, etc.

Environment is also used as a generic term to mean the external conditions that influence or affect something.

Error

(Service Operation) A design flaw or malfunction that causes a **Failure** of one or more **Configuration Items** or **IT Services**. A mistake made by a person or a faulty **Process** that affects a **CI** or **IT Service** is also an Error.

Escalation

(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 Service Providers (eSCM-SP)

(Service Strategy) A framework to help **IT Service Providers** develop their **IT Service Management Capabilities** from a **Service Sourcing** perspective. eSCM-SP was developed by Carnegie Mellon University, US.

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.

Evaluation

(Service Transition) The **Process** responsible for assessing a new or **Changed IT Service** to ensure that **Risks** have been managed and to help determine whether to proceed with the **Change**.

Evaluation is also used to mean comparing an actual **Outcome** with the intended **Outcome**, or comparing one alternative with another.

Event

(Service Operation) A change of state that has significance for the management of a **Configuration Item** or **IT Service**.

The term Event is also used to mean an **Alert** or notification created by any **IT Service**, **Configuration Item** or **Monitoring** tool. Events typically require **IT Operations** personnel to take actions, and often lead to **Incidents** being logged.

Event Management

(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 **KPIs** or other important targets that have exceeded defined **Thresholds**. Examples include **SLA** targets being missed or about to be missed, and a **Performance Metric** indicating a potential **Capacity** problem.

Expanded Incident Lifecycle

(Availability Management) Detailed stages in the **Lifecycle** of an **Incident**. The stages are **Detection**, **Diagnosis**, **Repair**, **Recovery**, **Restoration**. The Expanded Incident Lifecycle is used to help understand all contributions to the **Impact** of **Incidents** and to **Plan** how these could be controlled or reduced.

External Service Provider

(Service Strategy) An **IT Service Provider** that is part of a different **Organization** to its **Customer**. An **IT Service Provider** may have both **Internal Customers** and **External Customers**.

External Sourcing

See **Outsourcing**.

Facilities Management

(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

(Service Operation) Loss of ability to **Operate** to **Specification**, or to deliver the required output. The term Failure may be used when referring to **IT Services**, **Processes**, **Activities**, **Configuration Items**, etc. A Failure often causes an **Incident**.

Fast Recovery

(Service Design) A **Recovery Option** that is also known as Hot Standby. Provision is made to **Recover** the **IT Service** in a short period of time: typically less than 24 hours. Fast Recovery typically uses a dedicated **Fixed Facility** with computer **Systems**, and software configured ready to run the **IT Services**. Fast Recovery may take up to 24 hours if there is a need to **Restore** data from **Backups**.

Fault

See **Error**.

Fault Tolerance

(Service Design) The ability of an **IT Service** or **Configuration Item** to continue to **Operate** correctly after **Failure** of a **Component** part. See also **Resilience**, **Countermeasure**.

Fault Tree Analysis (FTA)

(Service Design) (Continual Service Improvement) A technique that can be used to determine the chain of events that leads to a **Problem**. Fault Tree Analysis represents a chain of events using Boolean notation in a diagram.

Financial Management

(Service Strategy) The **Function** and **Processes** responsible for managing an **IT Service Provider's Budgeting**, **Accounting** and **Charging Requirements**.

Fit for Purpose

An informal term used to describe a **Process**, **Configuration Item**, **IT Service**, etc. that is capable of meeting its objectives or **Service Levels**. Being Fit for Purpose requires suitable design, implementation, control and maintenance.

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 they use to carry out one or more **Processes** or **Activities**. For example the **Service Desk**.

The term Function also has two other meanings:

- An intended purpose of a **Configuration Item**, **Person**, **Team**, **Process**, or **IT Service**. For example one Function of an e-mail **Service** may be to store and forward outgoing mails, one Function of a **Business Process** may be to dispatch goods to **Customers**.
- To perform the intended purpose correctly, 'The computer is Functioning'.

Governance

Ensuring that **Policies** and **Strategy** are actually implemented, and that required **Processes** are correctly followed. Governance includes defining **Roles** and responsibilities, measuring and reporting, and taking actions to resolve any issues identified.

Gradual Recovery

(Service Design) A **Recovery Option** that is also known as Cold Standby. Provision is made to **Recover** the **IT Service** in a period of time greater than 72 hours. 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**.

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

(Service Design) An approach or design that minimizes or hides the effects of **Configuration Item Failure** on 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 of **Incidents**, and the **Impact** of **Incidents**.

Hot Standby

See **Fast Recovery** or **Immediate Recovery**.

Immediate Recovery

(Service Design) A **Recovery Option** that is also known as Hot Standby. Provision is made to **Recover** the **IT Service** with no loss of **Service**. Immediate Recovery typically uses Mirroring, Load Balancing and Split Site technologies.

Impact

(Service Operation) (Service Transition) A measure of the effect of an **Incident**, **Problem** or **Change** on **Business Processes**. Impact is often based on how **Service Levels** will be affected. Impact and **Urgency** are used to assign Priority.

Incident

(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

(Service Operation) The **Process** responsible for managing the **Lifecycle** of all **Incidents**. The primary **Objective** of **Incident Management** is to return the **IT Service** to **Customers** as quickly as possible.

Incident Record

(Service Operation) A **Record** containing the details of an **Incident**. Each Incident record documents the **Lifecycle** of a single **Incident**.

Indirect Cost

(Service Strategy) A **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**.

Information Security Management (ISM)

(Service Design) The Process that ensures the Confidentiality, Integrity and Availability of an Organization's Assets, information, data and IT Services. Information Security Management usually forms part of an Organizational approach to Security Management that has a wider scope than the IT Service Provider, and includes handling of paper, building access, phone calls, etc., for the entire Organization.

Information Security Management System (ISMS)

(Service Design) The framework of Policy, Processes, Standards, Guidelines and tools that ensures an Organization can achieve its Information Security Management Objectives.

Information Security Policy

(Service Design) The Policy that governs the Organization's approach to Information Security Management.

Information Technology (IT)

The use of technology for the storage, communication or processing of information. The technology typically includes computers, telecommunications, Applications and other software. The information may include Business data, voice, images, video, etc. Information Technology is often used to support Business Processes through IT Services.

Infrastructure Service

An IT Service that is not directly used by the Business, but is required by the IT Service Provider so they can provide other IT Services. For example directory services, naming services, or communication services.

Insourcing

See Internal Sourcing.

Integrity

(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

(Service Design) A Recovery Option that is also known as Warm Standby. Provision is made to Recover the IT Service in a period of time between 24 and 72 hours. Intermediate Recovery typically 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.

Internal Service Provider

(Service Strategy) An IT Service Provider that is part of the same Organization as its Customer. An IT Service Provider may have both Internal Customers and External Customers.

Internal Sourcing

(Service Strategy) Using an Internal Service Provider to manage IT Services.

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.

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 ISO.

ISO 9001

An international Standard for Quality Management Systems. See also ISO 9000, Standard.

ISO/IEC 20000

ISO Specification and Code of Practice for IT Service Management. ISO/IEC 20000 is aligned with ITIL Best Practice.

ISO/IEC 27001

(Service Design) (Continual Service Improvement) ISO Specification for Information Security Management. The corresponding Code of Practice is ISO/IEC 17799. See also Standard.

IT Infrastructure

All of the hardware, software, networks, facilities, etc. that are required to develop, **Test**, deliver, **Monitor**, **Control** or support **IT Services**. The term **IT Infrastructure** includes all of the **Information Technology** but not the associated people, **Processes** and documentation.

IT Operations

(Service Operation) **Activities** carried out by **IT Operations Control**, including Console Management, **Job Scheduling**, Backup and Restore, and Print and Output Management. **IT Operations** is also used as a synonym for **Service Operation**.

IT Service

A **Service** provided to one or more **Customers** by an **IT Service Provider**. An **IT Service** is based on the use of **Information Technology** and supports the **Customer's Business Processes**. An **IT Service** is made up from a combination of people, **Processes** and technology and should be defined in a **Service Level Agreement**.

IT Service Continuity Management (ITSCM)

(Service Design) The **Process** responsible for managing **Risks** that could seriously affect **IT Services**. ITSCM ensures that the **IT Service Provider** can always provide minimum agreed **Service Levels**, by reducing the **Risk** to an acceptable level and **Planning** for the **Recovery** of **IT Services**. ITSCM should be designed to support **Business Continuity Management**.

IT Service Continuity Plan

(Service Design) A **Plan** defining the steps required to **Recover** one or more **IT Services**. The **Plan** will also identify the triggers for **Invocation**, people to be involved, communications, etc. The **IT Service Continuity Plan** should be part of a **Business Continuity Plan**.

IT Service Management (ITSM)

The implementation and management of **Quality IT Services** that meet the needs of the **Business**. **IT Service Management** is performed by **IT Service Providers** through an appropriate mix of people, **Process** and **Information Technology**. See also **Service Management**.

IT Service Provider

(Service Strategy) A **Service Provider** that provides **IT Services** to **Internal Customers** or **External Customers**.

IT Steering Group (ISG)

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**.

ITIL

A set of **Best Practice** guidance for **IT Service Management**. ITIL is owned by the **OGC** and consists of a series of publications giving guidance on the provision of **Quality IT Services**, and on the **Processes** and facilities needed to support them. See www.itil.co.uk 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

(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)

(Service Design) (Continual Service Improvement) A **Metric** that is used to help manage a **Process**, **IT Service** or **Activity**. Many **Metrics** may be measured, but only the most important of these are defined as **KPIs** and used to actively manage and report on the **Process**, **IT Service** or **Activity**. KPIs should be selected to ensure that **Efficiency**, **Effectiveness**, and **Cost Effectiveness** are all managed. See also **Critical Success Factor**.

Knowledge Base

(Service Transition) A logical database containing the data used by the **Service Knowledge Management System**.

Knowledge Management

(Service Transition) The **Process** responsible for gathering, analysing, storing and sharing knowledge and information within an **Organization**. The primary purpose of **Knowledge Management** is to improve **Efficiency** by reducing the need to rediscover knowledge. See also **Service Knowledge Management System**.

Known Error

(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 **Detect**, **Respond**, **Diagnose**, **Repair**, **Recover**, **Restore**
- The Lifecycle of a Server may include: **Ordered**, **Received**, In **Test**, **Live**, **Disposed**, etc.

Line of Service (LOS)

(Service Strategy) A **Core Service** or **Supporting Service** that has multiple **Service Level Packages**. A line of Service is managed by a Product Manager and each **Service Level Package** is designed to support a particular market segment.

Live

(Service Transition) Refers to an **IT Service** or **Configuration Item** that is being used to deliver **Service** to a **Customer**.

Live Environment

(Service Transition) A controlled **Environment** containing **Live Configuration Items** used to deliver **IT Services** to **Customers**.

Maintainability

(Service Design) A measure of how quickly and **Effectively** a **Configuration Item** or **IT Service** can be restored to normal working after a **Failure**. Maintainability is often measured and reported as **MTRS**.

Maintainability is also used in the context of **Software** or **IT Service Development** to mean ability to be **Changed** or **Repaired** easily.

Major Incident

(Service Operation) The highest **Category of Impact** for an **Incident**. A Major Incident results in significant disruption to the **Business**.

Managed Services

(Service Strategy) A perspective on **IT Services** that emphasizes the fact that they are managed. The term **Managed Services** is also used as a synonym for **Outsourced IT Services**.

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 KPIs such as 'Percentage of **Changes** leading to **Incidents**', or 'first-time fix rate'.

Management of Risk (M_o_R)

The **OGC** methodology for managing **Risks**. 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.m-o-r.org for more details.

Management System

The framework of **Policy**, **Processes** and **Functions** that ensures an **Organization** can achieve its **Objectives**.

Manual Workaround

A **Workaround** that requires manual intervention. Manual Workaround is also used as the name of a **Recovery Option** in which the **Business Process Operates** without the use of **IT Services**. This is a temporary measure and is usually combined with another **Recovery Option**.

Maturity

(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.

Mean Time Between Failures (MTBF)

(Service Design) A **Metric** for measuring and reporting **Reliability**. MTBF is the average time that a **Configuration Item** or **IT Service** can perform its agreed **Function** without interruption. This is measured from when the **CI** or **IT Service** starts working, until it next fails.

Mean Time Between Service Incidents (MTBSI)

(Service Design) A **Metric** used for measuring and reporting **Reliability**. MTBSI is the mean time from when a **System** or **IT Service** fails, until it next fails. MTBSI is equal to **MTBF** + **MTRS**.

Mean Time To Repair (MTTR)

The average time taken to repair a **Configuration Item** or **IT Service** after a **Failure**. MTTR is measured from when the **CI** or **IT Service** fails until it is repaired. MTTR does not include the time required to **Recover** or **Restore**. MTTR is sometimes incorrectly used to mean **Mean Time to Restore Service**.

Mean Time to Restore Service (MTRS)

The average time taken to restore a **Configuration Item** or **IT Service** after a **Failure**. MTRS is measured from when the **CI** or **IT Service** fails until it is fully restored and delivering its normal functionality. See also **Maintainability**, **Mean Time to Repair**.

Metric

(Continual Service Improvement) Something that is measured and reported to help manage a **Process**, **IT Service** or **Activity**. See also **KPI**.

Middleware

(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 **Off the Shelf**.

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

(Service Operation) Repeated observation of a **Configuration Item**, **IT Service** or **Process** to detect **Events** and to ensure that the current status is known.

Objective

The defined purpose or aim of a **Process**, an **Activity** or an **Organization** as a whole. Objectives are usually expressed as measurable targets. The term **Objective** is also informally used to mean a **Requirement**. See also **Outcome**.

Off-The-Shelf

See **Commercial Off-The-Shelf**.

Office of Government Commerce (OGC)

OGC owns the **ITIL** brand (copyright and trademark). OGC is a UK Government department that supports the delivery of the government's procurement agenda through its work in collaborative procurement and in raising levels of procurement skills and capability within departments. It also provides support for complex public sector projects.

Off-shore

(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 **Service Desk**. See also **On-shore**.

On-shore

(Service Strategy) Provision of **Services** from a location within the country where the **Customer** is based. See also **Off-shore**.

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

(Service Operation) Day-to-day management of an **IT Service**, **System**, or other **Configuration Item**. Operation is also used to mean any pre-defined **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 **Operational** is also a synonym for **Live**.

Operational Cost

Cost resulting from running the **IT Services**. Often repeating payments. For example staff costs, hardware maintenance and electricity (also known as 'current expenditure' or 'revenue expenditure').

Operational Level Agreement (OLA)

(Service Design) (Continual Service Improvement) An **Agreement** between an **IT Service Provider** and another part of the same **Organization**. An OLA supports the **IT Service Provider's** delivery of **IT Services** to **Customers**. The OLA defines the goods or **Services** to be provided and the responsibilities of both parties. For example there could be an OLA:

- Between the **IT Service Provider** and a procurement department to obtain hardware in agreed times
- Between the **Service Desk** and a **Support Group** to provide **Incident Resolution** in agreed times.

See also **Service Level Agreement**.

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. Examples of Organizations that are not companies include **International Standards Organization** or **itSMF**. The term **Organization** 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**; delivering an **IT Service**, etc. The term **Outcome** is used to refer to intended results, as well as to actual results. *See also* **Objective**.

Outsourcing

(Service Strategy) Using an **External Service Provider** to manage **IT Services**.

Overhead

See **Indirect cost**.

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

(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.

Pattern of Business Activity (PBA)

(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.

Performance

A measure of what is achieved or delivered by a **System**, person, team, Process, or **IT Service**.

Performance Management

(Continual Service Improvement) The **Process** responsible for day-to-day **Capacity Management Activities**. These include monitoring, threshold detection, **Performance analysis** and **Tuning**, and implementing changes related to **Performance** and **Capacity**.

Pilot

(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* **Test**, **Evaluation**.

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

(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

(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**.

PMBOK

A **Project** management **Standard** maintained and published by the Project Management Institute. PMBOK stands for Project Management Body of Knowledge. See www.pmi.org for more information. *See also PRINCE2*.

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

(Service Design) A prefabricated building, or a large vehicle, provided by a **Third Party** and moved to a site when needed by an **IT Service Continuity Plan**. *See also Recovery Option.*

Post-Implementation Review (PIR)

A **Review** that takes place after a **Change** or a **Project** has been implemented. A PIR determines if the **Change** or **Project** was successful, and identifies opportunities for improvement.

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**. A PFS is often an output from one **Process** that is a required input to another **Process**.

Pricing

(Service Strategy) The **Activity** for establishing how much **Customers** will be **Charged**.

PRINCE2

The standard UK government methodology for Project management. See www.ocg.gov.uk/prince2 for more information. *See also PMBOK.*

Priority

(Service Transition) (Service Operation) A **Category** used to identify the relative importance of an **Incident**, **Problem** or **Change**. Priority is based on **Impact** and **Urgency**, and is used to identify required times for actions to be taken. For example, the **SLA** may state that Priority 2 **Incidents** must be resolved within 12 hours.

Problem

(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

(Service Operation) The **Process** responsible for managing the **Lifecycle** of all **Problems**. The primary objectives of Problem Management are to prevent **Incidents** from happening, and to minimize the **Impact of Incidents** that cannot be prevented.

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. A Process may include any of the **Roles**, responsibilities, tools and management **Controls** required to reliably deliver the outputs. A Process may define **Policies**, **Standards**, **Guidelines**, **Activities**, and **Work Instructions** if they are needed.

Process Control

The **Activity** of planning and regulating a **Process**, with the **Objective** of performing the **Process** in an **Effective**, **Efficient**, and consistent manner.

Process Owner

A Role responsible for ensuring that a **Process** is **Fit for Purpose**. The Process Owner's responsibilities include sponsorship, **Design**, **Change Management** and continual improvement of the **Process** and its **Metrics**. This **Role** is often assigned to the same person who carries out the **Process Manager Role**, but the two **Roles** may be separate in larger **Organizations**.

Pro-forma

A template, or example **Document** containing example data that will be replaced with the 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** required to achieve an **Objective** or other **Outcome**. Each Project has a **Lifecycle** that typically includes initiation, **Planning**, execution, **Closure**, etc. Projects are usually managed using a formal methodology such as **PRINCE2**.

Quality

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 Management System (QMS)

(Continual Service Improvement) The set of **Processes** responsible for ensuring that all work carried out by an **Organization** is of a suitable **Quality** to reliably meet **Business Objectives** or **Service Levels**. See also **ISO 9000**.

RACI

(Service Design) (Continual Service Improvement) A **Model** used to help define Roles and Responsibilities. RACI stands for Responsible, Accountable, Consulted and Informed. See also **Stakeholder**.

Reciprocal Arrangement

(Service Design) A **Recovery Option**. An agreement between two **Organizations** to share resources in an emergency. For example, **Computer Room** space or use of a mainframe.

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

(Service Design) (Service Operation) Returning a **Configuration Item** or an **IT Service** to a working state. Recovery of an **IT Service** often includes recovering data to a known consistent state. After Recovery, further steps may be needed before the **IT Service** can be made available to the **Users** (Restoration).

Recovery Option

(Service Design) A **Strategy** for responding to an interruption to **Service**. Commonly used **Strategies** are **Do Nothing**, **Manual Workaround**, **Reciprocal Arrangement**, **Gradual Recovery**, **Intermediate Recovery**, **Fast Recovery**, **Immediate Recovery**. Recovery Options may make use of dedicated facilities, or **Third Party** facilities shared by multiple **Businesses**.

Redundancy

See **Fault Tolerance**.

The term Redundant also has a generic meaning of obsolete, 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 **Configuration Management** it is a link between two **Configuration Items** that identifies a dependency or connection between them. For example **Applications** may be linked to the **Servers** they run on. **IT Services** have many links to all the **CIs** that contribute to them.

Relationship Processes

The ISO/IEC 20000 Process group that includes Business Relationship Management and Supplier Management.

Release

(Service Transition) A collection of hardware, software, documentation, Processes or other Components required to implement one or more approved Changes to IT Services. The contents of each Release are managed, tested, and deployed as a single entity.

Release and Deployment Management

(Service Transition) The Process responsible for both Release Management and Deployment.

Release Management

(Service Transition) The Process responsible for Planning, scheduling and controlling the movement of Releases to Test and Live Environments. The primary Objective of Release Management is to ensure that the integrity of the Live Environment is protected and that the correct Components are released. Release Management is part of the Release and Deployment Management Process.

Release Record

(Service Transition) A Record in the CMDB that defines the content of a Release. A Release Record has Relationships with all Configuration Items that are affected by the Release.

Reliability

(Service Design) (Continual Service Improvement) A measure of how long a Configuration Item or IT Service can perform its agreed Function without interruption. Usually measured as MTBF or MTBSI. The term Reliability can also be used to state how likely it is that a Process, Function, etc. will deliver its required outputs. See also Availability.

Repair

(Service Operation) The replacement or correction of a failed Configuration Item.

Request for Change (RFC)

(Service Transition) A formal proposal for a Change to be made. An RFC includes details of the proposed Change, and may be recorded on paper or electronically. The term RFC is often misused to mean a Change Record, or the Change itself.

Request Fulfilment

(Service Operation) The Process responsible for managing the Lifecycle of all Service Requests.

Requirement

(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

(Service Design) The ability of a Configuration Item or IT Service to resist Failure or to Recover quickly following a Failure. For example an armoured cable will resist failure when put under stress. See also Fault Tolerance.

Resolution

(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.

Resource

(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

(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

(Service Transition) Permanent removal of an **IT Service**, or other **Configuration Item**, from the **Live Environment**. Retired is a stage in the **Lifecycle** of many **Configuration Items**.

Return on Investment (ROI)

(Service Strategy) (Continual Service Improvement) 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.

Return to Normal

(Service Design) The phase of an **IT Service Continuity Plan** during which full normal operations are resumed. For example, if an alternate 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 **Post-Implementation Review**.

Rights

(Service Operation) Entitlements, or permissions, granted to a **User** or **Role**. For example the Right to modify particular data, or to authorize a **Change**.

Risk

A possible event that could cause harm or loss, or affect the ability to achieve **Objectives**. A Risk is measured by the probability of a **Threat**, the **Vulnerability** of the **Asset** to that **Threat**, and the **Impact** it would have if it occurred.

Risk Assessment

The initial steps of **Risk Management**. 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**. See also **Risk Assessment**.

Role

A set of responsibilities, **Activities** and authorities granted to a person or team. A Role is defined in a **Process**. One person or team may have multiple Roles, for example the Roles of **Configuration Manager** and **Change Manager** may be carried out by a single person.

Root Cause

(Service Operation) The underlying or original cause of an **Incident** or **Problem**.

Running Costs

See **Operational Cost**.

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 Policy

See **Information Security Policy**.

Separation of Concerns (SoC)

(Service Strategy) 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

(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**.

Service Acceptance Criteria (SAC)

(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 **Capability** or **Resource** of a **Service Provider**. See also **Asset**.

Service Capacity Management (SCM)

(Service Design) (Continual Service Improvement) The **Activity** responsible for understanding the **Performance** and **Capacity** of **IT Services**. The **Resources** used by each **IT Service** and the pattern of usage over time are collected, recorded, and analysed for use in the **Capacity Plan**. See also **Business Capacity Management**, **Component Capacity Management**.

Service Catalogue

(Service Design) A database or structured **Document** with information about all **Live IT Services**, including those available for **Deployment**. The Service Catalogue is the only part of the **Service Portfolio** published to **Customers**, and is used to support the sale and delivery of **IT Services**. The Service Catalogue includes information about deliverables, prices, contact points, ordering and request **Processes**.

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

(Service Design) A stage in the **Lifecycle** of an **IT Service**. Service Design includes a number of **Processes** and **Functions** and is the title of one of the Core **ITIL** publications. See also **Design**.

Service Design Package

(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

(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)

(Service Design) An **Activity** that identifies underlying causes of one or more **IT Service** interruptions. SFA identifies opportunities to improve the **IT Service Provider's Processes** and tools, and not just the **IT Infrastructure**. SFA is a time-constrained, project-like activity, rather than an ongoing process of analysis.

Service Hours

(Service Design) (Continual Service Improvement) 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)

(Continual Service Improvement) A formal **Plan** to implement improvements to a **Process** or **IT Service**.

Service Knowledge Management System (SKMS)

(Service Transition) A set of tools and databases that are used to manage knowledge and information. The SKMS includes the **Configuration Management System**, as well as other tools and databases. The SKMS stores, manages, updates, and presents all information that an **IT Service Provider** needs to manage the full **Lifecycle** of **IT Services**.

Service Level

Measured and reported achievement against one or more **Service Level Targets**. The term **Service Level** is sometimes used informally to mean **Service Level Target**.

Service Level Agreement (SLA)

(Service Design) (Continual Service Improvement) An **Agreement** between an **IT Service Provider** and a **Customer**. The SLA describes the **IT Service**, documents **Service Level Targets**, and specifies the responsibilities of the **IT Service Provider** and the **Customer**. A single SLA may cover multiple **IT Services** or multiple customers. See also **Operational Level Agreement**.

Service Level Management (SLM)

(Service Design) (Continual Service Improvement) The **Process** responsible for negotiating **Service Level Agreements**, and ensuring that these are met. SLM is responsible for ensuring that all **IT Service Management Processes**, **Operational Level Agreements**, and **Underpinning Contracts**, are appropriate for the agreed **Service Level Targets**. SLM monitors and reports on **Service Levels**, and holds regular **Customer reviews**.

Service Level Package (SLP)

(Service Strategy) A defined level of **Utility** and **Warranty** for a particular **Service Package**. Each SLP is designed to meet the needs of a particular **Pattern of Business Activity**. See also **Line of Service**.

Service Level Requirement (SLR)

(Service Design) (Continual Service Improvement) A **Customer Requirement** for an aspect of an **IT Service**. SLRs are based on **Business Objectives** and are used to negotiate agreed **Service Level Targets**.

Service Level Target

(Service Design) (Continual Service Improvement) 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 design is Fit for Purpose**. Service Level Targets should be **SMART**, and are usually based on **KPIs**.

Service Management

Service Management is a set of specialized organizational capabilities for providing value to **Customers** in the form of **Services**.

Service Management Lifecycle

An approach to **IT Service Management** that emphasizes the importance of coordination and **Control** across the various **Functions**, **Processes**, and **Systems** necessary to manage the full **Lifecycle of IT Services**. The Service Management Lifecycle approach considers the **Strategy**, **Design**, **Transition**, **Operation** and **Continuous Improvement** of **IT Services**.

Service Manager

A manager who is responsible for managing the end-to-end **Lifecycle** of one or more **IT Services**. The term Service Manager is also used to mean any manager within the **IT Service Provider**. Most commonly used to refer to a **Business Relationship Manager**, a **Process Manager**, an **Account Manager** or a senior manager with responsibility for **IT Services** overall.

Service Operation

(Service Operation) A stage in the **Lifecycle** of an **IT Service**. Service Operation includes a number of **Processes** and **Functions** and is the title of one of the Core **ITIL** publications. See also **Operation**.

Service Owner

(Continual Service Improvement) A **Role** that is accountable for the delivery of a specific **IT Service**.

Service Portfolio

(Service Strategy) The complete set of **Services** that are managed by a **Service Provider**. The Service Portfolio is used to manage the entire **Lifecycle** of all **Services**, and includes three **Categories**: **Service Pipeline** (proposed or in **Development**); **Service Catalogue** (Live or available for **Deployment**); and **Retired Services**. See also **Service Portfolio Management**.

Service Portfolio Management (SPM)

(Service Strategy) The **Process** responsible for managing the **Service Portfolio**. Service Portfolio Management considers **Services** in terms of the **Business** value that they provide.

Service Provider

(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**.

Service Reporting

(Continual Service Improvement) The **Process** responsible for producing and delivering reports of achievement and trends against **Service Levels**. Service Reporting should agree the format, content and frequency of reports with **Customers**.

Service Request

(Service Operation) A request from a **User** for information or advice, or for a **Standard Change** or for **Access** to an **IT Service**. For example to reset a password, or to provide standard **IT Services** for a new **User**. Service Requests are usually handled by a **Service Desk**, and do not require an **RFC** to be submitted. See also **Request Fulfilment**.

Service Strategy

(Service Strategy) The title of one of the Core **ITIL** publications. Service Strategy establishes an overall **Strategy** for **IT Services** and for **IT Service Management**.

Service Transition

(Service Transition) A stage in the **Lifecycle** of an **IT Service**. Service Transition includes a number of **Processes** and **Functions** and is the title of one of the Core **ITIL** publications. See also **Transition**.

Service Warranty

(Service Strategy) Assurance that an **IT Service** will meet agreed **Requirements**. This may be a formal **Agreement** such as a **Service Level Agreement** or **Contract**, or may be a marketing message or brand image. The **Business** value of an **IT Service** is created by the combination of **Service Utility** (what the **Service** does) and **Service Warranty** (how well it does it). See also **Warranty**.

Serviceability

(Service Design) (Continual Service Improvement) The ability of a **Third-Party Supplier** to meet the terms of its **Contract**. This **Contract** will include agreed levels of **Reliability**, **Maintainability** or **Availability** for a **Configuration Item**.

Shift

(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

(Service Design) (Continual Service Improvement) A technique that creates a detailed model to predict the behaviour of a **Configuration Item** or **IT Service**. Simulation Models can be very accurate but are expensive and time consuming to create. 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**.

Single Point of Failure (SPOF)

(Service Design) Any **Configuration Item** that can cause an **Incident** when it fails, and for which a **Countermeasure** has not been implemented. A SPOF may be a person, or a step in a **Process** or **Activity**, as well as a **Component** of the **IT Infrastructure**. See also **Failure**.

SMART

(Service Design) (Continual Service Improvement) An acronym for helping to remember that targets in **Service Level Agreements** and **Project Plans** should be **Specific**, **Measurable**, **Achievable**, **Relevant** and **Timely**.

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

All people who have an interest in an **Organization**, **Project**, **IT Service**, etc. Stakeholders may be interested in the **Activities**, targets, **Resources**, or **Deliverables**. Stakeholders may include **Customers**, **Partners**, employees, shareholders, owners, etc. See 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 **Standard** 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**.

Standby

(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)

(Service Design) A **Document** containing all **Requirements** for a product purchase, or a new or changed **IT Service**. See also **Terms of Reference**.

Status

The name of a required field in many types of **Record**. It shows the current stage in the **Lifecycle** of the associated Configuration Item, Incident, Problem, etc.

Strategic

(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**.

Strategy

(Service Strategy) A **Strategic Plan** designed to achieve defined **Objectives**.

Supplier

(Service Strategy) (Service Design) 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 **Underpinning Contract**, **Supply Chain**.

Supplier and Contract Database (SCD)

(Service Design) A database or structured **Document** used to manage **Supplier Contracts** throughout their **Lifecycle**. The SCD contains key **Attributes** of all **Contracts** with **Suppliers**, and should be part of the **Service Knowledge Management System**.

Supplier Management

(Service Design) The **Process** responsible for ensuring that all **Contracts** with **Suppliers** support the needs of the **Business**, and that all **Suppliers** meet their contractual commitments.

Supply Chain

(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

(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

(Service Design) (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

(Service Strategy) A **Service** that enables or enhances a **Core Service**. For example, a **Directory Service** or a **Backup Service**.

SWOT Analysis

(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 multiple **Processes** that are planned and managed together. For example, a **Quality Management System**
- A Database Management System or Operating System that includes many software modules that are designed to perform a set of related **Functions**.

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

(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 Service

See **Infrastructure Service**.

Technical Support

See **Technical Management**.

Terms of Reference (TOR)

(Service Design) A **Document** specifying the **Requirements**, **Scope**, **Deliverables**, **Resources** and schedule for a **Project** or **Activity**.

Test

(Service Transition) An **Activity** that verifies that a **Configuration Item**, **IT Service**, **Process**, etc. meets its **Specification** or agreed **Requirements**. See also **Acceptance**.

Third Party

A person, group, or **Business** that is not part of the **Service Level Agreement** for an **IT Service**, but is required to ensure successful delivery of that **IT Service**. For example, a software **Supplier**, a hardware maintenance company, or a facilities department. **Requirements** for Third Parties are typically specified in **Underpinning Contracts** or **Operational Level Agreements**.

Third-line Support

(Service Operation) The third level in a hierarchy of **Support Groups** involved in the resolution of **Incidents** and investigation of **Problems**. Each level contains more specialist skills, or has more time or other resources.

Threat

Anything that might exploit a **Vulnerability**. Any potential cause of an **Incident** can be considered to be a Threat. For example a fire is a Threat that could exploit the **Vulnerability** of flammable floor coverings. This term is commonly used in **Information Security Management** and **IT Service Continuity Management**, but also applies to other areas such as **Problem** and **Availability Management**.

Threshold

The value of a **Metric** 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

(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)

(Service Strategy) A methodology used to help make investment decisions. TCO assesses the full **Lifecycle Cost** of owning a **Configuration Item**, not just the initial **Cost** or purchase price.

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 complete successfully or none of them is carried out.

Transition

(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.

Trend Analysis

(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 part of **Performance Management**, which also includes **Performance monitoring** and implementation of the required **Changes**.

Underpinning Contract (UC)

(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 an **SLA**.

Urgency

(Service Transition) (Service Design) 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

(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

(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.

Utility

(Service Strategy) Functionality offered by a **Product** or **Service** to meet a particular need. Utility is often summarized as 'what it does'.

Validation

(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 **Verification, Acceptance**.

Value Chain

(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

(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 **Value Chain, Partnership**.

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

(Service Transition) An **Activity** that ensures a new or changed **IT Service**, **Process**, **Plan**, or other **Deliverable** is complete, accurate, **Reliable** and matches its design specification. See also **Validation, Acceptance**.

Version

(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**.

Vital Business Function (VBF)

(Service Design) A **Function** 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

(Service Strategy) A promise or guarantee that a product or **Service** will meet its agreed **Requirements**. See also **Service Warranty**.

Work Instruction

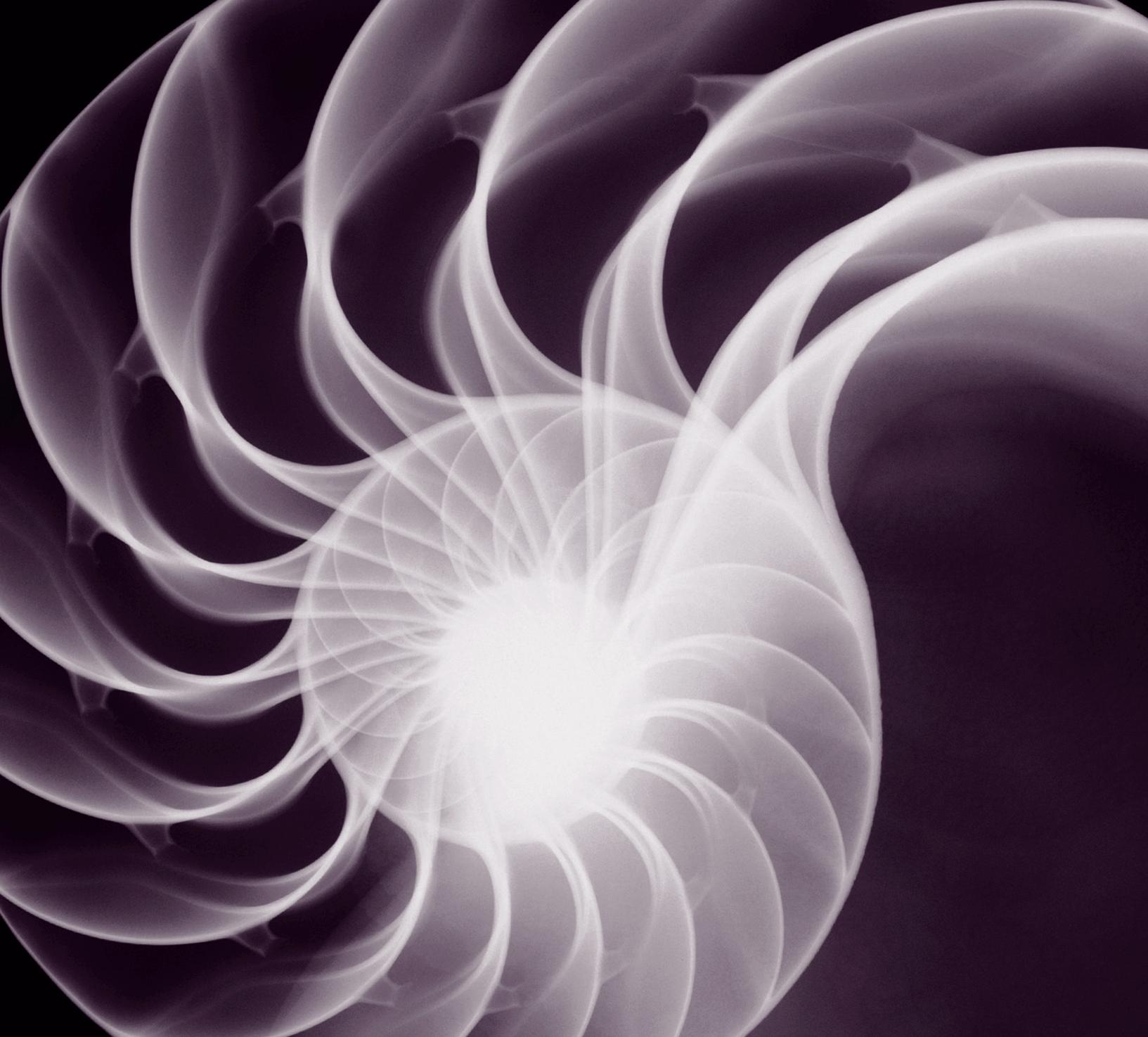
A **Document** containing detailed instructions that specify exactly what steps to follow to carry out an **Activity**. A Work Instruction contains much more detail than a **Procedure** and is only created if very detailed instructions are needed.

Workaround

(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 **Workload** is sometimes used as a synonym for **Throughput**.



Index

Index

- 80/20 rule 204
- 24 x 7 IT services 120
- acceptance, definition 289
- Accommodation and Services Plan 136
- accounting, definition 289
- acronyms list 287–288
- activity, definition 289
- activity sampling, requirement investigation 171
- agreed service time, definition 289
- agreement, definition 289
- alert, definition 289
- alignment, new services 31 (Fig)
- AMS *see* IBM Application Management Specification
- analysis of data 89
 - Availability Management 105
 - unavailability 105–106
 - Component Failure Impact Analysis 115–117
 - Fault Tree Analysis 117–118
 - Service Failure Analysis 110
 - Single Point of Failure 117
 - trends 92
- analytical modelling 92
 - definition 289
- analytical skills 190
- APIs *see* Application Program Interfaces
- application, definition 289
- application architecture 38, 39 *see also* Rapid Application Development
 - frameworks 181–182
- Application Management 180
 - coding conventions 184
 - definition 289
 - design processes 182–183
 - development phase 183–184
 - diagnostic hooks 185
 - frameworks 181–182
 - instrumentation 184
 - outputs 185
- Application Portfolio 180–181, 181 (Tab)
 - definition 289
- Application Program Interfaces 184
- Application Response Measurement 184
- Application Service Provider, definition 289
- Application Service Provision 51 (Tab), 52 (Tab)
- application sizing 93
 - definition 289
- applications 3 *see also* Application Management; IT assets
 - architectural design 182
 - definition 180
- functional business requirements 24
- management and control 28
- Service Design tools 202
- architectural design 38
 - applications 182
 - benefits of 39
 - definitions 35, 36, 37
 - documents 241
 - Enterprise Architecture 36 (Fig), 37 (Tab)
 - integration of requirements 36, 38, 38 (Fig)
 - management architectures 40–42
 - roles involved 39
 - technology architectures 39–40, 41 (Fig)
- architecture
 - clarity of 29
 - definitions 35, 289
 - design of 35–42
 - flexibility of 27
- ARMS *see* Application Response Measurement
- articulation skills 190
- aspects, of Service Design 14–18, 26, 30–31, 59
- assessment, definition 289
- asset, definition 289
- asset disposal policy 142
- Asset Management, definition 289–290
- assets, accountability for 143
- ATMs 40
- attribute, definition 290
- audit
 - culture of organization 211–212, 212 (Fig)
 - definition 290
 - Service Design processes 212–213, 212 (Fig)
- auto-discovery tools 201
- automatic call distribution, definition 290
- availability
 - definition 290
 - meaning 100, 101 (Fig), 104–105
- Availability Management 19, 99 (Fig)
 - activities 98–103
 - proactive 99 (Fig), 100, 111–121
 - reactive 99, 99 (Fig), 100, 103–111
 - challenges 125
 - critical success factors 125
 - definition 290
 - documentation 114, 115, 121
 - goal 97
 - information management 124–125
 - Information Security Management 147
 - IT Service Continuity Management 139

- Key Performance Indicators 123–124
 - monitoring 100–102, 101 (Fig), 102–103
 - measurement 103–104, 108
 - objectives 97–98
 - outputs 108, 123
 - principles of 100
 - purpose 97
 - reporting processes 105
 - review procedures 121–122
 - risks 98, 125
 - reduction of 132–133
 - triggers and information 122–123
- Availability Management Information System 35
 - definition 290
- Availability Manager 194–195
- Availability Plan 124–125
 - definition 290
- availability testing schedule 120
- back-out, definition 290
- backup, definition 290
- balance
 - architectural design 36
 - Capacity Management 81
 - design processes 25–27, 26 (Fig)
 - risk recovery 131–133
- Balanced Scorecards 46, 213
 - contracts 154
 - definition 290
- baseline, definition 290
- baselining, for modelling 92
- benchmark, definition 290
- benchmarking 92, 161
 - definition 290
- best practice, definition 290
- Boolean logic 117–118
- bottom up management 41
- BPO see Business Process Outsourcing
- brainstorming, definition 291
- budget, definition 291
- budgeting
 - definition 291
 - processes 29
- build, definition 291
- business
 - case, definition 291
 - customer, definition 291
 - data 96
 - definition 291
 - drivers 28–29
 - management 41
- call, definition 292
- Call Centre, definition 292
- capabilities 3 (Fig), 6
- objective, definition 291
- operations, definition 291
- perspective, definition 291
- process, definition 291
- requirements (*see* business requirements)
- success 3
- support 148, 149
- Business Architect 39
- Business Capacity Management 82, 83 (Fig), 84–85, 84 (Fig)
 - definition 291
- Business Continuity Management 97, 98, 136
 - definition 291
- Business Continuity Plans 30, 127 (Fig), 135–136
 - definition 291
 - invocation 138
- Business Continuity Strategy 127
- business critical processes 102
- Business Impact Analysis 23, 126, 128–130, 129 (Fig)
 - definition 291
 - implementation process 209
 - suppliers 158
- Business Process Outsourcing 51 (Tab), 52 (Tab)
- Business Relationship Management
 - definition 292
- business requirements 3, 15–16, 59 (Fig), 219, x
 - 80/20 rule 204
 - application management 180
 - availability 104, 112–113, 114, 122
 - Capacity Management 94–95
 - change processes 23 (Fig) , 24
 - documentation of 28–29
 - implementation processes 210–211, 211 (Fig)
 - Information Security Management 141
 - initial design actions 23
 - management architectures 41, 42
 - packaged services 48
 - review 17, 18
 - roles and responsibilities 190
 - Service Catalogue Management 64
 - vision 211–213
- Business Security Policy 141
- Business Service, definition 292
- Business Service Catalogue 62–63, 62 (Fig), 63 (Fig)
- Business Service Management 49–50, 49 (Fig)
 - definition 292
 - tools 201
- business unit, definition 292

- business maturity 32
- definition 292
- IT maturity 32–33
- metrics 44
- Service Management 11
- Capability Maturity Model Integration 183
- capacity, definition 292
- Capacity Management 19
 - activities 79–81, 84, 86–87
 - application sizing 93
 - Business Capacity Management 82, 83 (Fig), 84–85, 84 (Fig)
 - Business Continuity Management 97
 - challenges 97
 - Component Capacity Management 83, 86
 - Critical Success Factors 97
 - definition 292
 - demand management 91–92
 - demand pattern 84, 85 (Fig)
 - information inputs 93–94
 - Information Security Management 147
 - initial service design processes 23
 - IT Service Continuity Management 139
 - iterative processes 87–91, 87 (Fig)
 - Key Performance Indicators 94–95
 - modelling 92
 - monitoring 87–89
 - implementation 90
 - new technology 90
 - objectives 79, 84, 90, 92
 - outputs 94
 - principles of 81–82, 82 (Fig)
 - processes 82–84, 83 (Fig)
 - reporting 94, 95, 96–97
 - resilience, infrastructure 90
 - risks 97
 - Service Capacity Management 82–83, 83 (Fig), 86
 - threshold management 90–91
 - triggers 93
 - tuning techniques 89–90
- Capacity Management Information System 35, 87, 94, 96–97
 - definition 292
- Capacity Manager 195–196
- Capacity Plan 23, 81–82, 94
 - definition 292
 - example 273–274
- capacity planning, definition 292
- CARE (Computer Aided Requirements Engineering) 175
- CASE (Computer Aided Software Engineering) 175, 182
- category, definition 292
- certification, definition 292
- challenges, Service Design 219
- change, definition 292
- Change Advisory Board, definition 293
- change history, definition 293
- Change Management 137
 - business 23 (Fig)
 - Capacity Management 85
 - definition 293
 - documentation of 28–29
 - Information Security Management 147
 - IT as agent 3
 - IT Service Continuity Management 139
 - new suppliers 158
 - requirements 175
 - role of Service Design stage 23, 30
- change request, definition 293
- change schedule, definition 293
- change window, definition 293
- charging, definition 293
- CIM see Common Information Model
- classification
 - definition 293
 - of information 143, 144
- client
 - definition 293
 - systems 40
- closed, definition 293
- closed-loop systems 12
- closure, definition 293
- co-sourcing 51 (Tab), 52 (Tab)
- COBIT 211
 - definition 293
- cold standby 133
 - definition 293
- commercial justification 30
- commercial off-the-shelf
 - definition 293
 - solutions 55–56
- committees, IT services 17
- commodity categorization, suppliers 156
- Common Information Model 184
- Communication Plan 136
- communications
 - co-ordination, recovery 136
 - design processes 27, 32, 219
 - Information Security Management 144
 - Management of Risk 131
 - Service Failure Analysis 110
 - skills 190
 - suppliers 149, 153, 159
- complaints, response to 75
- compliance
 - definition 293
 - metrics 44

- component
 - availability 100
 - definition 293
- component-based reports 95
- Component Capacity Management 83, 86
 - definition 293
- Component CI, definition 293
- Component Failure Impact Analysis 115–117, 116 (Fig)
 - definition 293
- composition, services 24 (Fig)
- concurrency, definition 293
- confidentiality, definition 294
- configuration, definition 294
 - configuration baseline, definition 294
 - configuration control, definition 294
 - configuration fulfillment 204
 - configuration identification, definition 294
- Configuration Item, definition 294
- Configuration Management 137
 - definition 294
 - Information Security Management 147
 - IT Service Continuity Management 139
 - tools 201
- Configuration Management System 15, 202
 - definition 294
 - design of 35
 - Service Portfolio 33 (Fig)
- constraints
 - on design 47–48, 47 (Fig), 48 (Fig)
 - financial 92
 - management and operational 168
 - Rapid Application Development 54
- Continual Service Improvement 3, 7–8, 215 *see also* ITIL Framework
 - definition 294
- Continual Service Improvement System
 - definition 294
- continuity 18
- continuous availability, definition 294
- continuous operation, definition 294
- contract, definition 294
- contracts management 150, 151
 - basic contract contents 154
 - evaluation 152–157
 - formal contracts 155
 - renewal/termination 161
 - underpinning agreements 155
- control
 - definition 294
 - Information Security Management System 143
- control perspectives *see also* lifecycle approach; processes
 - definition 294–295
- converged technologies 40
- coordination 13
- corporate governance 141, 142
- corporate level SLAs 68–69, 69 (Fig)
- corrective security measures 146 *see also* security, controls
- cost benefit analysis
 - definition 295
- cost-effectiveness 4, 81, 95
 - definition 295
 - tools 203
- costs
 - availability 111 (Fig), 113, 122
 - definition 295
 - documentation processes 29
 - of failure 105–106
 - minimization of 25, 40
 - and risks 12 (Fig)
- counter-measure, definition 295
- Crisis Management, definition 295
- Crisis Management and Public Relations Plan 136
- Critical Success Factors
 - Availability Management 125
 - Capacity Management 97
 - definition 295
 - implementation processes 214–215
 - Information Security Management 148–149
 - IT Service Continuity Management 140–141
 - Service Catalogue Management 64–65
 - Service Level Management 78–79
 - Six Sigma 214
 - Supplier Management 164
- cultural maturity assessment 212 (Fig)
- culture
 - definition 295
 - organization 211–213
- customer level SLAs 68–69, 69 (Fig)
- customers 4–5
 - complaints and compliments 75
 - definition 295
 - demand management 91–92
 - engagement with 29
 - expectation management 71–72
 - feedback methods 72
 - processes 13
 - representatives of 77–78
 - response times 88–89
 - review processes 73–74
 - satisfaction 99, 100
 - Service Level Agreements 70–71
 - services for 11–12
 - meaning of 61
 - customization 156–157, 204

- Damage Assessment Plan 136
- dashboard, definition 295
- data 176–177 *see also* data management
 - architectures 39
 - monitoring 87–89
 - networks 39–40
- data design tools 201
- Data/Information Architecture 38
- data/information asset type
 - Service Design tools 202
- data management 28, 176–177
 - capture 179–180
 - classification 178
 - lifecycle approach 177–178
 - migration 179
 - ownership 179
 - quality 176–177, 178, 180
 - retrieval and usage 180
 - scope 177
 - service support 24, 177
 - standards 177, 179
 - storage 179
 - value of 176–177, 178
- deliverables
 - Availability Management 120
 - definition 295
 - design activities 30
- delivery, IT services 8 *see also* outsourcing
 - model options 50–51
 - strategies 50, 51 (Tab), 52 (Tab), 53
- demand management 84, 85 (Fig)
 - Capacity Management 91–92
 - definition 295
- dependency, definition 295
- deployment, definition 295
- description, requirement 175
- design, definition 295
- design, services and processes 3–4, 192, 223
 - activities 29–30
 - applications 182–184
 - for availability 111, 113–114
 - documents 241
 - management architecture 40–41, 41 (Fig)
 - for recovery 113
- Desktop Management Instrumentation 184
- detection
 - definition 295
 - of incident 107
- detective security measures 146 *see also* security, controls
- development
 - definition 295
 - stage 47
- development environment, definition 296
- diagnosis
 - definition 296
 - of incident 107
- diagnostic hooks 185
- differential charging, definition 296
- disaster planning 98, 126
- Distributed Management Task Force 42, 44, 184
- DMI *see* Desktop Management Instrumentation
- DMTF *see* Distributed Management Task Force
- document, definition 296
- documentation 18, 25
 - architectural design 241
 - availability 114, 121, 124
 - business requirements 28–29
 - contracts 155
 - design activities 29–30
 - Information Security Management 141
 - IT Service Continuity Plans 135
 - process framework 237
 - recovery design 115
 - requirements engineering 173–175
 - security controls 146
 - suppliers and contracts 153
- downtime 104, 106–108, 106 (Fig)
 - definition 296
 - planned 120–121
- driver, definition 296
- DSDM *see* Dynamic Systems Development Method
- duration, measurement of 103
- Dynamic Systems Development Method 54, 171
- e-mail policy 142
- economies of scale, definition 296
- education, service continuity 137 *see also* training effectiveness
 - definition 296
 - design processes 16
 - metrics 44
- efficiency
 - definition 296
 - metrics 44
- Emergency Response Plan 136
- Enterprise Architecture 26, 36 (Fig)
 - aspects of 38
 - definition 37
 - frameworks 37 (Tab)
 - roles involved 39
- environment, definition 296
- Environmental Architecture 38, 245–248
- environmental aspects

- Capacity Management 79
 - for infrastructure 24, 28
- environmental asset type
 - Service Design tools 202
- environmental design tools 201
- EPOS 40
- error, definition 296
- escalation, definition 296
- eSourcing Capability Model for Service Providers
 - definition 296
- estimation, definition 296
- evaluation
 - definition 296
 - Information Security Management System 144
 - Service Management tools 204–205, 205 (Fig)
 - suppliers and contracts 152–155
- event, definition 296
- Event Management, definition 297
- exception report 95
 - definition 297
- executive management 136, 142
- expanded incident lifecycle 106–108, 106 (Fig)
 - definition 297
- explicit knowledge 173 (Tab)
- external influences 47–48, 48 (Fig)
- External Service Provider, definition 297
- external sourcing, definition 297
- Extreme Programming 54

- Facilities Management, definition 297
- failure *see also* recovery, from incident
 - definition 297
 - IT projects 171–172
- fast recovery 134 *see also* recovery, from incident
 - definition 297
- fault, definition 297
- fault tolerance, definition 297
- Fault Tree Analysis 117–118, 117 (Fig)
 - definition 297
- Finance and Administration Plan 136
- financial
 - constraints 92
 - data 96–97
- financial management
 - definition 297
 - Information Security Management 147
 - initial design stages 23
 - supplier relationships 160–161
- fit for purpose, definition 297
- forecast reporting 94, 95
- formal contracts 155

- Four Ps 16 (Fig), 40, 142–143
- frameworks
 - application management 181–182
 - Enterprise Architecture 37 (Tab)
 - security policies 142, 143 (Fig)
- frequency of failure 103
- fulfillment, definition 297
- full tests 137 *see also* testing requirements
- functional requirements 4, 167–168
- functionality 25–26, 26 (Fig)
- functions 12, 13
 - definition 297

- goals
 - Availability Management 97
 - Capacity Management 79
 - Information Security Management 141
 - IT Service Continuity Management 125
 - Service Catalogue Management 60
 - Service Design 25
 - Service Level Management 65
 - Supplier Management 149
- governance, definition 297
- GPS systems 40
- gradual recovery 133 *see also* recovery, from incident
 - definition 298
- graphical representation tools 201
- guideline, definition 298

- hardware design tools 201
- high availability
 - definition 298
 - design 112
- holistic approach 14, 26
- hot standby 134
 - definition 298
- human resources 79 *see also* people
 - IT Service Continuity Management 128

- IBM Application Management Specification 184
- immediate recovery 134 *see also* recovery, from incident
 - definition 298
- impact
 - definition 298
 - of failure 103
- implementation 209–210
 - Information Security Management System 143
 - outcomes 213
 - Post Implementation Review 215

- prerequisites for success 214
- review processes 212–213, 212 (Fig)
- timing of 204, 210–211, 211 (Fig)
- incident**
 - definition 298
 - lifecycle 106–108, 106 (Fig)
 - record, definition 298
- Incident and Problem Management** 139, 146–147
- Incident Management**, definition 298
- incremental approach, development 53–54
- indirect cost, definition 298
- information, meaning 141
- information management 3 *see also* data management; IT assets
 - architectures 39
 - Availability Management 124–125
 - Capacity Management 93–94
 - collection of 28–29
 - Service Catalogue Management 64
 - Service Level Management 75
- information processes *see also* data management
- information resource management *see also* data management
- Information Security Management** 19 *see also* Security Manager
 - activities 144–146, 145 (Fig)
 - challenges 148
 - Critical Success Factors 148–149
 - definition 298
 - goal 141
 - information inputs 147, 148
 - IT Service Continuity Management 139
 - Key Performance Indicators 148
 - objectives 141
 - outputs 147
 - policies 142–144, 143 (Fig)
 - risks 149
 - scope 141–142
 - triggers 146
- Information Security Management System 142–143, 143 (Fig), 147
- definition 298
- Information Security Policy** 141, 142, 143, 146–147
 - definition 298
- information technology *see also* IT
 - definition 298
- infrastructure 3, 24 *see also* IT assets
 - nature of 28
- Infrastructure Service, definition 298
- initial design processes 23–25
- insourcing 51 (Tab), 52 (Tab)
 - definition 298
- integration, IT assets 3
- integrity, definition 298
- intermediate recovery 133–134 *see also* recovery, from incident
 - definition 299
- Internal Service Provider**, definition 299
- internal sourcing, definition 299
- International Organization for Standardization**
 - definition 299
- internet policy 142
- interviews, requirement investigation 168–169
- Invitation to Tender** 30, 46
 - example 269
- invocation 138 *see also* testing requirements
- ISO 9000 299
- ISO 9001 299
- ISO/IEC 27001 128, 143–144, 147
 - definition 299
- ISO/IEC 20000 6, 211
 - definition 299
- IT** 4
- IT assets** *see also* data management; information management
 - application frameworks 184
 - interfaces and dependencies 203
 - misuse of 142
 - Service Design tools 202–203
 - types of 3
- IT Designer/Architect** 192–193
- IT infrastructure**, definition 299
- IT Infrastructure Architect** 39
- IT Infrastructure Architecture** 38
- IT infrastructure asset type**
 - Service Design tools 202
- IT operations**, definition 299
- IT Planner** 191–192
- IT Plans** 241–242
- IT Service**, definition 299
- IT Service Continuity Management** 19, 98, 100, 127 (Fig)
 - challenges 140
 - Critical Success Factors 140–141
 - definition 299
 - goal 125
 - information 139, 140
 - Implementation 135–137
 - initiation 128
 - ongoing operations 137–138
 - strategy 128–135
 - objectives 126
 - outputs 139
 - purpose 125–126
 - recovery plan, example 277–280
 - risks 126, 131–133, 132 (Tab)
 - scope 126–127

- triggers 138–139
- IT Service Continuity Manager 195
- IT Service Continuity Plans 135–136
 - definition 299
 - invocation 138
- IT Service Continuity Strategy 131
- IT Service Management, definition 299
- IT Service Provider, definition 299
- IT Steering Group, definition 299
- IT Strategy/Steering Group 17–18, 17 (Fig)
- iterative
 - development 53
 - and incremental approaches 4, 53–54
- ITIL, definition 300
- ITIL Core 6 (Fig)
- ITIL Framework 6–8
- ITT *see* Invitation to Tender

- Java Management Extension 184
- JMX *see* Java Management Extension
- job description, definition 300
- job scheduling, definition 300
- justification, requirements 175

- Key Performance Indicators
 - Availability Management 123–124
 - Capacity Management 94–95
 - contracts 154
 - definition 300
 - implementation processes 214–215
 - Information Security Management 147–148
 - IT Service Continuity Management 139–140
 - KPI tree 45
 - Service Catalogue Management 64
 - Service Level Management 76–77
 - Supplier Management 163
- knowledge 5–6
 - business objectives 5 (Fig)
 - proprietary 5
 - public frameworks 5
- knowledge base, definition 300
- Knowledge Management, definition 300
- Knowledge Process Outsourcing 51 (Tab), 52 (Tab)
- known error, definition 300
- KPI tree 45
- KPO *see* Knowledge Process Outsourcing
- legislation 27, 30, 147
 - contracts and agreements 154
 - supplier management 150
 - termination of contracts 161
- lifecycle, definition 300
- lifecycle approach 13, 53, 59 (Fig), 60
 - balances, design processes 26
 - data management 177–178
 - expanded incident lifecycle 106–108, 106 (Fig)
 - implementation 31 (Fig), 32
 - IT assets 202
 - IT Service Continuity Management 127–135, 127 (Fig)
 - services 3
- line of service, definition 300
- live, definition 300
- live environment, definition 300
- mainframe architectures 39
- maintainability 101, 102
 - definition 300
- maintenance
 - for availability 120–121
 - Information Security Management System 144
- major incident, definition 300
- managed services, definition 300
- management, design activities 27, 30
- management and operational requirements 167, 168
- management architectures 40–42, 41 (Fig)
 - key elements 42
- Management Information 154
 - definition 300
- Management of Risk 119, 130–131, 130 (Fig)
 - definition 301
- management skills 190
- Management System, definition 301
- manual work-arounds 133 *see also* recovery, from incident
 - definition 301
- maturity, definition 301
- Mean Time Between Failures 100–101
 - definition 301
- Mean Time Between Service Incidents 100–101
 - definition 301
- Mean Time To Repair 101
 - definition 301
- Mean Time to Restore Service 101
 - definition 301
- measurable processes 13, 18
- measurement
 - Availability Management 103–104
 - improvement analysis 213–214
- measurement systems 15, 25
 - design of 44–46
- meeting skills 190

- mergers and acquisitions 50–51
- metadata 176
- metrics 44–46
 - definition 301
 - metrics tree 45 (Fig)
 - Service Level Management 76–77
 - tools 201
- Microsoft Windows © Management Instrumentation 184
- middleware, definition 301
- migration, of data 179
- mirroring 134
- model, definition 301
- modelling 50, 92
 - analytical 92
 - Availability Management 118
 - baselining 92
 - definition 301
 - delivery 50–52
 - design and development 52–56
 - RACI model 189, 189 (Tab)
 - review processes 50
 - simulation 92
 - trend analysis 92
 - use case 167–168
- monitoring
 - definition 301
 - response times 88–89
 - utilization 87–88
- MoSCoW analysis 203
- multi-sourcing 51 (Tab), 52 (Tab), 153

- NAS *see* Network Attached Storage
- negotiation skills 190
- Network Attached Storage 40
- new technology, exploitation 90, 95
- norms 44

- OASIS (Organization for the Advancement of Structured Information Standards) 48
- Object Management Architecture 183
- object-oriented development 53
- objectives
 - Availability Management 97–98
 - Capacity Management 79, 84, 90, 92
 - definition 301
 - Information Security Management 141
 - IT Service Continuity Management 126
 - of process 42–44
 - Service Catalogue Management 61
 - Service Design 25

- Service Failure Analysis 108
- Service Level Management 65
- Supplier Management 149–150
- observation, requirement investigation 170
- off-shore
 - arrangements 50
 - definition 301
- off-site storage 133
- off-the-shelf
 - definition 301
 - solutions (*see* Commercial Off-The-Shelf, solutions)
- Office of Government Commerce 301
- OMA *see* Object Management Architecture
- on-shore, definition 301
- operate, definition 302
- operation, definition 302
- operational, definition 302
- operational capability 25
- operational categorization, suppliers 156
- operational cost, definition 302
- operational data 178
- Operational Level Agreements 24, 66 *see also* Service Level Manager
 - definition 302
 - requirements of new services 28
 - review processes 72–73, 155
 - sample 251, 254–255
- optimize, definition 302
- Organizational Architect 39
- organizational readiness assessment 32–33
- organizations 4–5
 - benchmarking 5
 - definition 302
 - recovery planning 136
- origins, Service Management 11
- out-of-the-box fulfillment 204
- outcome, definition 302
- outputs, processes 43
 - application management 185
 - Availability Management 108, 123
 - Capacity Management 94
 - Information Security Management 147
 - IT Service Continuity Management 139
 - Service Catalogue Management 64
 - Service Level Management 75–76
 - Supplier Management 163
- outsourcing 5, 17
 - definition 302
 - delivery models 50, 51 (Tab), 52 (Tab), 53
 - IT Service Continuity Management 127–128
 - prime suppliers 157
 - requirements engineering 175–176

- risk reduction 133
- service improvement 76
- overhead, definition 302
- ownership, costs and risks 12 (Fig) *see also* Total Cost of Ownership
- partial tests 137 *see also* testing requirements
- partners 16
 - delivery strategies 51 (Tab), 52 (Tab)
 - multiple service providers 28
 - supplier relationships 153
- partnership, definition 302
- passive monitoring, definition 302
- Pattern of Business Activity
 - definition 302
- PDCA model *see* Plan–Do–Check–Act model
- people 3, 201, 202–203 *see also* Four Ps; IT assets
 - business drivers 28–29
 - Capacity Management 79
 - data management 177
 - management of 41
 - recovery processes 136, 137
 - staff awareness 64, 130, 140
 - stakeholders 29
- per cent available 103
- per cent unavailable 103
- performance, definition 302
- Performance Management, definition 302
- performance measurement 27
 - security governance 144
 - suppliers and contracts 159–162
- Personnel Plan 136
- pilot, definition 302
- plan
 - aspects of Service Design 30–31
 - definition 302
 - Information Security Management System 143
- Plan–Do–Check–Act model 8, 43, 144
 - definition 303
- planned downtime, definition 303
- planning, definition 303
- PMBOK, definition 303
- PMF *see* process maturity framework
- policies, IT 18, 128
- policy, definition 303
- portable facility, definition 303
- Post-Implementation Review 215
 - definition 303
- practice, definition 303
- predictive reports 95
- prerequisites for success 214
 - definition 303
- preventative security measures 146 *see also* security, controls
- pricing, definition 303
- PRINCE2, definition 303
- prioritization 174–175
- priority, definition 303
- privacy 145
- proactive activities
 - Availability Management 99, 111–121
 - Capacity Management 84
- problem, definition 303
- Problem Management, definition 303
- procedure, definition 303
- process
 - definition 303
 - enablers 43 (Fig)
- process control 43 (Fig)
 - definitions 42, 303
- process design tools 201
- process documentation framework 237
- process maturity framework 212 (Fig), 263–266
- process owner 190–191
 - definition 304
- processes 12, 13 (Fig), 59–60, 59 (Fig), 60 (Fig)
 - characteristics 13
 - management of 41
 - new services 15
 - theory and practice 42–44, 43 (Fig)
- procurement 23, 46
 - Availability Management 111–112
- Product Architecture 38
- professional practice
 - Service Management 11
- proforma, definition 304
- programme, definition 304
- progress, metrics 44
- project
 - authorization and review 17
 - definition 304
 - governance 29
 - team, new services 31 (Fig)
- project management 31–32, 31 (Fig)
 - development stage 47
 - implementation processes 210
 - IT Service Continuity Management 128
- Projected Service Outage document 121
- proprietary knowledge 5
- protocol analysis, requirement investigation 170
- prototyping, requirement investigation 171
- public frameworks and standards 5
- purpose
 - Availability Management 97
 - Capacity Management 79

- IT Service Continuity Management 125–126
- Service Catalogue Management 60
- Service Level Management 65

- quality 93
 - data 176–177, 178, 180
 - definition 304
 - management systems 18
- Quality Management System
 - definition 304
- questionnaires, requirement investigation 171

- RACI model 189, 189 (Tab)
 - definition 304
- Rapid Application Development 53–54, 55 (Tab)
- rate of change 29
- re-use, data 177
- reactive activities 4
 - Availability Management 99, 103–111
 - Capacity Management 84
- reciprocal arrangements 133 *see also recovery, from incident*
 - definition 304
- record, definition 304
- recovery, definition 304
 - recovery, from incident 107, 113–115
 - Business Impact Analysis 128–130
 - Component Failure Impact Analysis 116–117
 - IT Service Continuity Management 133–137, 134 (Fig)
 - recovery option, definition 304
 - recovery plan, example 277–280
 - reductive security measures 146 *see also security, controls*
 - redundancy
 - availability 112–115
 - definition 304
 - relationship, definition 304
 - relationship process, definition 304
 - relationships
 - architectural 38 (Fig)
 - design components 25
 - service aspects 27–28, 27 (Fig)
 - suppliers 149, 150–151, 150 (Fig), 157, 160–161
 - release, definition 304
 - Release and Deployment Management
 - definition 304
 - Release Management, definition 305
 - release record, definition 305
 - reliability 100–101, 101 (Fig), 102
 - definition 305
 - remote access policy 142
 - repair
 - definition 305
 - of incident 107
 - reporting processes
 - Availability Management 105, 110–111
 - Capacity Management 94, 95, 96–97
 - Service Failure Analysis 110
 - Service Level Management 73
 - repressive security measures 146 *see also security, controls*
 - Request for Change, definition 305
 - request fulfillment, definition 305
 - requirement, definition 305
 - Requirements Catalogue 174–175
 - requirements engineering 167–168
 - documentation 173–175
 - Catalogue 174–175, 174 (Tab)
 - full documents 175
 - identification of 27–28, 173–174
 - investigation techniques 168
 - interviews 168–169
 - other methods 170–171
 - workshops 169–170, 170 (Fig)
 - outsourcing 175–176
 - problems with 171–172, 173 (Tab)
 - support tools 175
 - resilience
 - definition 305
 - IT infrastructure 25, 90, 100
 - resolution, definition 305
 - resources 3 (Fig), 25–26, 26 (Fig)
 - definition 305
 - security governance 144
 - response times 88–89
 - definition 305
 - monitoring 88–89
 - responsiveness, definition 305
 - restoration, from incident 107
 - restore, definition 305
 - retire
 - definition 305
 - stages 3
 - Return on Investment 32
 - definition 305
 - return to normal, definition 305
 - review, definition 305
 - rights, definition 306
 - Risk Analysis 16, 25
 - Availability Management 118–119, 119 (Fig)
 - design activities 29, 30, 31
 - initial design processes 23
 - IT Service Continuity Management 126, 130–131, 131 (Fig)
 - supplier agreements 154

- Risk Analysis and Management 118–119, 119 (Fig)
 - definitions 119
- risk assessment, definition 306
- risk management
 - definition 306
 - security governance 144
- risk profile 131 (Fig)
- risk reduction 131–133
- risks 132 (Tab), 219–220
 - Availability Management 125
 - Capacity Management 97
 - definition 306
 - implementation processes 209–210
 - Information Security Management 149
 - IT Service Continuity Management 126
 - partnering 153
 - Service Catalogue Management 65
 - Service Level Management 78
 - Supplier Management 158, 164
- ROI *see* Return on Investment
- role, definition 306
- role, Service Design stage
 - definition 23
- roles and responsibilities 189
 - analysis 189–190
 - Availability Manager 194–195
 - Capacity Manager 195–196
 - IT Designer/Architect 192–193
 - IT Planner 191–192
 - IT Service Continuity Manager 195
 - Process owner 190–191
 - Security Manager 196
 - Service Catalogue Manager 194
 - Service Design Manager 191
 - Service Level Manager 74, 194
 - skills and attributes 190
 - Supplier Manager 151, 197
- root cause, definition 306
- running costs, definition 306

- SAC *see* Service Acceptance Criteria
- Salvage Plan 136
- SANs *see* Storage Area Networks
- scalability, definition 306
- SCD *see* Supplier and Contract Database
- scenario tests 137 *see also* testing requirements
 - analysis, requirement investigation 170
- schedule 25–26, 26 (Fig)
- scope
 - Availability Management 98
 - Capacity Management 79–80

- data management 177
- definition 306
- Information Security Management 141–142
- IT Service Continuity Management 126–127, 128
- Service Catalogue Management 61
- Service Design 14–18, 14 (Fig)
- Service Level Management 65–66
- Supplier Management 150
- SDLC *see* Service Development Life Cycle
- SDP *see* Service Design Package
- security *see also* Information Security Management
 - availability requirements 114
 - breaches 146
 - controls 145–146, 145 (Fig), 147
 - definition 306
 - governance 144
 - ISO 27001 128
 - levels 27
 - policies 30
 - strategy 142, 144–145
 - technology architectures 39
- Security Management, definition 306
- Security Management Information System 35, 145 (Fig), 147, 148
- Security Manager 196
- Security Plan 136
- Security Policy, definition 306
- security risk management 141
- Separation of Concerns, definition 306
- server, definition 306
- service
 - agreements 154
 - availability 100
 - data 96
 - definition 306
 - meaning of 61–62
 - relationships 27–28, 27 (Fig)
 - solutions 31–33, 31 (Fig)
- Service Acceptance Criteria 31, 32, 233–234
 - definition 306
- Service Architect 39
- Service Architecture 38
- Service Asset, definition 306
- service-based reports 95
- Service Capacity Management 82–83, 83 (Fig), 86
 - definition 306
- Service Catalogue 34, 35, 49, 60 (Fig)
 - definition 306
 - example 259
 - nature of 61–63, 62 (Fig), 63 (Fig)
- Service Catalogue Management 19, 35
 - activities 61, 63–64
 - challenges 64

- Critical Success Factors 64–65
- goal 60
- information and triggers 64
- Key Performance Indicators 64
- objective 61
- principles of 61–63
- purpose 60
- risks 65
- Service Catalogue Manager 194
- Service Continuity Management
 - definition 306
 - service culture, definition 306
- Service Design 7 *see also* ITIL Framework
 - definitions 223, 306
 - tools management 201–203
- Service Design Manager 191
- Service Design Package 15, 31, 33, 227–229
 - definition 307
- Service Desk
 - Availability Management 115
 - definition 307
 - implementation new services 23
 - logging procedures 75
 - monitoring SLAs 70–71
 - Projected Service Availability 121
 - recovery options 134 (Fig), 135
 - security breaches 146
 - Service Level Agreements 70, 78
 - staff awareness 64
 - system 35
- Service Development Life Cycle 53, 180
- Service Failure Analysis 105–106, 108–111, 109 (Fig)
 - definition 307
- service hours, definition 307
- Service Improvement Plan 66
 - definition 307
 - implementation processes 210
 - review process 73–74
- Service Level Management 76
 - suppliers 160, 163
- Service Knowledge Management System 15, 202
 - definition 307
 - design of 35
 - Service Portfolio 33 (Fig)
- service level, definition 307
- Service Level Agreements 4, 15, 24, 65
 - Capacity Management 85
 - customer-based 68
 - customer satisfaction 71–72
 - definition 307
 - design aspects 31
 - IT Service Continuity Management 136
 - management of 66
 - monitoring of 70–71
 - multi-level 68–69, 69 (Fig)
 - preparation of 69
 - review processes 72–73
 - sample 251–253
 - service-based 67–68
 - use of 155
- Service Level Management 19, 42, 65 *see also* Service Level Agreements; Service Level Requirements
 - activities 65–68, 68 (Fig)
 - Availability Management 113
 - challenges 77–78
 - communication 74–75
 - Critical Success Factors 78–79
 - definition 307
 - goal 65
 - information and triggers 75–76, 77
 - Information Security Management 147
 - IT Service Continuity Management 139
 - Key Performance Indicators 76–77
 - outputs 75–76
 - principles of 66, 67 (Fig)
 - reporting 73
 - review processes 72–74
- Service Level Manager 74, 194
- Service Level Package
 - definition 307
- Service Level Requirements 23, 24, 32
 - application development 93
 - Capacity Management 85
 - definition 307
 - implementation processes 209
 - preparation of 69–70
 - service level SLAs 68–69, 69 (Fig)
- Service Level Target, definition 307
- Service Lifecycle 26, 60
 - Service Portfolio 34
 - tools 201–202
- Service Management 5 (Fig), 6, 19, 112
 - capabilities 11
 - definitions 11, 307
 - new services 15
 - objectives 3
 - tools management 203–205
 - evaluation 204–205, 205 (Fig)
 - selection 203–204
- Service Management Lifecycle, definition 307
- Service Manager, definition 307
- Service Operation 3, 7, 15 *see also* ITIL Framework
 - definition 308
- Service Oriented Architecture 48–49
 - definition 48
- Service Owner, definition 308

- service performance reporting 94
- Service Pipeline 35
- Service Portfolio 14 (Fig), 15, 18, 30
 - Application Portfolio 181
 - contents 34 (Fig), 35
 - definition 308
 - design of 33–35
 - goals of design process 25
 - lifecycle approach 60
 - new service solutions 23
 - Requirements Catalogue 174–175
 - Service Catalogue 61
 - within SKMS 33 (Fig)
- Service Portfolio Management, definition 308
- service provider, definition 308
- service reporting, definition 308
- service request, definition 308
- Service Strategy 7, 59 (Fig) *see also* ITIL Framework
 - Capacity Management 81
 - definition 308
 - design activities 30
 - Service Portfolio 35
- Service Transition 3, 7, 15 *see also* ITIL Framework
 - definition 308
 - design activities 30
 - implementation new services 23
- Service Warranty, definition 308
- serviceability 101
 - definition 308
- services 24
 - assets 3, 3 (Fig)
 - composition 24 (Fig)
 - definition 11, 12 (Fig)
 - lifecycle of 3
- shadowing, requirement investigation 170
- shared services 48–49
- shift, definition 308
- 'significant' change 14
- simulation modelling 92
 - definition 308
- Single Points of Failure 100, 112, 116
 - analysis 117
 - definition 308
 - risk reduction 133
- Six Sigma 214
- skills and attributes 190 *see also* roles and responsibilities
 - Service Design tools 202–203
- SMART
 - definition 308
 - requirements 173
- SMIS *see* Security Management Information System
- SOA *see* Service Oriented Architecture
- soft skills 40
- software
 - architecture 39
 - design tools 201
- solutions, service design processes 31–33, 31 (Fig)
 - evaluation of 46
 - external influences 47–48, 48 (Fig)
- SOR *see* Statement of Requirements
- space planning 79
- special purpose records, requirement investigation 171
- specialization 12, 13
- specific events 13
- specification, definition 309
- stakeholders 29, 172
 - definition 309
- standards 5, 18
 - data 177, 179
 - definition 309
 - design and architectural processes 241
 - development of 25
 - environmental architecture 245–248
- standby, definition 309
- Statement of Requirements 30, 46
 - definition 309
 - example 269
 - Service Management tools 203
- status, definition 309
 - storage
 - of data 179
- devices 40
- Storage Area Networks 40
- strategic
 - categorization, suppliers 156
 - data 178
 - definition 309
- strategies
 - design activities 30
 - service solutions 32
- strategy, definition 309
- structured systems development 53
- supplier, definition 309
- Supplier and Contract Database 35, 150, 151–152, 151 (Fig), 163
 - definition 309
 - value of 157
- Supplier Management 19, 150 (Fig)
 - activities 152
 - categorization 155–157
 - contracts 161
 - evaluation 152–155
 - new suppliers 158
 - performance 159–162
 - challenges 164
 - Critical Success Factors 164
 - definition 309

- goal 149
- information inputs 162, 163
- Information Security Management 147
- Key Performance Indicators 163
- objectives 149–150, 160
- outputs 163
- policies 151–152
- procurement services 23
- purpose 149
- risks 158, 164
- scope 150–151
- triggers 162
- Supplier Manager 151, 197
- suppliers 24–25
 - categorization of 155–157, 156 (Fig)
 - evaluation of 46, 152–155
 - Information Security Management 141
- supply and demand 81
- supply chain, definition 309
- support
 - group, definition 309
 - hours, definition 309
 - services 24, 70
 - teams 24
- supporting service, definition 309
- SWOT analysis 211
 - definition 309
- system
 - analysis 23
 - definition 35–36, 310
- System Management, definition 310
- systems management 112
- tacit knowledge 5, 172, 173 (Tab)
- tactical
 - categorization, suppliers 156
 - data 178
 - definition 310
- TCO see Total Cost of Ownership
- Technical Management, definition 310
- technical responsibilities 193
- technical service, definition 310
- Technical Service Catalogue 62–63, 62 (Fig), 63 (Fig)
- technical support, definition 310
- technology architectures 15, 39–40, 167
- technology management 41, 79–81 *see also Capacity Management*
- tendering processes 46
- Terms of Reference, definition 310
- test, definition 310
- testing requirements 32
 - recovery plans 136–138
- third-line support, definition 310
- third party, definition 310
- threats 132 (Tab), 145–146
 - definition 310
- threshold, definition 310
- threshold management 90–91, 97
- throughput, definition 310
- tools management 41, 201
 - Service Design 201–203
 - Service Management 203–205
- top down management 41, 42
- Total Cost of Ownership 12 (Fig), 18, 32
 - definition 310
- training
 - continuity planning 137
 - implementation of new processes 23
 - security issues 148
 - Service Management tools 204
 - SOA related 49
- transaction, definition 310
- transition, definition 310
- trend analysis 92, 203
 - definition 310
- triggers
 - Availability Management 122
 - Capacity Management 93
 - Information Security Management 146
 - IT Service Continuity Management 138–139
 - Service Catalogue Management 64
 - Service Level Management 75
 - Supplier Management 162
- tuning, definition 311
- tuning techniques
 - Capacity Management 89–90
- UAT *see User Acceptance Testing*
- unavailability analysis 105–106
- underpinning agreements 155
- underpinning contract, definition 311
- upgrading 80
- urgency, definition 311
- usability
 - definition 311
 - requirements 167, 168
- use case
 - definition 311
 - modelling 167–168
- user
 - availability issues 104–105
 - definition 311
 - requirements 168, 171–172

- User Acceptance Testing 32
utility, definition 311
utilization monitoring 87–88
 data 96
- validation, definition 311
value chain, definition 311
value for money, definition 311
value network, definition 311
value to business
 Activity Management 99
 business requirements 18, 49 (Fig)
 Capacity Management 81
 creation 3 (Fig)
 data management 176–177, 178
 demonstration of 15
 Information Security Management 142
 IT Service Continuity Management 127
 security governance 144
 Service Catalogue Management 61
 Service Level Management 66
 services 11–12
 Supplier Management 151
 suppliers 156
- variance, definition 311
verification, definition 311
version, definition 311
virus policy 142
vision
 business requirements 211–213
 definition 311
- Vital Business Function 102, 104, 111
 definition 311
- Vital Records Plan 136
voice networks 40
vulnerability, definition 311
- walk-through tests 137 *see also* testing requirements
warm standby 133–134
 definition 312
- warranty 24 (Fig)
 definition 312
- WBEM *see* Web-Based Enterprise Management
Web-Based Enterprise Management 184
WMI *see* Microsoft Windows © Management Instrumentation
work instruction, definition 312
workaround, definition 312
workload
 definition 312
 management 91, 94, 95, 154
- workshops, requirement investigation 169–170, 170 (Fig)
- XP *see* Extreme Programming