Aligning CobiT®, ITIL® and ISO 17799 for Business Benefit

A Management Briefing from ITGI and OGC

IT Governance Institute®

OGC® Office of Government Commerce

itSMF® The IT Service Management Forum

The IT Governance Institute®

The IT Governance Institute (ITGI) (*www.itgi.org*) was established in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. Effective IT governance helps ensure that IT supports business goals, optimises business investment in IT, and appropriately manages IT-related risks and opportunities. The IT Governance Institute offers original research, electronic resources and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

The Office of Government Commerce

The mission of the Office of Government Commerce (OGC) (*www.ogc.gov.uk*) is to work with the public sector as a catalyst to achieve efficiency, value for money in commercial activities and improved success in the delivery of programmes and projects. OGC supports the achievement of its targets through concentrating its efforts in a wide ranging programme supporting three significant activities in public sector organisations—improving: efficiency, programme and project management, and procurement.

Disclaimer

The IT Governance Institute and the Office of Government Commerce (the "Owners") have designed and created this publication, titled *Aligning CobiT®, ITIL® and ISO 17799 for Business Benefit* (the "Work"), primarily as an educational resource for chief information officers, senior management and IT management. The Owners make no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, the chief information officers, senior management and IT management should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

Disclosure

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.590.7491
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

Office of Government Commerce
Rosebery Court, St Andrews Business Park
Norwich, Norfolk NR7 0HS, UK
Phone: +44.845.000.4999
Fax: +44.160.370.4817
E-mail: *ServiceDesk@ogc.gsi.gov.uk*
Web site: *www.ogc.gov.uk*

Aligning CobiT, ITIL and ISO 17799 for Business Benefit
Published simultaneously on the web sites of the joint owners in England and the United States of America

Acknowledgements

The Publishers wish to recognise:

The Development Team
ITGI:
Erik Guldentops, CISA, CISM, Belgium
Gary Hardy, South Africa
Jimmy Heschl, CISA, CISM, KPMG, Austria
Robert Stroud, Computer Associates, USA

OGC:
Tony Betts, ITIL Refresh Project Manager, Head of OGC Best Practice, Office of Government Commerce,UK
Jim Clinch, ITIL Refresh Chief Editor, Office of Government Commerce, UK
David S. Hinley, OGC-SACS Consultant, David S. Hinley Associates, UK

***it*SMF:**
Gary Hodgkiss, CITP, *it*SMF US Publications Committee, Capgemini plc, UK
Sharon Taylor, Chair, Executive Publications Committee, *it*SMF International, Canada

The IT Governance Institute wishes to recognise:

Table of Contents

1. Executive Summary

This management briefing is the result of a joint study initiated by the UK government's Office of Government Commerce and the IT Governance Institute in response to the growing significance of best practices to the IT industry and the need for senior business and IT managers to better understand the value of IT best practices and how to implement them.

The growing adoption of IT best practices has been driven by a requirement for the IT industry to better manage the quality and reliability of IT in business and respond to a growing number of regulatory and contractual requirements.

There is a danger, however, that implementation of these potentially helpful best practices will be costly and unfocused if they are treated as purely technical guidance. To be most effective, best practices should be applied within the business context, focusing on where their use would provide the most benefit to the organisation. Top management, business management, auditors, compliance officers and IT managers should work together to make sure IT best practices lead to cost-effective and well-controlled IT delivery.

IT best practices are important because:

- Management of IT is critical to the success of enterprise strategy.
- They help enable effective governance of IT activities.
- A management framework is needed so everyone knows what to do (policy, internal controls and defined practices).
- They provide many benefits, including efficiency gains, less reliance on experts, fewer errors, increased trust from business partners and respect from regulators.

The briefing applies generally to all IT best practices but focuses on three specific practices and standards that are becoming widely adopted around the world:

- ITIL—Published by the UK government to provide best practices for IT service management
- COBIT—Published by ITGI and positioned as a high-level governance and control framework
- ISO/IEC 17799: 2000—Published by the International Organisation for Standardisation (ISO) and International Electrotechnical Commission (IEC) and derived from the UK government's BS 7799 to provide a framework of a standard for information security management

Descriptions of each of these can be found in the main body of the briefing.

Implementation of best practices should be consistent with the enterprise's risk management and control framework, appropriate for the organisation, and integrated with other methods and practices that are being used. Standards and best practices are not a panacea, and their effectiveness depends on how they have been actually implemented and kept up to date. They are most useful when applied as a set of principles and as a starting point for tailoring specific procedures. To avoid practices becoming 'shelfware', management and staff must understand what to do, how to do it and why it is important.

Implementation should be tailored, prioritised and planned to achieve effective use. This briefing describes some pitfalls that should be avoided.

To achieve alignment of best practice to business requirements, formal processes in support of good IT governance should be used. The OGC provides management guidance in its Successful Delivery Toolkit (*www.ogc.gov.uk/sdtoolkit/)* and ITGI provides the *IT Governance Implementation Guide.*

CobiT can be used at the highest level of IT governance, providing an overall control framework based on an IT process model that is intended by ITGI to generically suit every organisation. There is also a need for detailed, standardised practitioner processes. Specific practices and standards, such as ITIL and ISO 17799, cover specific areas and can be mapped to the CobiT framework, thus providing a hierarchy of guidance materials. To better understand how ITIL and ISO 17799 map onto CobiT, refer to the appendix, where each of the 34 IT processes and high-level control objectives has been mapped to specific sections.

ITGI and OGC plan, as part of future updates to their best practices, to further align the terminology and content of their practices with other practices to facilitate easier integration.

OGC
OGC is a UK government organisation responsible for procurement and efficiency improvements in the UK public sector. OGC has produced world-class best practice guidance, including PRINCE (project management), MSP (Managing Successful Programmes) and ITIL (IT service management). ITIL is used throughout the world and is aligned with the ISO/IEC 20000 international standard in service management.

www.ogc.gov.uk

ITGI
ITGI is a not-for-profit research organisation affiliated with the Information Systems Audit and Control Association® (ISACA®), a global not-for-profit professional membership organisation focused on IT governance, assurance and security, with more than 47,000 members in more than 140 countries. ITGI undertakes research and publishes CobiT, an open standard and framework of controls and best practice for IT governance.

www.itgi.org

***it*SMF**
The IT Service Management Forum (*it*SMF) is the only internationally recognised and independent organisation dedicated to IT service management. It is a not-for-profit organisation, wholly owned and principally operated by its membership.

*it*SMF is a major influence on, and contributor to, industry ‘best practice’ and standards worldwide, working in partnership with a wide range of governmental and standards bodies worldwide.

www.itsmf.com

2. Background

This briefing is the result of a joint study initiated by OGC and ITGI, in recognition of the growing significance of best practices to the IT industry. *it*SMF also supported the study.

The intention is to explain to business users and senior management the value of IT best practices and how harmonisation, implementation and integration of best practices may be made easier.

Business Drivers for the Use of IT Best Practices

IT best practices have become significant due to a number of factors:

- Business managers and boards demanding better returns from IT investments, i.e., that IT delivers what the business needs to enhance stakeholder value
- Concern over the generally increasing level of IT expenditure
- The need to meet regulatory requirements for IT controls in areas such as privacy and financial reporting (e.g., the US Sarbanes-Oxley Act) and in specific sectors such as finance, pharmaceutical and healthcare
- The selection of service providers and the management of service outsourcing and acquisition
- Increasingly complex IT-related risks, such as network security
- IT governance initiatives that include adoption of control frameworks and best practices to help monitor and improve critical IT activities to increase business value and reduce business risk
- The need to optimise costs by following, where possible, standardised—rather than specially developed—approaches
- The growing maturity and consequent acceptance of well-regarded frameworks, such as ITIL, CobiT, ISO 17799, ISO 9002, Capability Maturity Model (CMM®), Project in Controlled Environments (PRINCE), Managing Successful Programmes (MSP), Management of Risk (M_o_R®) and Project Management Body of Knowledge (PMBOK®)
- The need for organisations to assess how they are performing against generally accepted standards and against their peers (benchmarking)
- Statements by analysts recommending the adoption of best practices, for example:

> *Strong framework tools are essential for ensuring IT resources are aligned with an enterprise's business objectives, and that services and information meet quality, fiduciary and security needs…. CobiT and ITIL are not mutually exclusive and can be combined to provide a powerful IT governance, control and best-practice framework in IT service management. Enterprises that want to put their ITIL program into the context of a wider control and governance framework should use CobiT.*[1]

Today's Challenges

The growth in the use of standards and best practices creates new challenges and demands for implementation guidance:

- Creating awareness of the business purpose and the benefits of these practices
- Supporting decision making on which practices to use and how to integrate with internal policies and procedures
- Tailoring to suit specific organisations' requirements

[1] This Gartner research note was issued in June 2002, and is considered by many to still be very relevant.

3. Why Senior Management Needs to Know About Best Practices

Due to their technical nature, IT standards and best practices are mostly known to the experts—IT professionals, managers and advisors—who may adopt and use them with good intent but potentially without a business focus or the customer's involvement and support.

Even in organisations where practices such as COBIT and ITIL have been implemented, some business managers understand little about their real purpose and are unable to influence their use.

To realise the full value of best practices, the customers of IT services need be involved, as the effective use of IT should be a collaborative experience between the customer and internal and external service providers, with the customer setting the requirements. Other interested stakeholders, such as the board, senior executives, auditors and regulators, also have a vested interest in either receiving or providing assurance that the IT investment is properly protected and delivering value.

Figure 1 summarises who has an interest in how IT standards and best practices can help address IT management issues.

Figure 1—Stakeholders in IT Management Issues

Top Management Issues Addressed by Standards and Best Practices (Based on the COBIT Framework)	**Who Has a Primary Interest?**			
	Board/ Executive	Business Management	IT Management	Audit/ Compliance
Plan and Organise				
Are IT and the business strategy in alignment?	✔	✔	✔	
Is the enterprise achieving optimum use of its resources?	✔	✔	✔	✔
Does everyone in the organisation understand the IT objectives?	✔	✔	✔	✔
Are IT risks understood and managed?		✔	✔	✔
Is the quality of IT systems appropriate for business needs?		✔	✔	
Acquire and Implement				
Are new projects likely to deliver solutions that meet business needs?		✔	✔	
Are new projects likely to deliver on time and within budget?		✔	✔	
Will the new systems work properly when implemented?		✔	✔	
Will changes be made without upsetting the current business operation?		✔	✔	
Deliver and Support				
Are IT services being delivered in line with business requirements and priorities?		✔	✔	
Are IT costs optimised?	✔	✔	✔	
Is the workforce able to use the IT systems productively and safely?		✔	✔	
Are adequate confidentiality, integrity and availability in place?		✔	✔	✔
Monitor				
Can IT's performance be measured, and can problems be detected before it is too late?	✔	✔	✔	
Is independent assurance needed to ensure that critical areas are operating as intended?	✔			✔

4. Why Best Practices Are Important

The effective use of IT is critical to the success of enterprise strategy, as illustrated by the following quote:

> *The use of IT has the potential to be the major driver of economic wealth in the 21st century. While IT is already critical to enterprise success, provides opportunities to obtain a competitive advantage and offers a means for increasing productivity, it will do all this even more so in the future.*
>
> *IT also carries risks. It is clear that in these days of doing business on a global scale around the clock, system and network downtime has become far too costly for any enterprise to afford. In some industries, IT is a necessary competitive resource to differentiate and provide a competitive advantage, while in many others it determines survival, not just prosperity.*[2]

Best Practices and Standards Help Enable Effective Governance of IT Activities

Increasingly, the use of standards and best practices, such as ITIL, COBIT and ISO 17799, is being driven by business requirements for improved performance, value transparency and increased control over IT activities.

The UK government recognised very early on the significance of IT best practices to government and, for many years, has developed best practices to guide the use of IT in government departments. These practices have now become *de facto* standards around the world in private and public sectors. ITIL was developed more than 15 years ago to document best practice for IT service management, with that best practice being determined through the involvement of industry experts, consultants and practitioners. BS 15000, which is aligned with ITIL, was recently created as a new service management standard. The IT Security Code of Practice, developed initially with support from industry, became BS 7799 and then became ISO 17799, the first international security management standard. PRINCE, and now PRINCE2, was created by CCTA (now OCG) to provide a best practice for project management.

ISACA recognised in the early 1990s that auditors, who had their own checklists for assessing IT controls and effectiveness, were talking a different language to business managers and IT practitioners. In response to this communication gap, COBIT was created as an IT control framework for business managers, IT managers and auditors based on a generic set of IT processes meaningful to IT people and, increasingly, business managers. The best practices in COBIT are a common approach to good IT control—implemented by business and IT managers, and assessed on the same basis by auditors. Over the years, COBIT has been developed as an open standard and is now increasingly being adopted globally as the control model for implementing and demonstrating effective IT governance. In 1998, ISACA created an affiliated body, the IT Governance Institute, to better communicate IT governance-related messages to business managers and, in particular, the boardroom.

Today, as every organisation tries to deliver value from IT while managing an increasingly complex range of IT-related risks, the effective use of best practices can help to avoid re-inventing wheels, optimise the use of scarce IT resources and reduce the occurrence of major IT risks, such as:

- Project failures
- Wasted investments
- Security breaches
- System crashes
- Failures by service providers to understand and meet customer requirements

OGC is at the forefront in delivering and disseminating best practice material to address these and other current challenges.

[2] ITGI, *Board Briefing on IT Governance, 2nd Edition*, 2003

An IT Management Framework Is Needed

Organisations wishing to adopt IT best practices need an effective management framework that provides an overall consistent approach and is likely to ensure successful outcomes when using IT to support the enterprise's strategy.

The OGC Successful Delivery Toolkit is a repository of best management and IT practices, which is free for end users to use and adapt. Commercial exploitation requires a license (see *www.ogc.gov.uk/sdtoolkit/copyright/index.html*). It describes proven best practice for procurement, programmes, projects, risk management and service management. The toolkit brings together policy and best practice in a single point of reference, helping to identify the critical questions about capability and project delivery and giving practical advice on ways to improve. Additional information is available at *www.ogc.gov.uk/sdtoolkit/*.

ITGI has published the *IT Governance Implementation Guide* for using COBIT for IT governance, a rapid implementation version titled COBIT® *Quickstart*™ and COBIT® *Security Baseline*™ for implementing IT security with cross-references to ISO 17799. ITGI also provides training in how to use the COBIT materials and an online version of COBIT to help users tailor the COBIT material for use in their own environments.

However, users need more guidance on how to integrate the leading global frameworks and other practices and standards. In response to this need, ongoing research has been undertaken into the mapping of COBIT to a wide range of other practices. In 2004, ITGI initiated a harmonisation initiative as part of its planned update of the COBIT materials.

COBIT is based on established frameworks, such as the Software Engineering Institute's Capability Maturity Model, ISO 9000, ITIL and ISO 17799. However, COBIT does not include process steps and tasks because, although it is oriented toward IT processes, it is a control and management framework rather than a process framework. COBIT focuses on what an enterprise needs to do, not how it needs to do it, and the target audience is senior business management, senior IT management and auditors.

ITIL is based on defining best practice processes for IT service management and support, rather than on defining a broad-based control framework. It focuses on the method and defines a more comprehensive set of processes.

Due to its high level and broad coverage and because it is based on many existing practices, COBIT is often referred to as the 'integrator', bringing disparate practices under one umbrella and, just as important, helping to link these various IT practices to business requirements.

Now that these standards and best practices are increasingly being used in real-world situations, experiences are maturing and organisations are moving from *ad hoc* and chaotic approaches to IT, to defined and managed processes.

As IT governance—the concept and the actual practice—gains momentum and acceptance, IT best practices will increasingly be aligned to business and governance requirements rather than technical requirements. IT governance addresses these main areas of IT activity:

- Strategic alignment, with a focus on aligning with the business and collaborative solutions
- Value delivery, concentrating on optimising costs and proving the value of IT
- Risk management, addressing the safeguarding of IT assets (including project investments), disaster recovery and continuity of operations
- Resource management, optimising knowledge and IT infrastructure
- Performance measurement, tracking project delivery and monitoring IT services

A key aspect of any IT governance initiative is the need to define decision rights and accountability. Achieving this both in theory (the organisation is clearly defined) and in practice (everyone knows what to do and how) requires the right culture, policy frameworks, internal controls and defined practices.

Best Practices Provide Many Benefits

The effective adoption of best practices can provide many benefits, especially in the area of advanced technology. These include:

- Avoiding re-inventing wheels
- Reducing dependency on technology experts
- Increasing the potential to utilise less-experienced staff if properly trained
- Making it easier to leverage external assistance
- Overcoming vertical silos and nonconforming behaviour
- Reducing risks and errors
- Improving quality
- Improving the ability to manage and monitor
- Increasing standardisation leading to cost reduction
- Improving trust and confidence from management and partners
- Creating respect from regulators and other external reviewers
- Safeguarding and proving value

Adherence to best practice also helps strengthen supplier/customer relations, make contractual obligations easier to monitor and enforce, and improve the market position of those service providers seen to be compliant with accepted standards, such as BS 15000.

5. COBIT, ITIL and ISO 17799—What These Practices Provide and Address

COBIT

Business orientation is the main theme of COBIT. It is designed to be employed not only by users and auditors, but also, and more important, as comprehensive guidance for management and business process owners. Increasingly, business practice involves the full empowerment of business process owners so they have total responsibility for all aspects of the business process. In particular, this includes providing adequate controls.

The COBIT framework provides a tool for the business process owner that facilitates the discharge of this responsibility. The framework starts from a simple and pragmatic premise: To provide the information that the organisation needs to achieve its objectives, IT resources need to be managed by a set of naturally grouped processes.

The framework continues with a set of 34 high-level control objectives, one for each of the IT processes, grouped into four domains: Plan and Organise, Acquire and Implement, Deliver and Support, and Monitor. This structure covers all aspects of information and the technology that supports it. By addressing these 34 high-level control objectives, the business process owner can ensure that an adequate control system is provided for the IT environment.

IT governance guidance is also provided in the COBIT framework. IT governance provides the structure that links IT processes, IT resources and information to enterprise strategies and objectives. IT governance integrates optimal ways of planning and organising, acquiring and implementing, delivering and supporting, and monitoring and evaluating IT performance. IT governance enables the enterprise to take full advantage of its information, thereby maximising benefits, capitalising on opportunities and gaining competitive advantage.

In addition, corresponding to each of the 34 high-level control objectives is an audit guideline to enable the review of IT processes against COBIT's 318 recommended detailed control objectives to provide management assurance and/or advice for improvement.

The management guidelines further enhance and enable enterprise management to deal more effectively with the needs and requirements of IT governance. The guidelines are action-oriented and generic, and they provide management direction for getting the enterprise's information and related processes under control, monitoring achievement of organisational goals, monitoring performance within each IT process, and benchmarking organisational achievement.

Specifically, COBIT provides maturity models for control over IT processes, so management can map where the organisation is today, where it stands in relation to the best in class in its industry and to international standards, and where the organisation wants to be. Critical success factors (CSFs) define the most important management-oriented implementation guidelines to achieve control over and within its IT processes. Key goal indicators (KGIs) define measures that tell management—after the fact—whether an IT process has achieved its business requirements. Key performance indicators (KPIs) are lead indicators that define measures of how well the IT process is performing in enabling the goal to be reached.

[3] ITGI, COBIT® *Framework*, 2000, *www.itgi.org*

COBIT's management guidelines are generic and action-oriented for the purpose of answering the following types of management questions: How far should we go and is the cost justified by the benefit? What are the indicators of good performance? What are the critical success factors? What are the risks of not achieving our objectives? What do others do? How do we measure and compare?[3]

References in this publication are to COBIT 3rd Edition. Readers should note that COBIT 4.0 will be released in the fourth quarter of 2005 (*www.isaca.org/cobit*). COBIT 4.0 is an enhancement of COBIT 3rd Edition and in no way invalidates any implementation or execution activities based on COBIT 3rd Edition.

ITIL

Organisations are increasingly dependent upon IT to satisfy their corporate aims and meet their business needs. This growing dependency necessitates quality IT services at a level matched to business needs and user requirements as they emerge.

IT service management is concerned with delivering and supporting IT services that are appropriate to the business requirements of the organisation. ITIL provides a comprehensive, consistent and coherent set of best practices for IT service management and related processes, promoting a quality approach for achieving business effectiveness and efficiency in the use of IS.

ITIL service management processes are intended to underpin, but not dictate, the business processes of an organisation. The generic processes described in ITIL promote best practice and may be used as a basis for achieving the British Standard for IT Service Management (BS 15000), which is currently being considered for fast-tracking to become an international standard—ISO/IEC 20000.

The core operational processes of IT service management are described within the two ITIL publications: *Service Support* and *Service Delivery.*

The processes of service support described in ITIL are:

- Incident management
- Problem management
- Configuration management
- Change management
- Release management
- Service desk function

The processes of service delivery described in ITIL are:

- Capacity management
- Availability management
- Financial management for IT services
- Service level management
- IT service continuity management

The latest ITIL publications are much broader in scope than IT service management and cover the major activities necessary to define and develop effective IT processes, including:

- The development of new systems
- Design and planning of the information and communication technologies (ICT) infrastructure
- Operation and maintenance of existing systems
- Adjustment of service delivery to the constantly evolving requirements of the core business

Two principal concepts characterise the basic thinking of ITIL:

- Holistic service management—IT service managers:
  - Assure the consideration of functional and non-functional requirements
  - Ensure that services are appropriately tested before live operational use
  - Assess the possible risks and impact on existing infrastructure caused by new or modified systems
  - Define future service requirements
- Customer orientation—IT services are provided at a level of quality that allows permanent reliance on them. To assure this quality, responsibility is assigned to individuals who:
  - Consult the users and help them use the services in an optimal manner
  - Collect and forward opinions and recommendations of users
  - Resolve incidents
  - Monitor the performance of the services delivered
  - Manage change

The book *Planning to Implement Service Management* discusses the key issues of planning and implementing IT service management. It also explains the steps required for implementation and improvement of IT service delivery.

ICT Infrastructure Management covers all aspects of ICT infrastructure from the identification of business requirements through the tendering process, to the testing, installation, deployment, and ongoing support and maintenance of the ICT components and IT services. The major processes involved in the management of all areas and aspects of technology are embraced by:

- Design and planning processes
- Deployment processes
- Operations processes
- Technical support processes

Applications Management discusses software development using a life cycle approach and expands on the issues of business change with emphasis on clear requirements definition and implementation of solutions to meet business needs.

ITIL Security Management details the process of planning and managing a defined level of security on information and ICT services, including all aspects associated with the reaction to security incidents.

Readers should note that the content of the IT Infrastructure Library is currently being refreshed, but that activity does not invalidate the guidance in this paper, although all references are to the current publications. (See the News section of *www.itil.co.uk* for further information.

ISO 17799

Essential parts of ISO 17799 Information Technology—Code of Practice for Information Security Management were developed and published by the British Standards Institution, including BS 7799-1:1999 and parts of BS 7799-2:1999.

The original standard was issued in two parts:

- BS 7799 Part 1: Information Technology—Code of Practice for Information Security Management
- BS 7799 Part 2: Information Security Management Systems—Specification with Guidance for Use

The ISO and IEC, which have established a joint technical committee, the ISO/IEC JTC 1, published the international standard.

ISO/IEC 17799:2000 provides information to responsible parties for implementing information security within an organisation. It can be seen as a basis for developing security standards and management practices within an organisation to improve reliability on information security in inter-organisational relationships.

The standard was published in 2000 in its first edition, which was updated in June 2005. It can be classified as current best practice in the subject area of information security management systems. The original BS 7799 was revised and reissued in September 2002.

The guiding principles are the initial point when implementing information security. They rely on either legal requirements or generally accepted best practices.

Measures based on legal requirements include:

- Protection and nondisclosure of personal data
- Protection of internal information
- Protection of intellectual property rights

Best practices mentioned are:

- Information security policy
- Assignment of responsibility for information security
- Problem escalation
- Business continuity management

When implementing a system for information security management several critical success factors are to be considered:

- The security policy, its objectives and activities reflect the business objectives.
- The implementation considers cultural aspects of the organisation.
- Open support from and engagement of senior management are required.
- Thorough knowledge of security requirements, risk assessment and risk management is required.
- Effective marketing of security targets all personnel, including members of management.
- The security policy and security measures are communicated to contracted third parties.
- Users are trained in an adequate manner.
- A comprehensive and balanced system for performance measurement is available, which supports continuous improvement by giving feedback.

After presenting introductory information (scope, terms and definitions), a framework for the development of an organisation-specific information security management system (ISMS) is presented.

Such a system should consist of at least the following parts:
- Security policy
- Organisational security
- Asset classification and control
- Personnel security
- Physical and environmental security
- Communications and operations management
- Access control
- Systems development and maintenance
- Business continuity management
- Compliance

6. How Best to Implement COBIT, ITIL and ISO 17799

There is no doubt that effective management policies and procedures help ensure that IT is managed as a routine part of everyday activities. Adoption of standards and best practices will help enable quick implementation of good procedures and avoid lengthy delays re-inventing wheels and agreeing on approaches.

However, the best practices adopted have to be consistent with the risk management and control framework, appropriate for the organisation, and integrated with other methods and practices that are being used. Standards and best practices are not a panacea, and their effectiveness depends on how they have been actually implemented and kept up to date. They are most useful when applied as a set of principles and as a starting point for tailoring specific procedures.

To avoid practices becoming shelfware, change enablement is required so management and staff understand what to do, how to do it and why it is important.

For best practices to be effective, the use of a common language and a standardised approach oriented toward real business requirements is best, as it ensures everyone follows the same set of objectives, issues and priorities.

Tailoring

Every organisation needs to tailor the use of standards and practices, such as those examined in this document, to suit its individual requirements. All three can play a very useful part—COBIT and ISO 17799 helping to define *what* should be done and ITIL providing the *how* for service management aspects. Typical uses for the standards and practices are:

- To support governance by:
  - Providing a management policy and control framework
  - Enabling process ownership, clear responsibility and accountability for IT activities
  - Aligning IT objectives with business objectives, setting priorities and allocating resources
  - Ensuring return on investments and optimising costs
  - Making sure significant risks have been identified and are transparent to management, responsibility for risk management has been assigned and embedded in the organisation, and assurance has been provided to management that effective controls are in place
  - Ensuring resources have been efficiently organised and sufficient capability (technical infrastructure, process and skills) exists to execute the IT strategy
  - Making sure critical IT activities can be monitored and measured, so problems can be identified and corrective action can be taken
- To define requirements in service and project definitions, internally and with service providers, for example:
  - Setting clear, business-related IT objectives and metrics
  - Defining services and projects in end-user terms
  - Creating service level agreements and contracts that can be monitored by customers
  - Making sure customer requirements have been properly cascaded down into technical IT operational requirements
  - Considering services and project portfolios collectively so that relative priorities can be set and resources can be allocated on an equitable and achievable basis
- To verify provider capability or demonstrate competence to the market by:
  - Independent third-party assessments and audits
  - Contractual commitments
  - Attestations and certifications

- To facilitate continuous improvement by:
  - Maturity assessments
  - Gap analyses
  - Benchmarking
  - Improvement planning
  - Avoidance of re-inventing already proven good approaches
- As a framework for audit/assessment and an external view through:
  - Objective and mutually understood criteria
  - Benchmarking to justify weaknesses and gaps in control
  - Increasing the depth and value of recommendations by following generally accepted preferred approaches

Prioritising

To avoid costly and unfocused implementations of standards and best practices, organisations need to prioritise where and how to use standards and practices. The organisation needs an effective action plan that suits its particular circumstances and needs. First, it is important for the board to take ownership of IT governance and set the direction management should follow. Making sure that the board operates with IT governance in mind does this best. The board should:

- Make sure IT is on the board agenda
- Challenge management's activities with regard to IT to make sure IT issues are uncovered
- Guide management by helping align IT initiatives with real business needs and ensure that it appreciates the potential impact on the business of IT-related risks
- Insist that IT performance be measured and reported to the board
- Establish an IT steering group or IT governing council with responsibility for communicating IT issues between the board and management
- Insist that there be a management framework for IT governance based on a common approach (e.g., COBIT) and a best practice framework for IT service management based on a global *de facto* standard (e.g., ITIL).

Planning

With this mandate and direction in place, management then can initiate and put into action an implementation approach. To help management decide where to begin and to ensure that the implementation process delivers positive results where they are needed most, the following steps are suggested:

1. Set up an organisational framework (ideally as part of an overall IT governance initiative) with clear responsibilities and objectives and participation from all interested parties that will take implementation forward and own it as an initiative.
2. Align IT strategy with business goals. In which current business objectives does IT have a significant contribution? Obtain a good understanding of the business environment, risk appetite and business strategy as they relate to IT. COBIT's management guidelines (specifically the KGIs) and the COBIT framework's information criteria help define IT objectives. Used in conjunction with ITIL, services and service level agreements (SLAs) can be defined in end-user terms.

3. Understand and define the risks. Given the business objectives, what are the risks relating to IT's ability to deliver against these objectives? Consider:
   – Previous history and patterns of performance
   – Current IT organisational factors
   – Complexity and size/scope of the existing or planned IT environment
   – Inherent vulnerability of the current and planned IT environment
   – Nature of the IT initiatives being considered, e.g., new systems projects, outsourcing considerations, architectural changes, etc.

   COBIT's process for risk management (PO9) and the application of the COBIT control framework and information criteria help ensure that risks are identified and owned. Instituting ITIL clarifies operational risks and ISO 17799 clarifies security risks.
4. Define target areas and identify the process areas in IT that are critical to managing these risk areas. The COBIT process framework can be used as the basis, underpinned by ITIL's definition of key service delivery processes and ISO 17799's security objectives. OGC's publication *Management of Risk: Guidance to Practioners*, can also be of assistance here in assessing and managing risks at any of the four main levels, i.e., strategic, programme, project or operational.
5. Analyse current capability and identify gaps. Perform a maturity capability assessment to find out where improvements are needed most. The COBIT management guidelines provide a basis supported in more detail by ITIL and ISO 17799 best practices.
6. Develop improvement strategies, and decide which are the highest priority projects that will help improve the management and governance of these significant areas. This decision should be based on the potential benefit, ease of implementation, and with a focus on important IT processes and core competencies. Specific improvement projects as part of a continuous improvement initiative should be outlined.

   The COBIT CSFs, control objectives and control practices can be supported by more detailed ITIL and ISO 17799 guidance.
7. Measure results, establish a scorecard mechanism for measuring current performance and monitor the results of new improvements considering, as a minimum, the following key considerations:
   – Will the organisational structures support strategy implementation?
   – Are responsibilities for risk management embedded in the organisation?
   – Do infrastructures exist that will facilitate and support the creation and sharing of vital business information?
   – Have strategies and goals been communicated effectively to everyone who needs to know within the organisation?

   COBIT's management guidelines (specifically the KPIs, aligned to previously defined KGIs) can form the basis of a scorecard.
8. Repeat steps 2 through 7 on a regular basis.

Avoiding Pitfalls

There are also some obvious, but pragmatic, rules that management ought to follow:

- Treat the implementation initiative as a project activity with a series of phases rather than a 'one-off' step.
- Remember that implementation involves cultural change as well as new processes. Therefore, a key success factor is the enablement and motivation of these changes.

- Make sure there is a clear understanding of the objectives.
- Manage expectations. In most enterprises, achieving successful oversight of IT takes time and is a continuous improvement process.
- Focus first on where it is easiest to make changes and deliver improvements and build from there one step at a time.
- Obtain top management buy-in and ownership. This needs to be based on the principles of best managing the IT investment.
- Avoid the initiative becoming perceived as a purely bureaucratic exercise.
- Avoid the unfocused checklist approach.

Aligning Best Practices

IT best practices need to be aligned to business requirements and integrated with one another and with internal procedures. CobiT can be used at the highest level, providing an overall control framework based on an IT process model that should generically suit every organisation. Specific practices and standards such as ITIL and ISO 17799 cover discrete areas and can be mapped to the CobiT framework, thus providing an hierarchy of guidance materials.

To better understand mapping between ITIL and ISO 17799 and CobiT, refer to the appendix, where each of the CobiT 34 IT processes and high-level control objectives has been mapped to specific sections of ITIL and ISO 17799. These mappings are based on subjective judgement and are intended only to be a guide. As part of future updates to ITIL and CobiT, OGC and ITGI plan to further align the terminology and content of their practices with other practices to facilitate easier integration.

Appendix I—Mapping ITIL and ISO 17799 to COBIT Control Objectives

Note that for the purposes of this mapping:

- Text shown in **bold** indicates where ITIL or ISO 17799 is considered to provide the best supporting detail for a COBIT control objective.
- Regular text indicates where it is considered that ITIL or ISO 17799 provides supporting detail for a COBIT control objective, but it is not necessarily the primary reference.

This mapping is not intended to be definitive or prescriptive; it is only a guide. Links are shown only at the high level, pointing to the relevant section in the other documents.

ISACA and ITGI are carrying out detailed research into the mapping between COBIT and other standards and best practices. More information can be found at *www.isaca.org/research.*

COBIT Domain: Plan and Organise

P01 Define a Strategic IT Plan

Defining a strategic IT plan satisfies the business requirement of striking an optimum balance of information technology opportunities and IT business requirements as well as ensuring its further accomplishment. It is enabled by a strategic planning process undertaken at regular intervals giving rise to long-term plans; the long-term plans should periodically be translated into operational plans setting clear and concrete short-term goals.

COBIT Control Objective		Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information	
P01.1	IT as part of the organisation's long- and short-range plan	Mission; goals; strengths, weaknesses, opportunities and threats (SWOT); IT alignment with business strategy	*The Business Perspective*, 4. Business/IS Alignment *ICT Infrastructure Management*, Design and Planning, 2.5 The process and deliverables of strategic planning	4.1	Information security infrastructure
P01.2	IT long-range plan	IT support of mission/goal achievement, stakeholder input	*The Business Perspective*, Business/IS Alignment, 4.3 The management governance framework *ICT Infrastructure Management*, Annex 2B, The Contents of ICT Policies, Strategies, Architectures and Plan	4.1	Information security infrastructure
P01.3	IT long-range planning—approach and structure	Structured approach, business model, risk assessment, benefits identification, performance indicators	*The Business Perspective*, Business/IS Alignment, 4.5 Establishing the IS direction *ICT Infrastructure Management*, Design and Planning, 2.5 The process and deliverables of strategic planning		
P01.4	IT long-range plan changes	Modifying plans to accommodate business change	*The Business Perspective*, Concepts, 2.9 Business change *The Business Perspective*, Managing the Provision of Service, 6.1.4 Change management		

PO1 Define a Strategic IT Plan (cont.)

CobiT Control Objective		Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information	
PO1.5	Short-range planning for the IT function	Resource allocation, response to change, feasibility studies	*The Business Perspective*, Managing the Provision of Service, 6.2 New services *ICT Infrastructure Management*, Appendix C.1, General Planning Procedures and Preparation *ICT Infrastructure Management*, Appendix L.2, Feasibility Study	4.1	Information security infrastructure
PO1.6	Communication of IT plans	Communication/awareness of business process owners	*ICT Infrastructure Management*, Annex 3C, Example of a Communications Plan	4.1	Information security infrastructure
PO1.7	Monitoring and evaluating of IT plans	Feedback on quality and usefulness	*Applications Management*, The Applications Management Lifecycle, 5.7 Optimise *ICT Infrastructure Management*, The Management Processes Involved, 2.4.5 Reviewing and evaluating progress of the plan *Planning to Implement*, How Do We Keep the Momentum Going, 7.4 Ongoing monitoring and process reviews		
PO1.8	Assessment of existing systems	Assessment of functionality, stability, complexity and costs; degree of business support	*Service Delivery*, Capacity Management, 6.2.3 Resource capacity management *Service Support*, Planning the Implementation of Service Manaagement, 11.3 Assessing the current situation *ICT Infrastructure Management,* Design and Planning, 2.8 The planning and implementation of new technology and services	4.1	Information security infrastructure

CobiT Domain: Plan and Organise

PO2 Define the Information Architecture

Defining the information architecture satisfies the business requirement of optimising the organisation of the information systems. It is enabled by creating and maintaining a business information model and ensuring that appropriate systems are defined to optimise the use of this information.

CobiT Control Objective	**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
PO2.1 Information architecture model	Information needs analysis, information architecture model maintained, corporate data model and Plans	*ICT Infrastructure Management*, Annex 2B, The Contents of ICT Policies, Strategies, Architectures	10.1 Security requirements of systems
PO2.2 Corporate data dictionary and data syntax rules	Corporate data dictionary		
PO2.3 Data classification scheme	Information classes, ownership, access rules		**5.2 Information classification** 4.1 Information security infrastructure 5.1 Accountability for assets 8.6 Media handling and security 8.7 Exchanges of information and software 9.1 Business requirement for access control
PO2.4 Security levels	Security levels for each information class	*Applications Management*, The Application Management Lifecycle, 5.2 Requirements	**5.2 Information classification** 4.1 Information security infrastructure 5.1 Accountability for assets 8.6 Media handling and security 9.1 Business requirement for access control

CobiT Domain: Plan and Organise

PO3 Determine Technological Direction

Determining technological direction satisfies the business requirement of taking advantage of available and emerging technology to drive and make possible the business strategy. It is enabled by the creation and maintenance of a technological infrastructure plan that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms.

CobiT Control Objective	**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
PO3.1 Technological infrastructure planning	Technological infrastructure plan, systems architecture, technological direction, migration strategies	*Applications Management*, The Application Management Lifecycle, 5.5 Deploy *ICT Infrastructure Management*, Design and Planning, 2.5 The processes and deliverables of strategic planning	3.1 Information security policy 4.1 Information security infrastructure 8.5 Network management
PO3.2 Monitor future trends and regulations	Technological infrastructure plan maintenance	*ICT Infrastructure Management*, Technical Support, 5.4 The technical support processes	4.1 Information security infrastructure
PO3.3 Technological infrastructure contingency	Systematic assessment, redundancy, resilience and evolutionary capability	***Service Delivery,* Capacity Management, 6.3 Activities in capacity management** ***Service Delivery,* Availability Management, 8.5 Availability planning** *ICT Infrastructure Management*, 3 Deployment	5.2 Information classification 11.1 Aspects of business continuity management
PO3.4 Hardware and software acquisition plans	Plan modification to accommodate business change	***Software Asset Management*, Logistics Processes, 5.3.4 Procurement**	4.1 Information security infrastructure

P03 Determine Technological Direction (cont.)			
COBIT Control Objective	**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
P03.5 Technology standards	Resource allocation, response to change, feasibility studies of new technology services	*ICT Infrastructure Management*, Design and Planning, 2.8 The planning and implementation *ICT Infrastructure Management* Technical Support*,* 5.4 The technical support processes *ICT Infrastructure Management*, Appendix L, The Contents of a Feasibility Study/Gap Analysis	8.2 System planning and acceptance 8.7 Exchanges of information and software 9.7 Monitoring system access and use 9.8 Mobile computing and teleworking

COBIT Domain: Plan and Organise P04 Define the IT Organisation and Relationships			
Defining the IT organisation and relationships satisfies the business requirement of delivering the right IT services. It is enabled by an organisation suitable in numbers and skills with roles and responsibilities defined and communicated, aligned with the business. It facilitates the strategy and provides for effective direction and adequate control.			
COBIT Control Objective	**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
P04.1 IT planning or steering committee	Oversight of IT function and activities,regular meetings and reporting to senior management	*Business Perspective*, Business/ IS Alignment, 4.3.5 The IS steering group	4.1 Information security infrastructure
P04.2 Organisational placement of the IT function	Authority and independence, critical mass, relationships, partnerships	*ICT Infrastructure Management*, ICT Infrastructuure Management Overview, 1.6.1 Organisational structure *Business Perspective*, 7. Supplier Relationship Management *Software Asset Management*, Organisation, Roles and Responsibilities, 4.1 Decision about centralisation *Software Asset Management*, 8. Partners and SAM	4.1 Information security infrastructure
P04.3 Review of organisational achievements	Framework for review, meeting business needs	*Service Delivery,* Service Level Management, 4.5 The ongoing process	4.1 Information security infrastructure
P04.4 Roles and responsibilities	Explicit roles and responsibilities	*Business Perspective*, 8. Roles, Responsibilities and Interfaces *Application Management*, 6. Organising Roles and Functions *Software Asset Management*, Organisation, Roles and Responsibilities, 4.4 Roles and responsibilities *ICT Infrastructure Management*, ICT Infrastructure Management Overview, 1.6 Roles, responsibilities and interfaces	4.1 Information security infrastructure 6.1 Security in job definition and resourcing 6.2 User training 8.1 Operational procedures and responsibilities
P04.5 Responsibility for quality assurance	Assigned responsibilities, expertise, satisfying business requirements	*The Business Perspective*, Roles, Responsibilities and Interfaces, 8.1 Overall IS role and the interactions	

PO4 Define the IT Organisation and Relationships (cont.)			
COBIT Control Objective	**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
PO4.6 Responsibility for logical and physical security	Assigned responsibilities, information security management	*Security Management*, Guidelines for Implementing Security Management, 5.2.1 The role of the security manager *ICT Infrastructure Management*, Appendix C, 3.5 Security	**4.1 Information security infrastructure** **6.1 Security in job definition and resourcing** 12.1 Compliance with legal requirements
PO4.7 Ownership and custodianship	Assigned data owners and custodians	*Security Management*, Security Management Measures, 4.2.1 Asset classification and control	**5.1 Accountability for assets** 4.1 Information security infrastructure
PO4.8 Data and system ownership	Information assets (data and systems) owned, classification, access rights	***ICT Infrastructure Management,* Design and Planning, 2.5.2 The ICT architecture** ***Software Asset Management,* Process Overview, 5.2 Core asset management processes** *Security Management*, Security Management Measures, 4.2.1 Asset classification and control	**5.1 Accountability for assets** 4.1 Information security infrastructure
PO4.9 Supervision	Roles and responsibilities, review of KPIs	*The Business Perspective*, Roles, Responsibilities and Interfaces, 8.6 The service delivery manager role	4.1 Information security infrastructure 5.1 Accountability for assets
PO4.10 Segregation of duties	Avoidance of subversion of critical processes		8.1 Operational procedures and responsibilities 8.5 Network management 9.7 Monitoring system access and use
PO4.11 IT staffing	Number and competency, requirements evaluation		
PO4.12 Job or position descriptions for IT staff	Job descriptions, delineation of authority, responsibility, skills, experience, evaluation	*ICT Infrastructure Management*, Annex 2A, ICT Planner and Designer Roles	6.1 Security in job definition and resourcing
PO4.13 Key IT personnel	Roles defined, individuals identified		
PO4.14 Contracted staff policies and procedures	Information assets protected		4.2 Security of third-party access 6.1 Security in job definition and resourcing 7.1 Secure areas 12.1 Compliance with legal requirements
PO4.15 Relationships	Optimal co-ordination, communications and liaison	***The Business Perspective*, 7. Supplier Relationship Management** *The Business Perspective*, Managing the Provision of Service, 6.1 Core ITIL process integration *ICT Infrastructure Management*, ICT Infrastructure Management Overview, 1.6.2 External interfaces *Service Delivery*, 2. Relationship Between Processes *Service Support*, 2. Relationship Between Processes *Software Asset Management*, 8. Partners and SAM	4.1 Information security infrastructure

CobiT Domain: Plan and Organise
PO5 Manage the IT Investment

Managing the IT investment satisfies the business requirement of ensuring funding and controlling disbursement of financial resources. It is enabled by a periodic investment and operational budget established and approved by the business.

CobiT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
PO5.1 Annual IT operating budget	Budgeting process, budget in line with business plans	***Service Delivery*, Financial Management for IT Services, 5.2 Budgeting**	3.1 Information security policy 6.3 Responding to security incidents and malfunctions
PO5.2 Cost and benefit monitoring	Benefits determined and reported, performance indicators, IT cost reporting	***Service Delivery*, Financial Management for IT Services, 5.1.7 Benefits** ***Service Delivery*, Financial Management for IT Services, 5.1.8 Costs** ***Service Delivery*, Financial Management for IT Services, 5.3 Developing the IT accounting system** *Service Delivery,* Service Level Management (SLM), 4.2 The SLM process *The Business Perspective,* Concepts, 2.10 Benefits, costs and possible problems	3.1 Information security policy
PO5.3 Cost and benefit justification	Benefits analysis, management controls	***Service Delivery*, Appendix F, Cost Benefit Analysis for IT Service Management Processes**	

CobiT Domain: Plan and Organise
PO6 Communicate Management Aims and Direction

Communicating management aims and direction satisfies the business requirement of ensuring user awareness and the understanding of those aims. It is enabled by policies established and communicated to the user community; standards need to be established to translate the strategic options into practical and usable rules.

CobiT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
PO6.1 Positive information control environment	Framework and awareness programme addressing integrity, ethics, competencies, accountability, security and business continuity planning	*Planning to Implement*, What is the Vision?, 2.2 Communicating the vision	**3.1 Information security policy** **6.3 Responding to security incidents and malfunctions** 4.1 Information security infrastructure 6.1 Security in job definition and resourcing 6.2 User training
PO6.2 Management's responsibility for policies	Promulgating and controlling policy, regular policy reviews		3.1 Information security policy 4.1 Information security infrastructure
PO6.3 Communication of organisation policies	Communications plan and effective communication channels	*The Business Perspective*, The Value of IT, 3.4 Establishing a value culture	3.1 Information security policy 6.1 Security in job definition and resourcing
PO6.4 Policy implementation resources	Appropriate resources, management monitoring of implementation plan	*Security Management*, Security Management Measures, 4.2 Implement *Security Management*, Security Management Measures, 4.3 Audit and evaluate	3.1 Information security policy 4.1 Information security infrastructure 6.1 Security in job definition and resourcing 12.2 Reviews of security policy and technical compliance

PO6 Communicate Management Aims and Direction (cont.)			
CobiT Control Objective	**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
PO6.5 Maintenance of policies	Regular review and adjustment in line with prevalent conditions		3.1 Information security policy 4.1 Information security infrastructure 12.2 Reviews of security policy and technical compliance
PO6.6 Compliance with policies, procedures and standards	Compliance with ethical, security and internal control standards	*Security Management*, Security Management Measures, 4.3 Audit and evaluate *Planning to Implement*, How Do We Keep the Momentum Going?, 7.4 Ongoing monitoring and process reviews *Service Support,* Change Management, 8.7.1 Auditing for compliance *Service Delivery,* Financial Management for IT Services, 5.7.11 Auditing the systems	6.1 Security in job definition and resourcing 6.2 User training 6.3 Responding to security incidents and malfunctions 12.2 Reviews of security policy and technical compliance
PO6.7 Quality commitment	Quality philosophy, policies and objectives		
PO6.8 Security and internal control framework policy	Policy to comply with overall business objectives aimed at minimising risk, prioritised measures		**3.1 Information security policy** **12.2 Reviews of security policy and technical compliance** 6.3 Responding to security incidents and malfunctions
PO6.9 Intellectual property rights (IPR)	IPR policy covering in-house and contract-developed software		4.2 Security of third-party access 6.1 Security in job definition and resourcing 10.5 Security in development and support processes 12.1 Compliance with legal requirements
PO6.10 Issue-specific policies	Document management decisions		5.2 Information classification 7.1 Secure areas 7.3 General controls 7.2 Equipment security 8.7 Exchanges of information and software 9.4 Network access control 9.8 Mobile computing and teleworking
PO6.11 Communication of IT security awareness	Awareness of IT security policy		**3.1 Information security policy** **6.1 Security in job definition and resourcing** **6.2 User training** 4.1 Information security infrastructure

CobiT Domain: Plan and Organise
PO7 Manage Human Resources

Managing human resources satisfies the business requirement of acquiring and maintaining a motivated and competent workforce and maximising personnel contributions to the IT processes. It is enabled by sound, fair and transparent personnel management practices to recruit, line, vet, compensate, train, appraise, promote and dismiss.

CobiT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
PO7.1 Personnel recruitment and promotion	Personnel recruitment and promotion practices based on objective criteria, skills mapped to organisational goals		6.1 Security in job definition and resourcing
PO7.2 Personnel qualifications	Verification of qualifications, professional membership encouraged		4.1 Information security infrastructure 6.1 Security in job definition and resourcing
PO7.3 Roles and responsibilities	Defined roles and responsibilities related to terms and conditions of employment		4.1 Information security infrastructure 6.1 Security in job definition and resourcing 6.3 Responding to security incidents and malfunctions
PO7.4 Personnel training	Organisational induction and ongoing training to raise technical and management skill levels		4.2 Security of third-party access 8.2 System planning and acceptance 9.8 Mobile computing and teleworking 11.1 Aspects of business continuity management
PO7.5 Cross-training or staff backup	Address resource availability of key functions, succession planning		6.1 Security in job definition and resourcing
PO7.6 Personnel clearance procedures	Security clearance dependent upon sensitivity of position		6.1 Security in job definition and resourcing
PO7.7 Employee job performance evaluation	Performance evaluation reinforced by award system		6.1 Security in job definition and resourcing
PO7.8 Job change and termination	Appropriate and timely action so as not to compromise security		**9.2 User access management** 6.1 Security in job definition and resourcing

CobiT Domain: Plan and Organise PO8 Ensure Compliance With External Requirements			
Ensuring compliance with external requirements satisfies the business requirement of meeting legal, regulatory and contractual obligations. It is enabled by identifying and analysing external requirements for their IT impact and taking appropriate measures to comply with them.			
CobiT Control Objective	**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
PO8.1 External requirements review	Impact assessment of external relationships on overall information needs, e.g., alignment of IT strategies		4.1 Information security infrastructure 12.2 Reviews of security policy and technical compliance 12.1 Compliance with legal requirements
PO8.2 Practices and procedures for complying with external requirements	Timely corrective action to guarantee compliance with external requirements		12.1 Compliance with legal requirements
PO8.3 Safety and ergonomic compliance	Compliance with safety and ergonomic standards in the working environment		5.1 Accountability for assets 7.1 Secure areas 8.1 Operational procedures and responsibilities
PO8.4 Privacy, intellectual property and data flow	Cryptographic regulations applicable to IT practices		8.7 Exchanges of information and software 10.3 Cryptographic controls 12.1 Compliance with legal requirements
PO8.5 Electronic commerce	Contracts on communication processes, standards for message security, compliance with local laws and regulations		8.7 Exchanges of information and software
PO8.6 Compliance with insurance contracts	Insurance contract requirements identified and met		5.1 Accountability for assets 7.2 Equipment security

CobiT Domain: Plan and Organise
PO9 Assess Risks

Assessing risks satisfies the business requirement of supporting management decisions through achieving IT objectives and responding to threats by reducing complexity, increasing objectivity and identifying important decision factors. It is enabled by the organisation engaging itself in IT risk identification and impact analysis, involving multidisciplinary functions and taking cost-effective measures to mitigate risks.

CobiT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
PO9.1 Business risk assessment	Risk assessment framework, risk assessment at a number of levels, reassessments and information updates	*ICT Infrastructure Management*, Annex 3B, Risk Management Plan *Service Delivery,* Availability Management, 8.9.3 Central Computer and Telecommunications Agency (CCTA) Risk Analysis and Management Method (CRAMM) *Service Delivery,* IT Service Continuity Management, 7.3.2 Requirements analysis and strategy definition	
PO9.2 Risk assessment approach	Management-led identification of vulnerabilities and the risk mitigation solution, appropriate skills	*Service Delivery,* IT Service Continuity Management, 7.5 Risk assessment model *ICT Infrastructure Management*, Annex 3B, Risk Management Plan *Service Delivery,* Availability Management, 8.9.3 CRAMM	3.1 Information security policy 4.1 Information security infrastructure
PO9.3 Risk identification	Cause/effect relationships, qualitative and quantitative risk ranking, risk classification	*Service Delivery,* Availability Management, 8.9.3 CRAMM	4.2 Security of third-party access 5.2 Information classification 7.1 Secure areas 7.2 Equipment security 9.2 User access management 9.4 Network access control 10.3 Cryptographic controls
PO9.4 Risk measurement	Measurement of risk exposure, assessment of risk acceptance capacity	*Service Delivery,* Availability Management, 8.9.3 CRAMM	
PO9.5 Risk action plan	Cost-effective controls and security measures, risk strategies in terms of avoidance, mitigation or acceptance	*Service Delivery,* IT Service Continuity, 7.3.2 Risk reduction measures *Service Delivery,* IT Service Continuity, 7.3.3 Implement risk reduction measures	10.1 Security requirements of systems
PO9.6 Risk acceptance	Formal acceptance of residual risk, offset by insurance, contractual liabilities	*The Business Perspective,* Understanding the Business Viewpoint, 5.1.1 Business views on risk	
PO9.7 Safeguard selection	Control system to balance prevention, detection, correction and recovery measures		4.2 Security of third-party access
PO9.8 Risk assessment commitment	Important tool in design and implementation as well as monitoring and evaluation mechanisms		3.1 Information security policy

CobiT Domain: Plan and Organise
PO10 Manage Projects

Managing projects satisfies the business requirement of setting priorities and delivering on time and within budget. It is enabled by the organisation identifying and prioritising projects in line with the operational plan, and the adoption and application of sound project management techniques for each project undertaken

CobiT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
PO10.1 Project management framework	Methodology covering responsibilities, task breakdown, budgeting of time and resources, milestones, checkpoints, approvals	*ICT Infrastructure Management*, Design and Planning, 2.4.4 Design and implementing a plan *ICT Infrastructure Management*, Annex 3B, Running a Deployment Project	
PO10.2 User department participation in project initiation	Participation in definition and authorisation of development, implementation and modification		4.1 Information security infrastructure
PO10.3 Project team membership and responsibilities	Framework specifying basis for assigning staff to projects	*ICT Infrastructure Management*, Appendix F2, Appoint a Project Team	
PO10.4 Project definition	Nature and scope of project clear before work begins	*ICT Infrastructure Management*, Annex 3B, Running a Deployment Project	
PO10.5 Project approval	Feasibility study reports review, basis for project decision	*ICT Infrastructure Management*, Annex 3B, Running a Deployment Project	
PO10.6 Project phase approval	Designated manager approval of deliverables in each phase, prior to start of the next phase	*ICT Infrastructure Management*, Annex 3B, Running a Deployment Project	
PO10.7 Project master plan	Adequate plan for maintaining control over the project, method of monitoring time and cost	*ICT Infrastructure Management*, Annex 3B, Running a Deployment Project	
PO10.8 System quality assurance plan	Quality plan integrated with project plan, formal review		
PO10.9 Planning of assurance methods	Support accreditation, assuring that internal controls and security features meet related requirements		
PO10.10 Formal project risk management	Elimination or minimisation of project risks		
PO10.11 Test plan	Test plan for every development, implementation and modification project		
PO10.12 Training plan	Training plan for every development, implementation and modification project		
PO10.13 Post-implementation review plan			

COBIT Domain: Plan and Organise
PO11 Manage Quality

Managing quality satisfies the business requirement of meeting the IT customer requirements. It is enabled by the planning, implementing and maintaining of quality management standards and systems providing for distinct development phases, clear deliverables and explicit responsibilities.

COBIT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
PO11.1 General quality plan	Overall quality plan based on long-range plans, promoting continuous improvement		
PO11.2 Quality assurance approach	Standard approach covering general and project-specific QA activities		
PO11.3 Quality assurance planning	Scope and timing of QA activities		
PO11.4 Quality assurance review of adherence to IT standards and procedures	Review of general IT standards and procedures		
PO11.5 System development life cycle (SDLC) methodology	SDLC appropriate for the systems to be developed, acquired, implemented and maintained	*Application Management*, The Application Management Life Cycle, 5.1 The application life cycle	
PO11.6 System development life cycle methodology for major changes to existing technology	SDLC observed for major changes	*Application Management*, The Application Management Life Cycle, 5.1 The application life cycle	
PO11.7 Updating of the system development life cycle methodology	Periodic review to ensure SDLC reflects currently accepted techniques and procedures	*Application Management*, The Application Management Life Cycle, 5.1 The application life cycle	
PO11.8 Co-ordination and communication	Close co-ordination between customers and systems implementers, structured methods for close co-operation and communication throughout SDLC	*Application Management*, Organising Roles and Function, 6.1 Team dynamics	
PO11.9 Acquisition and maintenance framework for the technology infrastructure	Steps (acquiring, programming, documenting, testing, etc.) governed by the framework		
PO11.10 Third-party implementer relationships	Good working relationships, acceptance criteria, handling of changes, problems		4.2 Security of third-party access 6.1 Security in job definition and resourcing 10.5 Security in development and support processes
PO11.11 Programme documentation standards	IS documentation that conforms to standards		
PO11.12 Programme testing standards	Test requirements, verification, documentation and retention periods covered by standards; levels of testing		
PO11.13 System testing standards	System test standards covered in SDLC		
PO11.14 Parallel/pilot testing	Circumstances for parallel/pilot testing defined in SDLC		
PO11.15 System testing documentation	Retention of system testing documentation		
PO11.16 Quality assurance evaluation of adherence to development standards	Post-implementation review to assess levels of adherence to the provisions of the SDLC methodology		
PO11.17 Quality assurance review of achievement of IT objectives	Level of objective achievement through IS function		
PO11.18 Quality metrics	Measure quality goal achievement		
PO11.19 Reports of quality assurance reviews	QA reports submitted to management		

COBIT Domain: Acquire and Implement AI1 Identify Automated Solutions				
Identifying automated solutions satisfies the business goal of ensuring an effective and efficient approach to satisfy the user requirements. It is enabled by an objective and clear identification and analysis of the alternative opportunities measured against user requirements.				
COBIT Control Objective		**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
AI1.1	Definition of information requirements	Requirements definition, functional and operational requirements specified including performance, reliability and security	*Application Management*, The Application Management Life Cycle, 5.2 Requirements *ICT Infrastructure Management*, Appendix F3, Requirements Analysis	
AI1.2	Formulation of alternative courses of action	Alternative solutions to satisfying business requirements put forward	*Software Asset Management*, Logistics Processes, 5.3.3 Evaluation *ICT Infrastructure Management*, Appendix F6, Produce Alternative Designs, Approaches and Plans	
AI1.3	Formulation of acquisition strategy	Software acquisition strategy plan	*Application Management*, Aligning the Delivery Strategy with Key Business Drivers and Organisational Capabilities, 4.3 Preparing to deliver the application	
AI1.4	Third-party service requirements	Evaluation of requirements and specification of request for proposal (RFP)	*ICT Infrastructure Management*, Appendix F11, Prepare a Formal Invitation to Tender (ITT) or Statement of Requirements (SOR) *ICT Infrastructure Management*, Appendix F12, Prepare for the Review Process and Selection Method	10.5 Security in development and support processes
AI1.5	Technological feasibility study	Examination of alternatives for satisfying business requirements	*ICT Infrastructure Management*, Appendix F6, Produce Alternative Designs, Approaches and Plans *ICT Infrastructure Management*, Annex 3B.2, Project Feasibility Phase *ICT Infrastructure Management*, Appendix L, The Contents of a Feasibility Study	4.1 Information security infrastructure
AI1.6	Economic feasibility study	Cost-benefit analysis	*ICT Infrastructure Management,* Annex 3B.2, Project Feasibility Phase *ICT Infrastructure Management*, Appendix L, The Contents of a Feasibility Study	
AI1.7	Information architecture	Enterprise data model		
AI1.8	Risk analysis report	Analysis of security threats, potential vulnerabilities and impacts	*Application Management*, Control Methods and Techniques, 7.2.2 Using the quality attributes as a control tool *ICT Infrastructure Management*, Design and Planning, 2.6.1 Security issues	4.1 Information security infrastructure 9.6 Application access control 10.1 Security requirements of systems 10.2 Security in application systems

AI1 Identify Automated Solutions (cont.)			
COBIT Control Objective	**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
AI1.9 Cost-effective security controls	Security requirements identification, justification and agreement; business continuity management	*Service Delivery,* IT Service Continuity Management, 7.3.4 Operational management	**10.1 Security requirements of systems** **10.2 Security in application systems** 6.3 Responding to security incidents and malfunctions 9.4 Network access control 9.7 Monitoring system access and use 11.1 Aspects of business continuity management
AI1.10 Audit trails design	Solutions containing adequate audit trails, protection of sensitive data		9.7 Monitoring system access and use 10.2 Security in application systems 12.1 Compliance with legal requirements 12.3 System audit considerations
AI1.11 Ergonomics	Ergonomic issues associated with IS solutions		
AI1.12 Selection of system software	Standard procedure for identifying potential systems to satisfy operational requirements		
AI1.13 Procurement control	Central procurement approach, common set of standards and procedures, product review and tests prior to financial settlement		
AI1.14 Software product acquisition	Procurement policy		
AI1.15 Third-party software maintenance	Procedures to validate, protect and maintain software product integrity rights	*Application Management,* The Application Management Life Cycle, 5.6.2 Day-to-day maintenance activities to maintain service levels	10.5 Security in development and support processes
AI1.16 Contract application programming	Stipulate deliverables, e.g., software, documentation; subject to testing and review prior to acceptance		10.5 Security in development and support processes
AI1.17 Acceptance of facilities	Agreed-upon acceptance plan containing acceptance procedures and criteria	***ICT Infrastructure Management***, **Appendix C, Systems Installation Policies**	4.1 Information security infrastructure 8.2 System planning and acceptance
AI1.18 Acceptance of technology	Acceptance test includes inspection, functionality tests and workload trials	***ICT Management***, **Appendix M, Checklist for the Acceptance of New Services**	8.2 System planning and acceptance

COBIT Domain: Acquire and Implement
AI2 Acquire and Maintain Application Software

Acquiring and maintaining application software satisfies the business requirement of providing automated functions that effectively support the business process. It is enabled by the definition of specific statements of functional and operational requirements and a phased implementation with clear deliverables.

COBIT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
AI2.1 Design methods	Appropriate SDLC, close liaison with users, design specification	*Application Management*, The Application Management Life Cycle, 5.1 The application Life Cycle verified	
AI2.2 Major changes to existing systems	Similar development process	*Application Management*, Concluding Remarks, 8.3 Application evolution	
AI2.3 Design approval	Design review, including user/customer representatives	*Application Management*, The Application Management Life Cycle, 5.3 Design	4.1 Information security infrastructure 8.2 System planning and acceptance
AI2.4 File requirements definition and documentation	Data dictionary rules	*Application Management*, the Application Management Life Cycle, 5.2.2 Functional requirements	10.5 Security in development and support processes
AI2.5 Programme specifications	Programme specifications verified against system design specifications		
AI2.6 Source data collection design	Mechanisms specified		
AI2.7 Input requirements definition and documentation	Mechanisms specified	*Application Management*, The Application Management Life Cycle, 5.2 Requirements *Software Asset Management,* Logistics Processes, 5.3.1 Requirements definition	10.2 Security in application systems
AI2.8 Definition of interfaces	Interface specification	*Application Management*, Aligning the Delivery Strategy With Key Business Drivers and Organisational Capabilities, 4.3 Preparing to deliver the application *Software Asset Management*, Logistics Processes, 5.3.1 Requirements definition	10.2 Security in application systems
AI2.9 User-machine interface	Usability, built-in help	*Application Management*, Aligning the Delivery Strategy With Key Business Drivers and Organisational Capabilities, 4.3 Preparing to deliver the application	
AI2.10 Processing requirements definition and documentation	Mechanisms specified	*Application Management*, The Application Management Life Cycle, 5.2 Requirements *Software Asset Management,* Logistics Processes, 5.3.1 Requirements definition	8.2 System planning and acceptance 10.2 Security in application systems 10.5 Security in development and support processes
AI2.11 Output requirements definition and documentation	Mechanisms specified	*Application Management*, The Application Management Life Cycle, 5.2 Requirements *Software Asset Management*, Logistics Processes, 5.3.1 Requirements definition	5.2 Information classification 10.2 Security in application systems

AI2 Acquire and Maintain Application Software (cont.)

CobiT Control Objective		Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
AI2.12	Controllability	Internal controls, security requirements, application controls, accuracy, completeness, timeliness, authorisation	*Application Management*, 7. Control Methods and Techniques	4.1 Information security infrastructure 9.7 Monitoring system access and use 10.2 Security in application systems
AI2.13	Availability as a key design factor	Availability considered in design, availability analysis, maintainability, reliability	***Service Delivery*, Availability Management, 8.4.1 New IT services** ***Service Delivery*, Availability Management, 8.5 Availability planning** *Application Management*, Control Methods and Techniques, 7.2 Understanding the characteristics of the application	8.2 System planning and acceptance
AI2.14	IT integrity provisions in application programme software	Data integrity, restoration, verification		10.2 Security in application systems
AI2.15	Application software testing	Unit, application, integration, system, load and stress testing, project test plan, adequate test measures	*Application Management*, Control Methods and Techniques, 7.2 Understanding the characteristics of the application *Application Management*, The Application Management Life Cycle, 5.4 Build	8.6 Media handling and security 10.4 Security of system files
AI2.16	User reference and support materials	Support manuals	*Application Management*, Control Methods and Techniques, 7.1 Understanding the applications relationship to IT services	8.1 Operational procedures and responsibilities
AI2.17	Reassessment of system design	Recognition of technical/logical discrepancies		

COBIT Domain: Acquire and Implement
AI3 Acquire and Maintain Technology Infrastructure

Acquiring and maintaining technology infrastructure satisfies the business requirement of providing the appropriate platforms for supporting business applications. It is enabled by judicious hardware and software acquisition, software standardisation, hardware assessment, software performance, and consistent system administration.

COBIT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
AI3.1 Assessment of new hardware and software	Selection criteria based on functional specification, mandatory/optional requirements, impact assessment	*ICT Infrastructure Management,* Technical Support, 5.4 The technical support processes *ICT Infrastructure Management,* Appendix F, Implementation Schedule for a New Service	8.2 System planning and acceptance 9.6 Application access control
AI3.2 Preventative maintenance for hardware	Preventive maintenance schedule	*ICT Infrastructure Management,* Operations, 4.4.2 Operational control and management of the services, components and their configuration	**7.2 Equipment security**
AI3.3 System software security	Security parameter assessment		**10.4 Security of system files** 4.1 Information security infrastructure
AI3.4 System software installation	Testing, authorisation, test libraries and environments	*ICT Infrastructure Management,* Deployment, 3.5.4 Acceptance testing	8.2 System planning and acceptance 10.4 Security of system files
AI3.5 System software maintenance	Maintenance procedures	*ICT Infrastructure Management,* 4. Operations	**10.4 Security of system files** 4.1 Information security infrastructure
AI3.6 System software change controls	Change controls	*ICT Infrastructure Management,* Deployment, 3.3.3 External interfaces (change management)	10.4 Security of system files 10.5 Security in development and support processes
AI3.7 Use and monitoring of system utilities	Policy and control on the use of system utilities	***ICT Infrastructure Management,* Design and Planning, 2.7.2 The tools** ***ICT Infrastructure Management,* Operations, 4.1.1 Managed objects** ***ICT Infrastructure Management,* Operations, 4.4.1 Management of all ICT infrastructure events**	**8.1 Operational procedures and responsibilities** **9.5 Operating system access control** **9.7 Monitoring system access and use** **12.3 System audit considerations**

COBIT Domain: Acquire and Implement
AI4 Develop and Maintain Procedures

Developing and maintaining procedures satisfies the business requirement of ensuring the proper use of the applications and technological solutions put in place. It is enabled by a structured approach to the development of user and operations procedure manuals, service requirements and training materials.

COBIT Control Objective		Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information	
AI4.1	Operational requirements and service levels	SDLC ensuring timely definition of operational requirements and service levels	***Service Delivery,* Service Level Management, 4.4.1 Produce a service catalogue** ***The Business Perspective,* Managing the Provision of Service, 6.1.6 Service level management** ***The Business Perspective,* Understanding the Business Viewpoint, 5.3 Service catalogue and portfolio of services**		
AI4.2	User procedures manual	User manual prepared and refreshed as part of development, implementation and modification project		8.1	Operational procedures and responsibilities
AI4.3	Operations manual	Operations manual prepared and kept up to date		8.1 8.2	Operational procedures and responsibilities System planning and acceptance
AI4.4	Training materials	Training materials focus on systems use		6.3 8.1	Responding to security incidents and malfunctions Operational procedures and responsibilities

COBIT Domain: Acquire and Implement
AI5 Install and Accredit Systems

Installing and accrediting systems satisfies the business requirement of verifying and confirming that the solution is fit for the intended purpose. It is enabled by the realisation of a well-formalised installation migration, conversion and acceptance plan.

COBIT Control Objective		Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information	
AI5.1	Training	Staff trained in accordance with training plan		8.2	System planning and acceptance
AI5.2	Application software performance sizing	Resource forecasting	*ICT Infrastructure Management*, Appendix F, Conduct Outline Application Sizing Exercise	8.2	System planning and acceptance
AI5.3	Implementation plan	Site preparation, equipment acquisition and installation, user training	***Service Support*, Annex 9A, Rollout Plans** *Application Management*, The Application Management Life Cycle, 5.5.2 Planning the deployment *ICT Infrastructure Management,* Design and Planning, 2.8 The planning and implementation of new technology and services *ICT Infrastructure Management,* Deployment, 3.5.5 Roll-out phase *ICT Infrastructure Management*, Appendix F.13, Prepare an Outline Implementation Plan and Schedule		

AI5 Install and Accredit Systems (cont.)				
CobiT Control Objective		**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
AI5.4	System conversion	Conversion plan		
AI5.5	Data conversion	Collecting and verifying data, identifying and resolving errors, compatibility checks		
AI5.6	Testing strategies and plans	Sign-off by system owner and IT management	*Service Support*, Release Management, 9.6.1 Release planning *ICT Infrastructure Management*, Deployment, 3.5.4 Acceptance testing *Application Management,* The Application Management Life Cycle, 5.3.8 Testing the requirements	
AI5.7	Testing of changes	Independent test group, back-out plans, acceptance testing	*Service Support,* Release Management, 9.6.1 Release planning *Service Support,* Change Management, 8.5.9 Change building testing and implementation	8.1 Operational procedures and responsibilities 8.2 System planning and acceptance
AI5.8	Parallel/pilot testing criteria and performance	Pre-established plan and termination criteria	*Service Support,* Release Management, 9.11.3 Release Management *ICT Infrastructure Management,* Deployment, 3.5.4 Acceptance testing	
AI5.9	Final acceptance test	Formal evaluation and approval of test results	*Service Support,* Release Management, 9.6.3 Release acceptance *ICT Infrastructure Management,* Deployment, 3.5.4 Acceptance testing	
AI5.10	Security testing and accreditation	Security level of systems and residual risk		**8.2 System planning and acceptance** **10.5 Security in development and support processes** 4.1 Information security infrastructure
AI5.11	Operational test	Validation of operation under 'normal' conditions	*ICT Infrastructure Management,* Deployment, 3.5.4 Acceptance testing	4.1 Information security infrastructure
AI5.12	Promotion to production	Controlled handover, environment segregation	***Service Support,* Release Management, 9.6.6 Distribution and installation** *ICT Infrastructure Management,* Deployment, 3.5.2 Working environments	4.1 Information security infrastructure 5.1 Accountability for assets 8.1 Operational procedures and responsibilities 10.5 Security in development and support processes
AI5.13	Evaluation of meeting user requirements	Post-implementation review (PIR) to assess whether user needs are being met		
AI5.14	Management's post-implementation review	Benefits realisation		4.1 Information security infrastructure

COBIT Domain: Acquire and Implement
AI6 Manage Changes

Managing changes satisfies the business requirement minimising the likelihood of disruption, unauthorised alterations and errors. It is enabled by a management system that provides for the analysis, implementation and follow-up of all changes requested and made to the existing IT infrastructure.

COBIT Control Objective		Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
AI6.1	Change request initiation and control	Request for change, formal change management, change categories, priorities, status, urgency	***Service Support,*** **Change Management, 8.3 Basic concepts of change management** ***Service Support,*** **Change Management, 8.5 Activities**	4.1 Information security infrastructure 4.2 Security of third-party assets 6.3 Responding to security incidents and malfunctions 8.1 Operational procedures and responsibilities 10.5 Security in development and support processes
AI6.2	Impact assessment	Impact analysis (system and functionality), change assessment	***Service Support,*** **Change Management, 8.5.6 Impact and resource assessment**	8.1 Operational procedures and responsibilities 10.5 Security in development and support processes
AI6.3	Control of changes	Change management, software control and distribution, integrated configuration management, changes recorded and tracked	***Service Support,*** **Configuration Management, 7.9 Relations to other processes**	6.3 Responding to security incidents and malfunctions 7.2 Equipment security 10.5 Security in development and support processes
AI6.4	Emergency changes	Management assessment	***Service Support,*** **Change Management, 8.2 Scope of change management** ***Service Support,*** **Change Management, 8.3.2 Change advisory board**	8.1 Operational procedures and responsibilities 10.5 Security in development and support processes
AI6.5	Documentation and procedures	Change implementation, documentation updates	***Service Support,*** **Relationships Between Processes, 2.2 Change management** ***Service Support,*** **Change Management, 8.2 Scope of change management**	5.1 Accountability for assets 6.3 Responding to security incidents and malfunctions 10.5 Security in development and support processes 11.1 Aspects of business continuity management
AI6.6	Authorised maintenance	System access rights, risk avoidance		4.1 Information security infrastructure 4.2 Security of third-party assets 7.1 Secure areas 7.2 Equipment security
AI6.7	Software release policy	Release approval, sign-off, regression testing, handover	***Service Support,*** **Release Management, 9.3.2 Release policy and planning** ***Service Support,*** **Release Management, 9.5 Planning and implementation**	10.5 Security in development and support processes
AI6.8	Distribution of software	Internal controls, integrity, audit trails	***Service Support,*** **Release Management, 9.3.6 Definitive software library**	10.5 Security in development and support processes

CobiT Domain: Deliver and Support
DS1 Define and Manage Service Levels

Defining and managing service levels satisfies the business requirement of establishing a common understanding of the level of service required. It is enabled by service level agreements, which formalise the performance criteria against which the quantity and quality of service are measured.

CobiT Control Objective		Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
DS1.1	Service level agreement framework	Formal SLAs, service levels	***Service Delivery,* Service Level Management, 4.3.1 Initial planning activities**	
DS1.2	Aspects of service level agreements	Availability, reliability, performance, capacity for growth, levels of support, continuity planning, security and demand constraints	***Service Delivery,* Service Level Management, 4.6 SLA contents and key targets**	
DS1.3	Performance procedures	Governing relations (non-disclosure agreements, etc.), communications	***Service Delivery,* Service Level Management, 4.7 KPI and metrics for SLM efficiency and effectiveness**	
DS1.4	Monitoring and reporting	Service level manager, service performance criteria, corrective action	***Service Delivery,* Service Level Management, 4.3.2 Plan monitoring capabilities**	
DS1.5	Review of SLAs and contracts	Regular management reviews, underpinning contracts	***Service Delivery,* Service Level Management, 4.3.4 Underpinning contracts and operational level agreements (OLAs)**	
DS1.6	Chargeable items	Trade-offs, service levels vs. costs	***Service Delivery,* Financial Management for IT Services, 5.4.2 Charging policies**	
DS1.7	Service improvement programme	Agreed-upon, cost-justified improvements; service levels	***Service Delivery,* Service Level Management, 4.5.3 Service improvement programme**	

COBIT Domain: Deliver and Support
DS2 Manage Third-party Services

Managing third-party services satisfies the business requirement of ensuring that roles and responsibilities of third parties are clearly defined and adhered to and continue to satisfy requirements. It is enabled by service level agreements, which formalise the performance criteria against which the quantity and quality of service will be measured.

COBIT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
DS2.1 Supplier interfaces	Third-party services properly identified, interfaces defined	*The Business Perspective*, Supplier Relationship Management, 7.1 Types of supplier relationship	4.1 Information security infrastructure 4.2 Security of third-party access 11.1 Aspects of business continuity management
DS2.2 Owner relationships	Relationship management	*The Business Perspective*, Supplier Relationship Management, 7.2 Characterising relationships	4.2 Security of third-party access
DS2.3 Third-party contracts	Formal contracts defined and agreed upon before work starts	*The Business Perspective,* Supplier Relationship Management, 7.4 Contract management	4.2 Security of third-party access
DS2.4 Third-party qualifications	Capability assessment, due diligence		6.1 Security in job definition and resourcing
DS2.5 Outsourcing contracts	Facilities management contracts based on required processing levels, security, monitoring and contingency requirements	*The Business Perspective,* Supplier Relationship Management, 7.1.4 Outsourcing	4.3 Outsourcing 8.1 Operational procedures and responsibilities 10.5 Security in development and support processes
DS2.6 Continuity of services	Business risk, escrow contracts	*The Business Perspective*, Developing the Supplier Relationship 7.6.4 Ending a relationship	4.3 Outsourcing 10.5 Security in development and support processes
DS2.7 Security relationships	Nondisclosure agreements, liabilities		4.2 Security of third-party access 6.1 Security in job definition and resourcing 6.3 Responding to security incidents and malfunctions 8.1 Operational procedures and responsibilities 8.7 Exchanges of information and software 10.3 Cryptographic controls 10.5 Security in development and support processes
DS2.8 Monitoring	Adherence to contract agreements	***Service Delivery*, Service Level Management, 4.4.7 Establish monitoring capabilities** *The Business Perspective*, Supplier Relationship Management, 7.4 Contract management	4.3 Outsourcing 6.1 Security in job definition and resourcing 10.5 Security in development and support processes

CobiT Domain: Deliver and Support
DS3 Manage Performance and Capacity

Managing performance and capacity satisfies the business requirement ensuring that adequate capacity is available and best and optimal use is made of it to meet required performance needs. It is enabled by data collection, analysis and reporting on resource performance, application sizing and workload demand.

CobiT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
DS3.1 Availability and performance requirements	Business needs regarding availability and performance	***Service Delivery*, Availability Management, 8.5.1 Determining availability requirements** ***Service Delivery*, Capacity Management, 6.2.1 Business capacity management**	8.2 System planning and acceptance
DS3.2 Availability plan	Monitor and control availability of IS	***Service Delivery*, Availability Management, 8.5 Availability planning**	
DS3.3 Monitoring and reporting	Monitor performance of IT resources, exception reporting	***Service Delivery*, Availability Management, 8.7 Availability measurement and reporting** ***Service Delivery*, Capacity Management, 6.3.1 Monitoring**	6.3 Responding to security incidents and malfunctions 8.2 System planning and acceptance 8.4 Housekeeping 9.7 Monitoring system access and use
DS3.4 Modelling tools	Current systems model, actual workload, prediction of capacity, configuration reliability, performance, availability	***Service Delivery*, Availability Management, 8.5.3 Designing for availability** ***Service Delivery*, Capacity Management, 6.3.7 Modelling**	8.2 System planning and acceptance
DS3.5 Proactive performance management	Forecasting capability, proactive problem management, problem analysis	***Service Delivery*, Capacity Management, 6.2 The capacity management process** ***Service Delivery*, Capacity Management, 6.3.6 Demand management** ***Service Support*, Problem Management, 6.8 Proactive problem management**	8.2 System planning and acceptance 8.4 Housekeeping
DS3.6 Workload forecasting	Identify trends, capacity plan	***Service Delivery*, Capacity Management, 6.3.2 Analysis** ***Service Delivery*, Capacity Management, 6.3.6 Demand management** ***Service Delivery*, Capacity Management, 6.3.9 Production of the capacity plan**	8.2 System planning and acceptance
DS3.7 Capacity management of resources	Review of performance, cost-justifiable capacity, agreed-upon workloads		8.2 System planning and acceptance
DS3.8 Resources availability	Availability requirements, fault tolerance, prioritisation, resource allocation	***Service Delivery*, Availability Management, 8.3 The availability management process**	8.5 Network management
DS3.9 Resources schedule	Timely acquisition of capacity, resilience, contingency, workloads, storage plans	***Service Delivery*, Capacity Management, 6.2 The capacity management process**	8.2 System planning and acceptance

COBIT Domain: Deliver and Support
DS4 Ensure Continuous Service

Ensuring continuous service satisfies the business requirement of making sure IT services are available as required and ensuring that there is a minimum business impact in the event of a major disruption. It is enabled by service level agreements, which formalise the performance criteria against which the quantity and quality of service will be measured.

COBIT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
DS4.1 IT continuity framework	Risk-based approach, rules and structure, approval procedures	***Service Delivery,* IT Service Continuity Management, 7.3 The business continuity life cycle**	**4.1 Information security infrastructure** **11.1 Aspects of business continuity management**
DS4.2 IT continuity plan strategy and philosophy	Alignment with overall business continuity plan	***Service Delivery,* IT Service Continuity Management, 7.3 The business continuity life cycle**	**11.1 Aspects of business continuity management**
DS4.3 IT continuity plan contents	Emergency, response and recovery procedures, co-ordination and communication, critical information	***Service Delivery,* IT Service Continuity Management, 7.3 Service continuity management generic recovery plan**	**11.1 Aspects of business continuity management**
DS4.4 Minimising IT continuity requirements	Requirements relating to personnel and other resources		**4.1 Information security infrastructure**
DS4.5 Maintaining the IT continuity plan	Change control to reflect changing business requirements	***The Business Perspective,* Understanding the Business Viewpoint, 5.7 Business continuity**	**11.1 Aspects of business continuity management**
DS4.6 Testing the IT continuity plan	Regular testing, implementing action plan	***Service Delivery,* IT Service Continuity Management, 7.3.4 Stage 4—Operational management**	**11.1 Aspects of business continuity management**
DS4.7 IT continuity plan training	Disaster recovery training	***Service Delivery,* IT Service Continuity Management, 7.3.3 Stage 3—Implementation**	**11.1 Aspects of business continuity management**
DS4.8 IT continuity plan distribution	Safeguard against unauthorised disclosure	***Service Delivery,* IT Service Continuity Management, 7.3.4 Stage 4—Operational management**	**7.1 Secure areas**
DS4.9 User department alternative processing backup procedures	Continuity methodology		**11.1 Aspects of business continuity management**
DS4.10 Critical IT resources	Critical resources identified	***Service Delivery,* IT Service Continuity Management, 7.3 The business continuity life cycle**	**11.1 Aspects of business continuity management** 4.1 Information security infrastructure
DS4.11 Backup site and hardware	Alternatives identified, contracts for service provision	***Service Delivery,* IT Service Continuity Management, 7.3.2 Stage 2—Requirements analysis and strategy definition**	**7.2 Equipment security** **11.1 Aspects of business continuity management**
DS4.12 Offsite backup storage	Support recovery and business continuity plans, periodic assessment	*Service Delivery,* IT Service Continuity Management, 7.3.2 Stage 2—Requirements analysis and strategy definition	**7.1 Secure areas** **7.2 Equipment security**
DS4.13 Wrap-up procedures	Assessing adequacy of plan, plan updates	***Service Delivery,* IT Service Continuity Management, 7.3.4 Stage 4—Operational management**	

CobiT Domain: Deliver and Support
DS5 Ensure Systems Security

Ensuring systems security satisfies the business requirement of safeguarding information against unauthorised use, disclosure, or modification, damage or loss. It is enabled by logical access controls, which ensure that access to systems, data and programmes is restricted to authorised users.

CobiT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
DS5.1 Manage security measures	Translating risk assessment into IT security plans, implementing plan	*Security Management*, Fundamental of Information Security, 2.3.1.2 Plan *Security Management*, Security Management Measures, 4.1 Control	**3.1 Information security policy** **4.1 Information security infrastructure** **7.1 Secure areas** **8.1 Operational procedures and responsibilities** **8.5 Network management** **8.6 Media handling and security** **9.1 Business requirement for access control** **9.3 User responsibilities** **9. Network access control** **9.6 Application access control** **10.3 Cryptographic controls**
DS5.2 Identification, authentication and access	Logical access to and use of resources restricted to authorised personnel	*Security Management*, Security Management Measures, 4.2.4 Access control	**4.2 Security of third-party access** **9.2 User access management** **9.4 Network access control** **9.5 Operating system access control**
DS5.3 Security of online access to data	Access security control	*Security Management*, Security Management Measures, 4.2.2 Access control	**4.2 Security of third-party access** **9.6 Application access control**
DS5.4 User account management	Access privileges, security of third-party access	*Security Management,* Security Management Measures, 4.2 Implement	**4.2 Security of third-party access** **4.1 Information security infrastructure** **6.1 Security in job definition and resourcing** **7.1 Secure areas** **8.1 Operational procedures and responsibilitie** **8.6 Media handling and security** **9.1 Business requirement for access control** **9.2 User access management** **9.6 Application access control** **10.4 Security of system files**
DS5.5 Management review of user accounts	Review and confirm access rights	*Security Management*, Security Management Measures, 4.3 Audit and evaluate security reviews of IT systems	**8.6 Media handling and security** **9.2 User access management**
DS5.6 User control of user accounts	Information mechanisms to oversee accounts	*Security Management*, Security Management Measures, 4.2 Implement	**9.3 User responsibilities** **9.5 Operating system access control**
DS5.7 Security surveillance	IT security administration, security violation reports	*Security Management*, Security Management Measures, 4.2 Implement	**3.1 Information security policy** **9.5 Operating system access control** **9.7 Monitoring system access and use** **10.4 Security of system files** **12.1 Compliance with legal requirements**

DS5 Ensure Systems Security (cont.)

COBIT Control Objective		**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
DS5.8	Data classification	Data sensitivity, data owner, disposition and sharing of data	*Security Management*, Security Management Measures, 4.2 Implementation	**4.1 Information security infrastructure** **5. Information classification** **9.1 Business requirement for access control** **10.1 Security requirements of systems** **12.1 Compliance with legal requirements**
DS5.9	Central identification and access rights management	Identity of system and data ownership established; consistency and efficiency of global access control	*Security Management,* Security Management Measures, 4.2 Implementation	
DS5.10	Violation and security activity reports	Security activity logs, review and escalation	*Security Management*, Security Management Measures, 4.5 Report	**4.1 Information security infrastructure** **6.3 Responding to security incidents and malfunctions** **9.1 Business requirement for access control** **9.7 Monitoring system access and use** **12.2 Reviews of security policy and technical compliance**
DS5.11	Incident handling	Incident management of security incidents	*Security Management,* ITIL and Security Management, 3.3.2 Incident control/help desk	**3.1 Information security policy** **4.1 Information security infrastructure** **6.3 Responding to security incidents and malfunctions** **8.1 Operational procedures and responsibilities** **9.5 Operating system access control**
DS5.12	Reaccreditation	Formally approved security levels and acceptance of residual risk	*Security Management,* Security Management Measures, 4.3 Audit and evaluate *Security Management,* Security Management Measures, 4.4 Maintain	**4.1 Information security infrastructure** **12.2 Reviews of security policy and technical compliance**
DS5.13	Counterparty trust	Authenticity, passwords, tokens, cryptographic keys	*Security Management,* Security Management Measures, 4.2 Implementation	**8.7 Exchanges of information and software**
DS5.14	Transaction authorisation	Validity of user identify	*Security Management*, Security Management Measures, 4.2 Implementation	**8.7 Exchanges of information and software** **10.3 Cryptographic controls**
DS5.15	Nonrepudiation	Digital signatures, time-stamping, trusted third parties	*Security Management,* Security Management Measures, 4.2 Implementation	**10.2 Security in application systems** **10.3 Cryptographic controls**
DS5.16	Trusted path	Encryption	*Security Management,* Security Management Measures, 4.2 Implementation	**8.5 Network management** **9.4 Network access control** **10.3 Cryptographic controls**
DS5.17	Protection of security functions	Protection against tampering; nondisclosure of secret keys, security design	*Security Management,* Security Management Measures, 4.2 Implementation	**7.1 Secure areas** **8.6 Media handling and security** 10.3 Cryptographic controls
DS5.18	Cryptographic key management	Protocols for generation, change, revocation	*Security Management,* Security Management Measures, 4.2 Implementation	**10.3 Cryptographic controls**

DS5 Ensure Systems Security (cont.)

CobiT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
DS5.19 Malicious software prevention, detection and correction	Viruses, Trojan horses	*Security Management,* Security Management Measures, 4.2 Implementation	**6.3 Responding to security incidents and malfunctions** **8.3 Protection against malicious software**
DS5.20 Firewall architectures and connections with public networks	Denial of service	*Security Management,* Security Management Measures, 4.2 Implementation	**8.5 Network management** **9.4 Network access control**
DS5.21 Protection of electronic value	Protection of authentication devices	*Security Management*, Security Management Measures, 4.2 Implementation	**5.2 Information classification**

CobiT Domain: Deliver and Support
DS6 Identify and Attribute Costs

Identifying and allocating costs satisfies the business requirement of ensuring a correct awareness of the costs attributable to IT services. It is enabled by a cost accounting system, which ensures that costs are recorded, calculated and allocated to the required level of detail and to the appropriate service offering.

CobiT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
DS6.1 Chargeable items	Identified, measurable and predictable chargeable items; user's ability to control	***Service Delivery,*** **Financial Management for IT Services*,*** **5.4 Developing the charging system**	
DS6.2 Costing procedures	Management information on cost, cost variance forecast vs. actual, cost monitoring	***Service Delivery,*** **Financial Management for IT Services, 5.3 Developing the IT accounting system**	
DS6.3 User billing and chargeback procedures	Proper use of resources, rates reflecting associated costs	***Service Delivery,*** **Financial Management for IT Services, 5.6 Implementation**	

CobiT Domain: Deliver and Support
DS7 Educate and Train Users

Educating and training users satisfies the business requirement of ensuring that users are making effective use of technology and are aware of the risks and responsibilities involved. It is enabled by service level agreements, which formalise the performance criteria against which the quantity and quality of service will be measured.

CobiT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
DS7.1 Identification of training needs	Training curriculum for each group of employees	*Service Support,* Problem Management, 6.8 Proactive problem management	3.1 Information security policy 6.2 User training 9.3 User responsibilities
DS7.2 Training organisation	Identify and appoint trainers, training schedule		4.1 Information security infrastructure
DS7.3 Security principles and awareness training	Security practices	*Security Management*, Security Management Measures, 4.2 Implementation	**6.2 User training** **6.3 Responding to security incidents and malfunctions** **8.3 Protection against malicious software** **9.3 User responsibilities** 3.1 Information security policy 4.1 Information security infrastructure 9.8 Mobile computing and teleworking 12.1 Compliance with legal requirements

COBIT Domain: Deliver and Support **DS8 Assist and Advise Customers**			
Assisting and advising customers satisfies the business requirement of ensuring that any problem experienced by the user is appropriately resolved. It is enabled by a help desk facility that provides first-line support and advice.			
COBIT Control Objective	**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
DS8.1 Help desk	User support, close interaction with problem management	***Service Support,* Service Desk, 4.8 Service desk processes and procedures**	6.3 Responding to security incidents and malfunctions
DS8.2 Registration of customer queries	Incident registration	***Service Support,* Incident Management, 5.6.2 Classification and initial support**	6.3 Responding to security incidents and malfunctions
DS8.3 Customer query escalation	Incident escalation		6.3 Responding to security incidents and malfunctions
DS8.4 Monitoring of clearance	Timely monitoring, outstanding incident investigation	***Service Support,* Incident Management, 5.4.3 Investigation and diagnosis** ***Service Support,* Incident Management, 5.6.6 Ownership, monitoring, training and communication**	6.3 Responding to security incidents and malfunctions
DS8.5 Trend analysis and reporting	Incident resolution, response times, trend identification	***Service Support,* Service Desk, 4.9 Incident reporting and review** ***Service Support,* Problem Management, 6.8 Proactive problem management**	

COBIT Domain: Deliver and Support
DS9 Manage the Configuration

Managing the configuration satisfies the business requirement of accounting for all IT components, preventing unauthorised alterations, verifying physical existence and providing a basis for sound change management. It is enabled by controls that identify and record all IT assets and their physical location, and a regular verification programme that confirms their existence.

COBIT Control Objective		Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
DS9.1	Configuration recording	Configuration identifications (CIs) recorded, inventory, change history, configuration management database review	***Service Support,* Configuration Management, 7.6.2 Configuration identification**	5.1 Accountability for assets 8.1 Operational procedures and responsibilities
DS9.2	Configuration baseline	Configuration baselines established and used in change	***Service Support,* Configuration Management, 7.3.6 Configuration baseline**	8.1 Operational procedures and responsibilities
DS9.3	Status accounting	CI records reflect status, history of change	***Service Support,* Configuration Management, Annex 7C, Suggested CI Attributes** ***Service Support,* Configuration Management, 7.6.4 Configuration status accounting**	5.1 Accountability for assets 7.3 General controls
DS9.4	Configuration control	Consistency in CI recording	***Service Support,* Configuration Management, 7.6.3 Control of CIs**	
DS9.5	Unauthorised software	Policy and controls, virus detection and remedy	***Service Support,* Release Management, 9.3.6 Definitive software library**	**8.3 Protection against malicious software** 12.1 Compliance with legal requirements
DS9.6	Software storage	Definitive software library, environment control	***Service Support,* Release Management, 9.3.6 Definitive software library**	8.1 Operational procedures and responsibilities 10.4 Security of system files
DS9.7	Configuration management procedures	Critical components identified, demand management	***Service Support,* Configuration Management, 7.11.1 Level of control** ***Service Delivery,* Availability Management, 8.9.1 Component failure impact analysis**	5.1 Accountability for assets 10.4 Security of system files
DS9.8	Software accountability	Identification, licencing, library management, audit trails, version numbering	***Service Support,* Configuration Management, 7.3.8 Software and document libraries** ***Service Support,* Configuration Management, 7.3.10 Licence management**	10.4 Security of system files

COBIT Domain: Deliver and Support
DS10 Manage Problems and Incidents

Managing problems and incidents satisfies the business requirement of ensuring that problems and incidents are resolved and the cause is investigated to prevent any recurrence. It is enabled by a problem management system that records and traces the progress of all incidents.

COBIT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
DS10.1 Problem management system	Incidents, problems and errors recorded, analysed and resolved	***Service Support,*** **4. The Service Desk** ***Service Support,*** **5. Incident Management** ***Service Support*****, 6. Problem Management** ***Service Support,*** **Incident Management*****,*** **5.3.5 Relationship between incidents, problems and known errors**	**6.3 Responding to security incidents and malfunctions** **8.1 Operational procedures and responsibilities**
DS10.2 Problem escalation	Prioritisation, escalation, IT continuity	***Service Support,*** **The Service Desk, 4.4.4 Escalation management** ***Service Support,*** **Incident Management*****,*** **5.3.3 Functional vs. hierarchical escalation** ***Service Support,*** **Incident Management*****,*** **5.6.6 Ownership, monitoring, tracking and communication**	4.1 Information security infrastructure 8.1 Operational procedures and responsibilities 11.1 Aspects of business continuity management
DS10.3 Problem tracking and audit trail	Audit trail, underlying cause, problem resolution requiring change	***Service Support,*** **Problem Management*****,*** **6.7.5 Problem/error resolution monitoring**	6.3 Responding to security incidents and malfunctions 7.2 Equipment security 8.1 Operational procedures and responsibilities
DS10.4 Emergency and temporary access authorisations	Documented approach, security management		**4.2 Security of third-party access** 4.1 Information security infrastructure 7.2 Equipment security 8.1 Operational procedures and responsibilities 9.1 Business requirement for access control
DS10.5 Emergency processing priorities	Management approval		4.1 Information security infrastructure 11.1 Aspects of business continuity management

CobiT Domain: Deliver and Support
DS11 Manage Data

Managing data satisfies the business requirement of ensuring that data remain complete, accurate and valid during their input, update and storage. It is enabled by an effective combination of application and general controls over the IT operations.

CobiT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
DS11.1 Data preparation procedures	Input form design, minimising errors and omissions, error handling procedures		
DS11.2 Source document authorisation procedures	Document preparation, segregation of duties		
DS11.3 Source document data collection	Completeness and accuracy		
DS11.4 Source document error handling	Detection, reporting and correction		
DS11.5 Source document retention	Legal requirements, retrieval and reconstruction mechanisms		12.1 Compliance with legal requirements
DS11.6 Data input authorisation procedures	Data input by authorised staff		**9.6 Application access control** **10.2 Security in application systems** 8.6 Media handling and security
DS11.7 Accuracy, completeness and authorisation checks	Data input validation		8.6 Media handling and security 10.2 Security in application systems
DS11.8 Data input error handling	Correction and resubmission of erroneous data		10.2 Security in application systems
DS11.9 Data processing integrity	Routine verification, update controls		10.2 Security in application systems
DS11.10 Data processing validation and editing	Vital decisions approved		10.2 Security in application systems
DS11.11 Data processing error handling	Identification of erroneous transactions		8.1 Operational procedures and responsibilities 10.2 Security in application systems
DS11.12 Output handling and retention	Prevention of misuse		**8.6 Media handling and security** 5.2 Information classification 8.1 Operational procedures and responsibilities 9.6 Application access control
DS11.13 Output distribution	Written procedures for distribution		8.6 Media handling and security 9.6 Application access control
DS11.14 Output balancing and reconciliation	Output routinely balanced against relevant controls		8.6 Media handling and security 10.2 Security in application systems
DS11.15 Output review and error handling	Procedures to assure accuracy of output		10.2 Security in application systems
DS11.16 Security provision for output reports	Security of output awaiting distribution		**8.6 Media handling and security** 5.2 Information classification 7.3 General controls 8.7 Exchanges of information and software
DS11.17 Protection of sensitive information during transmission and transport	Misaddressing, unauthorised access		**8.7 Exchanges of information and software** 4.1 Information security infrastructure 4.2 Security of third-party access 5.2 Information classification 8.5 Network management

DS11 Manage Data (cont.)			
COBIT Control Objective	**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
DS11.18 Protection of disposed sensitive information	Data marking, data cannot be retrieved		7.2 Equipment security
DS11.19 Storage management	Data storage	*ICT Infrastructure Management*, Annex 4D, Back-up and Storage	5.2 Information classification 8.6 Media handling and security
DS11.20 Retention periods and storage terms	All documents, applications and keys		8.4 Housekeeping 12.1 Compliance with legal requirements
DS11.21 Media library management system	Systematic inventory	*ICT Infrastructure Management,* Operations, 4.5 The processes and deliverables of operations	5.2 Information classification 8.6 Media handling and security
DS11.22 Media library management responsibilities	Housekeeping procedures	*ICT Infrastructure Management*, Operations, 4.5 The processes and deliverables of operations	5.2 Information classification 8.6 Media handling and security 8.7 Exchanges of information and software
DS11.23 Backup and restoration	Backup and restoration strategy	*ICT Infrastructure Management,* Annex 4D, Back-up and Storage	8.4 Housekeeping
DS11.24 Backup jobs	Usability of backups verified	*ICT Infrastructure Management,* Annex 4D, Back-up and Storage	8.4 Housekeeping
DS11.25 Backup storage	Onsite and offsite storage	*ICT Infrastructure Management,* Annex 4D, Back-up and Storage	8.4 Housekeeping 12.1 Compliance with legal requirements
DS11.26 Archiving	Archive meeting legal and business requirements		12.1 Compliance with legal requirements
DS11.27 Protection of sensitive messages	Data transmission		**8.7 Exchanges of information and software** **10.3 Cryptographic controls** 4.1 Information security infrastructure 4.2 Security of third-party access 5.2 Information classification
DS11.28 Authentication and integrity	Authentication checks		**8.7 Exchanges of information and software** **10.3 Cryptographic controls** 4.2 Security of third-party access 9.4 Network access control 10.2 Security in application systems
DS11.29 Electronic transaction integrity	Integrity and authenticity		4.2 Security of third-party access 8.7 Exchanges of information and software 10.2 Security in application systems
DS11.30 Continued integrity of stored data	Media checks, correctness of data		8.4 Housekeeping 12.1 Compliance with legal requirements

COBIT Domain: Deliver and Support
DS12 Manage Facilities

Managing facilities satisfies the business requirement of providing a suitable physical surrounding that protects the IT equipment and people against man-made and natural hazards. It is enabled by the installation of suitable environmental and physical controls, which are regularly reviewed for proper functioning.

COBIT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
DS12.1 Physical security	Access control, offsite storage, backups, protection measures		**7.1 Secure areas** **7.2 Equipment security** **7.3 General controls** **8.5 Network management** **8.6 Media handling and security** 4.1 Information security infrastructure 4.2 Security of third-party access 6.1 Security in job definition and resourcing 8.1 Operational procedures and responsibilities 9.3 User responsibilities
DS12.2 Low profile of the IT site	Physical identification		**7.1 Secure areas**
DS12.3 Visitor escort	Visitor logs		**7.1 Secure areas**
DS12.4 Personnel health and safety	Health and safety practice		7.1 Secure areas 8.1 Operational procedures and responsibilities
DS12.5 Protection against environmental factors	Monitor and control environment		7.1 Secure areas 7.2 Equipment security
DS12.6 Uninterruptible power supply	Criticality of applications, power failure and fluctuations	*ICT Infrastructure Management,* Appendix D6, Office Environments *Service Delivery,* Availability Management, 8.3 The availability management process	7.2 Equipment security

COBIT Domain: Deliver and Support **DS13 Manage Operations**			
Managing operations satisfies the business requirement of ensuring that important IT support functions are performed regularly and in an orderly fashion. It is enabled by a schedule of support activities that recorded and cleared for the accomplishment of all activities.			
COBIT Control Objective	**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
DS13.1 Processing operations procedures and instructions manual	IT solution and platform operational effectiveness	***ICT Infrastructure Management*, Technical Support, 5.4.1 The technical support processes**	8.1 Operational procedures and responsibilities
DS13.2 Start-up process and other operations documentation	Documentation, periodic testing, awareness	***ICT Infrastructure Management*, Operations, 4.4.6 Management of the supporting operational processes**	8.1 Operational procedures and responsibilities
DS13.3 Job scheduling	Maximising throughput and utilisation to meet SLAs	***ICT Infrastructure Management*, Operations, 4.6.2 The tools—scheduling tools** ***ICT Infrastructure Management*, Operations, 4.4.3 Workload, output, resilience testing management and scheduling**	8.1 Operational procedures and responsibilities 8.4 Housekeeping
DS13.4 Departures from standard job schedules	Management approvals		**6.3 Responding to security incidents and malfunctions** 7.2 Equipment security 8.1 Operational procedures and responsibilities
DS13.5 Processing continuity	Formal handover of activities, status updates and reports		
DS13.6 Operations logs	Reconstruction, review of time sequences, supporting processes	***ICT Infrastructure Management*, Operations, 4.4.1 Management of all ICT infrastructure events**	8.1 Operational procedures and responsibilities 8.4 Housekeeping
DS13.7 Safeguard special forms and output devices	Physical safeguards, sensitive devices, accounting, protection	***ICT Infrastructure Management*, Operations, 4.4.5 Management and control of all aspects of ICT operational security**	**8.6 Media handling and security** 5.2 Information classification 8.1 Operational procedures and responsibilities 12.1 Compliance with legal requirements
DS13.8 Remote operations	Specific procedures for connection/disconnection of links		4.2 Security of third-party access 8.5 Network management 9.4 Network access control

COBIT Domain: Monitor
M1 Monitor the Processes

Monitoring the process satisfies the business requirement of ensuring the achievement of the performance objectives set for the IT processes. It is enabled by the definition of relevant performance indicators, the systematic and timely reporting of performance, and prompt acting upon deviation.

COBIT Control Objective		Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
M1.1	Collecting monitoring data	benchmarks, proprietary nature and integrity of data	*ICT Infrastructure Management,* Operations, 4.6.1 The techniques *Service Delivery,* Service Level Management, 4.4.7 Establish monitoring capabilities	12.1 Compliance with legal requirements
M1.2	Assessing performance	targets, continual assessment basis	*ICT Infrastructure Management*, Operations, 4.6.1 The techniques *The Business Perspective,* Business/IS Alignment, 4.5.2 Benchmarking *Planning to Implement,* How Do We Check our Milestones Have Been Reached?, 6.1 Critical success factors and key performance indicators *Planning to Implement,* How Do We Keep the Momentum Going?, 7.4 Ongoing monitoring and process reviews *Service Delivery,* Service Level Management, 4.3.3 Establish initial perception of the services	
M1.3	Assessing customer	satisfaction service shortfalls identified	***Service Support,* The Service Desk, 4.4.8 Customer satisfaction analysis and surveys** ***Service Delivery*, Service Level Management, 4.5.2 Service review meetings**	
M1.4	Management reporting	reports, risk mitigation	*The Business Perspective,* Managing the Provision of Service, 6.3 Service reporting *Service Delivery,* Service Level Management, 4.4.9 Define reporting and review procedures *Service Delivery,* Service Level Management, 4.5.1 Monitoring and reporting	

CobiT Domain: Monitor M2 Assess Internal Control Adequacy			
Assessing internal control adequacy satisfies the business requirement of ensuring the achievement of the internal control objectives set for the IT processes. It is enabled by the commitment to monitoring internal controls, assessing their effectiveness and reporting on them on a regular basis.			
CobiT Control Objective	**Key Areas**	**ITIL Supporting Information**	**ISO 17799 Supporting Information**
M2.1 Internal control monitoring	Comparisons, reconciliations, deviation analysis and corrective action, reporting and communications		8.1 Operational procedures and responsibilities 8.5 Network management 12.1 Compliance with legal requirements
M2.2 Timely operation of internal controls	Controls operate promptly, highlighting errors and inconsistencies		3.1 Information security policy 4.1 Information security infrastructure 6.3 Responding to security incidents and malfunctions 8.1 Operational procedures and responsibilities 8.5 Network management
M2.3 Internal control level reporting	Exception reporting, reporting needs analysis		4.1 Information security infrastructure 6.3 Responding to security incidents and malfunctions 8.1 Operational procedures and responsibilities 8.4 Housekeeping
M2.4 Operational security and internal control assurance	Self-assessment and independent audit, identifying vulnerabilities and security problems		3.1 Information security policy 4.1 Information security infrastructure 6.3 Responding to security incidents and malfunctions 8.4 Housekeeping 12.2 Reviews of security policy and technical compliance

CobiT Domain: Monitor
M3 Obtain Independent Assurance

Obtaining independent assurance satisfies the business requirement of increasing confidence and trust amongst the organisation, customers and third-party providers. It is enabled by independent assurance reviews carried out at regular intervals.

CobiT Control Objective	Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
M3.1 Independent security and internal control (certification/ accreditation of IT services)	Security controls checked prior to implementation		**4.1 Information security infrastructure** **12.2 Reviews of security policy and technical compliance**
M3.2 Independent security and internal control (certification/ accreditation of third-party service providers)	Security controls of third parties checked		
M3.3 Independent effectiveness evaluation of IT services	Routine, independent checks of effectiveness		
M3.4 Independent effectiveness evaluation of third-party service providers	Routine, independent checks of effectiveness		
M3.5 Independent assurance of compliance with laws and regulatory requirements and contractual commitments	Routine, independent compliance checks		4.1 Information security infrastructure
M3.6 Independent assurance of compliance with laws and regulatory requirements and contractual commitments by third-party service providers	Routine, independent compliance checks		
M3.7 Competence of independent assurance function	Technical competence, skills and knowledge for reviews recognised		4.1 Information security infrastructure 12.2 Reviews of security policy and technical compliance
M3.8 Proactive audit involvement	IT service solution audit and review		

COBIT Domain: Monitor M4 Provide for Independent Audit				
Providing for independent audit satisfies the business requirement of increasing confidence levels and benefiting from best practice advice. It is enabled by independent audits carried out at regular intervals.				
COBIT Control Objective		Key Areas	ITIL Supporting Information	ISO 17799 Supporting Information
M4.1	Audit charter	Audit function responsibilities, charter review, accountability of audit function		12.3 System audit considerations
M4.2	Independence	Independence of audit function		
M4.3	Professional ethics and standards	Professional codes, auditing standards		
M4.4	Competence	Technical competence, skills and knowledge, professional development		
M4.5	Planning	Audit plan and priorities, audit objectives		
M4.6	Performance of audit work	Audit objectives set and achievement supervise, appropriate analysis and interpretation of evidence		
M4.7	Reporting	Audit report with specified scope and objectives; findings, conclusion and recommendations		
M4.8	Follow-up activities	Resolution of audit comments, action plan and implementation		

Appendix II—Mapping COBIT Control Objectives to ITIL

This mapping shows the reverse relationship between the sections of ITIL and the COBIT control objectives. It is hopeful that this mapping will make COBIT more accessable to ITIL practioners.

Note that for the purposes of this mapping the primary control objective(s) in COBIT has been identified although there may be other objectives in COBIT that can be related. In most cases one objective has been selected, but in some cases more have been chosen where they are considered helpful.

This mapping is not intended to be definitive or prescriptive; it is only a guide. Links are shown only at the high level, pointing to the relevant section in the other documents.

ITGI is carrying out detailed research into the mapping between COBIT and other standards and best practices. More information can be found at *www.isaca.org/research*.

As part of the current ITIL refresh project, OGC and its partners will be examining the relationship between ITIL and other best practices and standards, and intends to make supporting material available online during the next 18 months. For up-to-date information on the progress of the ITIL refresh project, please see *www.itil.co.uk*.

Mapping ITIL to COBIT			
ITIL	**COBIT**		
Process	**Process**	**Detailed Control Objective**	
1. Business Perspective			
Understand business context (value chain and governance framework)	PO6	PO6.1	Positive information control environment
Develop business relationships and establish communications plan	PO6	PO6.3	Communication of organisational policies
Establish service portfolio	DS1	DS1.1	Service level agreement framework
Analyse business requirements and ascertain future business direction	PO1	PO1.3	IT long-range planning approach and structure
Develop IS strategy	PO1	PO1.2	IT long-range plan
Review business and IS strategic alignment	PO1	PO1.2	IT long-range plan
Develop service plans	AI1	AI1.1	Definition of information requirements
Formalise supplier relationships	DS2	DS2.1	Supplier interfaces
Manage service provision	AI1	AI1.4	Third-party service requirements
Manage contracts	DS2	DS2.3	Third-party contracts
Establish service reporting policy	PO4	PO4.3	Review of organisational achievements
Manage performance and realise business benefits	M1	M1.2	Assessing performance
2. Planning to Implement Service Management			
Analyse business needs	PO6	PO6.1	Positive information control environment
Create a service management vision	DS1 DS2	All All	Define and manage service levels Manage third-party services
Establish appropriate policies and standards	PO6	PO6.3	Communication of organisation policies
Evaluate current organisational position—benchmarking/ maturity assessment	M1	M1.2	Assessing performance
Undertake gap analysis and determine action plans	M1	M1.2	Assessing performance
Determine CSFs and KPIs	M1	M1.2	Assessing performance
Manage organisational change	PO4	PO4.4	Roles and responsibilities
Report on delivery—progress monitoring and process improvements	M1	M1.4	Management reporting
Review benefits and revise service improvement plans	DS1	DS1.7	Service improvement programme
3. ICT Infrastructure Management			
Maintain ICT business plans	PO1	PO1.4	IT long-range plan changes
Review current position and determine ICT strategies	PO3	PO3.1	Technological infrastructure planning

Mapping ITIL to CobiT

ITIL	CobiT		
Process	**Process**	**Detailed Control Objective**	
3. ICT Infrastructure Management *cont.*			
Establish ICT standards and policies	PO3	PO3.5	Technology standards
Maintain ICT architectural blueprints	PO3	PO3.1	Technological infrastructure planning
Design and implement technical migration plans	PO3	PO3.1	Technological infrastructure planning
Review programme against strategy and business plans	PO4	PO4.1	IT planning or steering committee
Develop and ratify ICT solutions	AI	All	Acquire and implement
Build appropriate working environments	AI5	AI5.12	Promotion to production
Test ICT solutions	AI5	AI5.6	Testing strategies and plans
Define appropriate roll-out strategy	AI5	AI5.3	Implementation plan
Roll-out ICT solutions	AI5	AI5.12	Promotion to production
Undertake post-project evaluation and reviews	AI5	AI5.14	Management's post-implementation review
Establish operational controls and management of services	DS13	DS13.1	Processing operations procedures and instructions manual
Manage ICT infrastructure events	DS13	All	Manage operations
Workload management and scheduling	DS13	DS13.3	Job scheduling
Manage storage, backup, and recovery operations	DS12	DS12.1	Physical security
Maintain operation documentation and procedures	DS13	DS13.1	Processing operations procedures and instructions manual
Manage and control operational security	M2	M2.4	Operational security and internal control assurance
Undertake ICT research studies and evaluations	PO3	PO3.2	Monitor future trends and regulations
Create and maintain working environments	AI5	AI5.12	Promotion to production
Provide technical guidance and specialist support	DS8 DS10	All All	Assist and advise customers Manage problems and incidents
4. Application Management			
Develop models that demonstrate business and IS strategic alignment	PO2	PO2.1	Information architecture model
Assess IT capabilities	PO6	PO6.4	Policy implementation resources
Ascertain the delivery strategy	AI1	AI1.2	Formulation of alternative courses of action
Align delivery strategy with business drivers and organisational capabilities	AI1	AI1.3	Formulation of acquisition strategy
Prepare to deliver	AI1	AI1.13	Procurement control
Determine application life cycle	AI2	AI2.1	Design methods
Align application management and service management	AI2	AI2.13	Availability as a key design factor
Plan deployment	AI5	AI5.3	Implementation plan
Plan handover and support	AI5	AI5.3	Implementation plan
Review application portfolio	AI2	AI2.17	Reassessment of system design
5. Service Level Management			
Undertake service planning	DS1	DS1.2	Aspects of service level agreements
Produce service catalogue	DS1	DS1.1	Service level agreement framework
Establish service level requirements	DS1	DS1.2	Aspects of service level agreements
Negotiate SLAs	DS1	DS1.1	Service level agreement framework
Manage customer expectations	DS8	DS8.1	Help desk
Establish service monitoring capability	DS1	DS1.4	Monitoring and reporting
Review underpinning contracts and OLAs	DS1	DS1.5	Review of service level agreements and contracts
Raise awareness and determine reporting needs	DS1	DS1.4	Monitoring and reporting
Schedule service reviews	DS1	DS1.5	Review of service level agreements and contracts
Initiate and manage service improvement programme	DS1	DS1.7	Service improvement programme
6. Financial Management for IT Services			
Prepare budgets to support strategic and tactical plans	PO5	PO5.1	Annual IT operating budget
Negotiate expenditure plans and agree investment programmes	PO5	PO5.1	Annual IT operating budget
Develop an IT accounting system	DS6	DS6.2	Costing procedures
Undertake investment appraisals	AI1	AI1.6	Economic feasibility study
Develop a charging system	DS6	DS6.1	Chargeable items

Mapping ITIL to COBIT			
ITIL	**COBIT**		
Process	**Process**	**Detailed Control Objective**	
6. Financial Management for IT Services *cont.*			
Implement IT accounting and charging systems	DS6	DS6.2	Costing procedures
Study variances	PO5	PO5.1	Annual IT operating budget
Liaise with change management and service level management	PO5		Not specifically covered
Produce management reports	DS6	DS6.2	Costing procedures
Audit and review IT accounting and charging systems	M3	M3.5	Independent assurance of compliance with laws and regulatory requirements and contractual commitments
7. Capacity Management			
Identify and agree service level requirements	DS3	DS3.1	Availability and performance requirements
Design, procure and modify configuration	DS9	All	Manage the configuration
Maintain CMDB and CDB	DS3	DS3.4	Modeling tools
Understand resource usage and workflow	DS3	DS3.4	Modeling tools
Prepare and maintain capacity plan	DS3	DS3.6	Workload forecasting
Balance supply and demand, assuring SLAs are not compromised	DS3	DS3.5	Proactive performance management
Monitor and optimise resource utilisation	DS3	DS3.9	Resources schedule
Review capacity management effectiveness and efficiency	DS3	DS3.7	Capacity management of resources
8. IT Service Continuity Management			
Determine scope of ITSCM	DS4	DS4.1	IT continuity framework
Establish roles and responsibilities	DS4	DS4.1	IT continuity framework
Undertake risk assessment and business impact analysis	PO9	PO9.1	Business risk assessment
Develop business continuity strategy	DS4	DS4.2	IT continuity plan strategy and philosophy
Develop and test ITSCM plans	DS4	DS4.6	Testing the IT continuity plan
9. Availability Management			
Determine availability requirements from the business	DS3	DS3.1	Availability and performance requirements
	DS4	DS4.2	IT continuity plan strategy and philosophy
Formulate availability and recovery design criteria	DS4	DS4.3	IT continuity plan contents
Maintain availability plan	DS3	DS3.2	Availability plan
Define targets for availability, reliability and maintainability	DS3	DS3.1	Availability and performance requirements
Establish measures that reflect stakeholder perspectives	DS4	DS4.4	Minimising IT continuity requirements
Monitor availability and report on trends	DS3	DS3.3	Monitoring and reporting
Review IT service and component availability	DS3	DS3.4	Modeling tools
Consider security requirements	DS5	All	Ensure systems security
Improve availability within cost constraints	DS4	All	Ensure continuous service
10. The Service Desk			
Understand business and customer service criteria	AI1	AI1.1	Definition of information requirements
Plan and design service desk infrastructure	DS8	DS8.1	Help desk
Specify targets and effectiveness metrics	DS8	DS8.5	Trend analysis and reporting
Determine service desk functions	DS8	DS8.1	Help desk
Resource and manage service desk effectively	DS8	DS8.1	Help desk
Define responsibilities and resolution pathways	DS8	DS8.3	Customer query escalation
Monitor workload	DS8	DS8.4	Monitoring of clearance
Undertake customer/user satisfaction surveys	PO8	PO8.1	External requirements review
Produce management reports	DS8	DS8.5	Trend analysis and reporting
Facilitate service management reviews	M2	M2.3	Internal control level reporting
11. Incident Management			
Record incidents	DS8	DS8.2	Registration of customer queries
Incident investigation and diagnosis	DS10	DS10.1	Problem management system
Assign ownership	DS10	DS10.1	Problem management system
Incident resolution and recovery	DS10	DS10.1	Problem management system
Incident closure	DS10	DS10.1	Problem management system

Mapping ITIL to CobiT			
ITIL	**CobiT**		
Process	**Process**	**Detailed Control Objective**	
12. Problem Management			
Identify and record problems	DS10	DS10.1	Problem management system
Classify and prioritise problems	DS10	DS10.1	Problem management system
Investigate and diagnose problems	DS10	DS10.1	Problem management system
Control problems	DS10	DS10.1	Problem management system
Assess infrastructure errors	DS10	DS10.1	Problem management system
Control errors	DS10	DS10.1	Problem management system
Record error resolution and close errors	DS10	DS10.3	Problem tracking and audit trail
Analyse trends, target support and preventive actions	DS10	DS10.3	Problem tracking and audit trail
Provide management information	DS8	DS8.5	Trend analysis and reporting
Undertake major problem reviews	DS10	DS10.2	Problem escalation
13. Configuration Management			
Undertake configuration management planning	DS9	All	Manage the configuration
Identify configuration items	DS9	DS9.1	Configuration recording
Establish CMDB and DSL	DS9	DS9.1	Configuration recording
Control configuration	DS9	DS9.2	Configuration baseline
Maintain and track CI status	DS9	DS9.3	Status accounting
Verify and audit CIs against CMDB records	DS9	DS9.4	Configuration control
Manage libraries and licences	DS9	DS9.6	Software storage
14. Change Management			
Establish change approach, advisory board and procedures	AI6	All	Manage changes
Assess and prioritise change	AI6	AI6.1	Change request initiation and control
Approve change	AI6	AI6.2	Impact assessment
Plan change	AI6	AI6.3	Control of changes
Maintain forward schedule of change	AI6	AI6.1	Change request initiation and control
Co-ordinate change implementation	AI6	AI6.3	Control of changes
Review change	AI5	AI5.14	Management's post-implementation review
Report on change metrics	AI6	AI6.3	Control of changes
15. Release Management			
Release policy and planning	AI6	AI6.7	Software release policy
Release design, build and configuration	AI6	AI6.7	Software release policy
Release testing and acceptance	AI5	AI5.6	Testing strategies and plans
Roll-out planning	AI5	AI5.3	Implementation plan
Release distribution and installation	AI6	AI6.8	Distribution of software
Release sign-off	AI5	AI5.12	Promotion to production
Release review	AI5	AI5.12	Promotion to production