COBIT® MAPPING

Mapping of NIST SP800-53 Rev 1 With COBIT® 4.1

GOVERNANCE INSTITUTE®

LEADING THE IT GOVERNANCE COMMUNITY

© 2007 IT Governance Institute. All rights reserved.

IT Governance Institute®

The IT Governance Institute (ITGI™) (*www.itgi.org*) was established by ISACA in 1998 to advance international thinking and standards in directing and controlling an enterprise's information technology. ITGI developed *Control Objectives for Information and related Technology* (CobiT®), now in its fourth edition, and Val IT™, and offers original research and case studies to assist enterprise leaders and boards of directors in their IT governance responsibilities.

Disclaimer

ITGI (the 'Owner') and the author have designed this publication, titled *CobiT® Mapping: Mapping of NIST SP800-53 Rev 1 With CobiT® 4.1* (the 'Work'), primarily as an educational resource for control professionals. The Owner makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of any proper information, procedures and tests or exclusive of other proper information procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information procedure or test, controls professionals should apply their own professional judgement to the specific control circumstances presented by the particular systems or information technology environment.

Disclosure

© 2007 ITGI. All rights reserved. No part of this publication may be used, copied, reproduced, modified, distributed, displayed, stored in a retrieval system or transmitted in any form by any means (electronic, mechanical, photocopying, recording or otherwise) without prior written authorisation of ITGI. Reproduction and use of all or portions of this publication is solely permitted for academic, internal and non-commercial use and for consulting/advisory engagements, and must include full attribution of the material's source. No other right or permission is granted with respect to this work.

IT Governance Institute
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.660.5700
Fax: +1.847.253.1443
E-mail: *info@itgi.org*
Web site: *www.itgi.org*

ISBN 978-1-60420-034-8
CobiT Mapping: Mapping of NIST SP800-53 Rev 1 With CobiT 4.1
Printed in the United States of America

© 2007 IT Governance Institute. All rights reserved.

ACKNOWLEDGEMENTS

ITGI wishes to recognise:

Researcher
John W. Lainhart IV, CISA, CISM, CIPP/G, IBM, USA
Nichola M. Tiesenga, CISA, CISM, IBM, USA
Robert W. Weaver, Ph.D., CISSP, IBM, USA

Expert Reviewers
Guy H. Groner, CISA, CIA, CISSP, USA
Jimmy Heschl, CISA, CISM, KPMG, Austria
Benjamin Hsiao, CISA, Federal Deposit Insurance Corporation, USA
James Koh, CISA, CISSP, PricewaterhouseCoopers LLP, USA
Linda Kostic, CISA, CPA, E*Trade Financial, USA
Anh Tran, CISA, BearingPoint Inc., USA

ITGI Board of Trustees
Lynn Lawton, CISA, FBCS CITP, FCA, FIIA, PIIA, KPMG LLP, UK, International President
Georges Ataya, CISA, CISM, CISSP, ICT Control sa-nv, Belgium, Vice President
Avinash Kadam, CISA, CISM, CBCP, CISSP, Miel e-Security Pvt. Ltd., India, Vice President
Howard Nicholson, CISA, City of Salisbury, Australia, Vice President
Jose Angel Pena Ibarra, Consultoria en Comunicaciones e Info., SA & CV, Mexico, Vice President
Robert E. Stroud, CA Inc., USA, Vice President
Kenneth L. Vander Wal, CISA, CPA, Ernst & Young LLP, USA, Vice President
Frank Yam, CISA, FHKCS, FHKIoD, CIA, CCP, CFE, CFSA, FFA, Focus Strategic Group, Hong Kong, Vice President
Marios Damianides, CISA, CISM, CA, CPA, Ernst & Young LLP, USA, Past International President
Everett C. Johnson, CPA, Deloitte & Touche LLP (retired), USA, Past International President
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada, Trustee
Tony Hayes, FCPA, Queensland Government, Australia, Trustee

IT Governance Committee
Tony Hayes, FCPA, Queensland Government, Australia, Chair
Max Blecher, Virtual Alliance, South Africa
Sushil Chatterji, Edutech, Singapore
Anil Jogani, CISA, FCA, Avon Consulting Ltd., UK
John W. Lainhart IV, CISA, CISM, IBM, USA
Lucio Molina Focazzio, CISA, Colombia
Ronald Saull, CSP, Great-West Life Assurance and IGM Financial, Canada
Michael Schirmbrand, Ph.D., CISA, CISM, CPA, KPMG, Austria
Robert E. Stroud, CA Inc., USA
John Thorp, The Thorp Network Inc., Canada
Wim Van Grembergen, Ph.D., University of Antwerp, University of Antwerp Management School, and IT Alignment and Governance Research Institute (ITAG), Belgium

COBIT Steering Committee
Robert E. Stroud, CA Inc., USA, Chair
Gary S. Baker, CA, Deloitte & Touche, Canada
Rafael Eduardo Fabius, CISA, Republica AFAP SA, Uruguay
Urs Fischer, CISA, CIA, CPA (Swiss), Swiss Life, Switzerland
Erik Guldentops, CISA, CISM, University of Antwerp Management School, Belgium
Jimmy Heschl, CISA, CISM, KPMG, Austria
Debbie A. Lew, CISA, Ernst & Young LLP, USA
Maxwell J. Shanahan, CISA, FCPA, Max Shanahan & Associates, Australia
Dirk E. Steuperaert, CISA, PricewaterhouseCoopers, Belgium

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

ITGI Affiliates and Sponsors
ISACA Chapters
American Institute for Certified Public Accountants
ASIS International
The Center for Internet Security
Commonwealth Association for Corporate Governance Inc.
FIDA Inform
Information Security Forum
Information Systems Security Association
Institut de la Gouvernance des Systèmes d'Information
Institute of Management Accountants Inc.
ISACA
ITGI Japan
Solvay Business School
University of Antwerp Management School
Aldion Consulting Pte. Ltd.
Analytix Holdings Pty. Ltd.
BWise B.V.
CA
Hewlett-Packard
IBM
ITpreneurs Nederlands B.V.
LogLogic Inc.
Phoenix Business and Systems Process Inc.
Project Rx Inc.
Symantec Corporation
Wolcott Group LLC
World Pass IT Solutions

Table of Contents

1. Purpose of the Document 6
2. Methodology for the Mapping 8
3. CobiT Overview 9
4. NIST SP800-53 Overview 16
5. High-level Mapping 23
6. Detailed Mapping 26
7. References 56
Appendix—CobiT and Related Products 57

1. Purpose of the Document

The IT Governance Institute (ITGI) (*www.itgi.org*) exists to assist enterprise leaders in their responsibility to ensure that IT goals align with those of the business, it delivers value, its performance is measured, its resources properly allocated and its risks mitigated. Through original research, symposia and electronic resources, the ITGI helps ensure that boards and executive management have the tools and information they need for IT to deliver against expectations. One such tool is the CobiT framework. CobiT was initially created by the Information Systems Audit and Control Foundation® (ISACF®) in 1996, and the IT Governance Institute, which was founded by ISACA in 1998, released the third edition in 2000, CobiT® 4.0 in 2005 and CobiT® 4.1 in 2007. This series of CobiT mapping papers supports the effective use of CobiT in conjunction with a number of IT-related frameworks and standards.

CobiT provides a high-level, complete IT governance and control framework based on the harmonisation of more than 50 IT good practice sources published by various international standards bodies, governments and other institutions.

ITGI has been conducting a research project to provide a detailed comparison between CobiT and a selection of these standards and best practices, to support ongoing CobiT developments and to provide guidance to CobiT users implementing IT governance, addressing questions such as:
- What should be defined?
- What is an appropriate level of detail?
- What should be measured?
- What should be automated?
- What is best practice?
- Is there a certification available?

The results of the research project can be used to further enhance the definition of CobiT's control objectives and alignment with other good practices and standards. In addition, the results help entities that are planning to apply standards and guidance in their organisation to harmonise those initiatives and use CobiT as the overall framework for sound IT governance.

Although many of these questions can be addressed using the openly available CobiT guidance, more specific information is required. This project addresses the gaps by mapping the most important and commonly used standards[1] to the CobiT processes and control objectives. The project consists of two components:
1. A high-level overview of a variety of international standards and guidance, and a mapping of CobiT to ITIL and ISO 17799 are posted on the ISACA web site at *www.isaca.org/cobitmapping*:
   - *CobiT® Mapping: Overview of International IT Guidance, 2nd Edition*
   - *Aligning CobiT®, ITIL and ISO 17799 for Business Benefit*
2. A series of more detailed mapping documents focusing on individual standards or guidance are posted at *www.isaca.org/cobitmapping* and available in the ISACA Bookstore:
   - *CobiT® Mapping: Mapping of CMMI® for Development V1.2 With CobiT® 4.0*
   - *CobiT® Mapping: Mapping of ISO/IEC 17799:2000 With CobiT®, 2nd Edition*
   - *CobiT® Mapping: Mapping of ISO/IEC 17799:2005 With CobiT® 4.0*
   - *CobiT® Mapping: Mapping of ITIL With CobiT® 4.0*
   - *CobiT® Mapping: Mapping of PMBOK© With CobiT® 4.0*
   - *CobiT® Mapping: Mapping of PRINCE2 With CobiT® 4.0*
   - *CobiT® Mapping: Mapping of SEI's CMM for Software With CobiT® 4.0*
   - *CobiT® Mapping: Mapping of TOGAF 8.1 With CobiT® 4.0*

Other planned detailed mappings include:
- *CobiT® Mapping: Mapping of FFEIC With CobiT® 4.1*
- *CobiT® Mapping: Mapping of ITIL V3 With CobiT® 4.1*
- *CobiT® Mapping: Mapping of PRINCE2 With CobiT® 4.1*
- *CobiT® Mapping: Mapping of AICPA/CICA Privacy Framework With CobiT® 4.1*
- *CobiT® Mapping: Mapping of COSO ERM With CobiT® 4.1*
- *CobiT® Mapping: Mapping of ISO 20000 With CobiT® 4.1*
- *CobiT® Mapping: Mapping of TOGAF 9 With CobiT® 4.1*
- *CobiT® Mapping: Mapping of CMMI® for Development V1.2 With CobiT® 4.1*
- *CobiT® Mapping: Mapping of ITIL V2 With CobiT® 4.1*
- *CobiT® Mapping: Mapping of IT Baseline Protection Manual With CobiT® 4.1*

[1] The term 'standard' is used in this document to encompass guidance publications.

© 2007 IT Governance Institute. All rights reserved.

- *COBIT® Mapping: Mapping of PMBOK© With COBIT® 4.1*
- *COBIT® Mapping: Mapping of ISI/IEC 1220 With COBIT® 4.1*
- *COBIT® Mapping: Mapping of ISO 19770-1 With COBIT® 4.1*
- *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT® 4.1*
- *COBIT® Mapping: Mapping of V-Model-XT With COBIT® 4.1*• *COBIT® Mapping: Overview of International IT Guidance, 3rd Edition*

This publication contains a detailed mapping of National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 1 with COBIT 4.1 and also contains the classification of the standards as presented in the overview document, *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*.

A brief overview of the standards mapped against each other in this publication is as follows:

- **COBIT**—Originally released as an IT process and control framework linking IT to business requirements, it was initially used mainly by the assurance community in conjunction with business and IT process owners. With the addition of management guidelines in 1998, COBIT was used more frequently as a management framework, providing management tools such as metrics and maturity models to complement the control framework. With the release of COBIT 4.0 in 2005, it became a more complete IT governance framework. Incremental updates to COBIT 4.0 were made in 2007; they can be seen as a fine-tuning of the framework, not fundamental changes. The current version is COBIT 4.1.
- **NIST SP800-53 Rev 1**—The application of the security controls defined in NIST SP800-53 Rev 1 represents the current state-of-the-practice safeguards and countermeasures for US federal information systems. The 17 areas represent a broad-based, balanced information security programme that addresses the management, operational, and technical aspects of protecting US federal information and information systems.

This publication does not contain all of the details of NIST SP800-53. Some language is included as provided in the publication, but it is recommended to obtain a copy of the original document. The document is available from the NIST Computer Security Resource Center web site at *http://csrc.nist.gov/publications/*.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

2. Methodology for the Mapping

The mapping is performed in two layers. A high-level mapping compares the objectives stated by NIST SP800-53 Rev 1 with the control processes of CobiT. The detailed mapping was done as shown in **figure 1**.

Figure 1—Detailed Mapping Process

Step	Description
1	The NIST SP800-53 Rev 1 was divided into the major family controls, which were mapped to one or more CobiT control objectives. Those major family controls are called 'information requirements' and correspond to the NIST divisions, e.g., AC-1, AC-2, AC-3.
2	The information requirements were mapped to CobiT control objectives as follows: a. A 1:1 mapping was done for information requirements that fit to a single control objective. b. A 1:n mapping was done for information requirements that fit to more than one control objective. c. If the information requirement covers a complete CobiT process, it was mapped to the respective CobiT process (control objective n.n, e.g., DS5.1) d. If a, b and c failed, then CobiT does not cover the requirement of this specific information requirement. The most appropriate process was selected and the information requirement was mapped to the (non-existent) control objective 99 of the process.
3	The requirements described by the information requirements were detailed from NIST SP800-53 Rev 1 and the result was sorted as defined by the CobiT framework.

The resulting information of step 3 helps implementers and auditors using the CobiT framework to see if they consider the requirements of NIST SP800-53 Rev 1.

© 2007 IT Governance Institute. All rights reserved.

3. CobiT Overview

DOCUMENT TAXONOMY

CobiT represents a collection of documents that can be classified as generally accepted good practice for IT governance, control and assurance.

ISSUER

The first edition of CobiT was issued by ISACF in 1996. In 1998, the second edition was published with additional control objectives and the *Implementation Tool Set*. The third edition was issued by ITGI in 2000 and included the management guidelines and several new control objectives. In 2005, ITGI finalised a complete rework of the CobiT content and published CobiT 4.0, which demonstrates a clear focus on IT governance. The current version 4.1 encompasses incremental updates.

GOAL OF THE GUIDANCE

The CobiT mission is:

> *To research, develop, publicise and promote an authoritative, up-to-date, internationally accepted IT governance control framework for adoption by enterprises and day-to-day use by business managers, IT professionals and assurance professionals.*[2]

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE, INCLUDING TYPICAL SITUATIONS

CobiT is usually implemented subject to one or more of the following business cases:
- There is a need for IT governance.
- Services delivered by IT are to be aligned with business goals.
- IT processes are to be standardised/automated.
- A framework for overall IT processes is needed.
- IT processes are to be unified.
- A framework is needed for a quality management system for IT.
- A structured audit approach is to be defined.
- Mergers and acquisitions are occurring with an IT impact.
- IT cost-control initiatives are desired.
- Part or all of the IT function is to be outsourced.
- Compliance with external requirements (e.g., regulators, organisations or third parties) is of concern.
- Important changes in an organisation, its business goals and processes affect IT.

RELATED RISKS OF NOT IMPLEMENTING THE GUIDANCE

Risks of not implementing CobiT include:
- Misaligned IT services, divergence
- Weak support of business goals due to misalignment
- Wasted opportunities due to misalignment
- Persistence of the perception of IT as a black box
- Shortfall between management's measurements and expectations
- Know-how tied to key individuals, not to the organisation
- Excessive IT cost and overhead
- Erroneous investment decisions and projections
- Dissatisfaction of business users with IT services supplied
- Regulatory breaches with potential significant financial penalties on organisations, restrictions on operating licences, and fiduciary liability of directors and officers if deemed not to have exercised due care and responsibility
- Unfulfilled information criteria
- Adverse effects on the organisation's internal control system due to a weak enterprise architecture for IT

[2] IT Governance Institute, CobiT 4.1, USA, 2007

© 2007 IT Governance Institute. All rights reserved.

TARGET AUDIENCE

All types of organisations, public and private companies, and external assurance and advisory professionals form the relevant target group. Within organisations, CobiT intends to support executive management and boards, business and IT management as well as governance, assurance, control and security professionals. The primary and secondary audiences are indicated in **figure 2**.

Figure 2—Chart of CobiT Audiences

Activities	Functions: Primary (P), secondary (S) to the pertinence of CobiT to that particular audience										
	Chief Executive Officer (CEO)	Chief Financial Officer (CFO)	Business Executive	Chief Information Officer (CIO)	Business Process Owner	Head of Operations	Chief Architect	Head of Development	Head of IT Administration	Project Management Office (PMO)	Compliance, Audit, Risk and Security
CobiT	S	S	P	P	P	S	S	S	S	S	P

TIMELINESS

The core content of CobiT was updated in 2005, resulting in CobiT 4.0, and further refined in 2007, resulting in CobiT 4.1. The research conducted for these updates addressed components of the control objectives and management guidelines. Specific areas that were addressed include:

- CobiT—IT governance bottom-up and top-down alignment
- CobiT and other detailed standards—Detailed mapping between CobiT and ITIL®,[3] CMM®,[4] COSO,[5] PMBOK©,[6] ISF's *Standard of Good Practice for Information Security*,[7] ISO/IEC 27000 series[8] and other global and regional frameworks and standards, to enable harmonisation with those standards in language, definitions and concepts
- Review of the quality of the critical success factors (CSFs)—CSFs were replaced by process inputs (success factors needed from others) and activity goals (goals that the process owner must address).
- Review of CSFs content—Splitting the CSFs into 'what you need from others' and 'what you need to do yourself'. CSFs were replaced by process inputs (success factors needed from others) and activity goals (goals that the process owner must address themselves).
- Linking of business goals, IT goals and IT processes—Detailed research in eight different industries, resulting in more detailed insight into how CobiT processes support the achievement of specific IT goals and, by extension, business goals
- Review of maturity models content—Ensured consistency and quality of maturity levels between and within processes, including better definitions of maturity model attributes

Also, the range of CobiT-related products was expanded in 2007 to include a new *IT Assurance Guide: Using CobiT®, IT Governance Implementation Guide: Using CobiT® and Val IT™,* and *CobiT® Control Practices, 2nd Edition*.

CERTIFICATION OPPORTUNITIES

The *IT Assurance Guide* can be used for auditing and self-assessment against the control objectives, but there is no certification for organisations. However, the CobiT framework is used frequently by Certified Public Accountants (CPAs) and Chartered Accountants (CAs) when performing a Statement on Auditing Standards (SAS) No. 70 service organisation review, earning SysTrust certification or pursuing Sarbanes-Oxley compliance. The *IT Assurance Guide* is aligned with CobiT 4.1 and can be used for auditing and self-assessment against the control objectives.

[3] British Office of Government Commerce (OCG®), IT Infrastructure Library® (ITIL), UK, 1999-2004

[4] Software Engineering Institute (SEI) of Carnegie Mellon University, Capability Maturity Model for Software (CMM), USA, 1993, and Capability Maturity Model Integration (CMMI®), 2000

[5] Committee of Sponsoring Organisations of the Treadway Commission (COSO), *Internal Control—Integrated Framework*, USA, 1994, and *Enterprise Risk Management—Integrated Framework*, 2004

[6] Project Management Institute, *A Guide to the Project Management Body of Knowledge* (PMBOK), *3rd Edition*, 2004

[7] Information Security Forum (ISF), *Standard of Good Practice for Information Security*, UK, 2003

[8] International Organisation for Standardisation(ISO)/International Electrotechnical Commission (IEC), 27000 (Series working title: *Information Technology—Security Techniques—Information Security Management Systems—Overview and Vocabulary*), Switzerland. The first document, 27001, was published in 2005. Others are still in development.

© 2007 IT Governance Institute. All rights reserved.

For certification of individuals, the COBIT Foundation Course™ is offered. Non-COBIT certification is available through ISACA, ITGI's affiliated association, in the form of the Certified Information Systems Auditor™ (CISA®) and Certified Information Security Manager® (CISM®) certifications.

CIRCULATION

COBIT is used worldwide. In addition to the English version, COBIT has been translated into French, German, Hungarian, Italian, Japanese, Korean, Portuguese and Spanish. Further translations (Czech, Hebrew, Turkish) and updates of translations to COBIT 4.1 are in development.

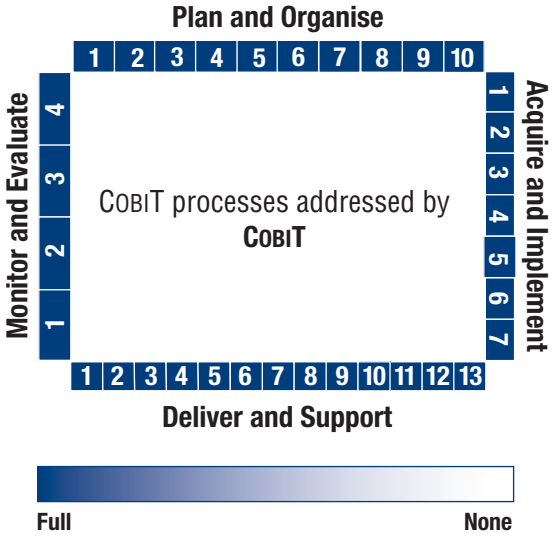
COMPLETENESS

COBIT addresses a broad spectrum of duties in IT management. COBIT includes the most significant parts of IT management, including those covered by other standards. Although no technical details have been included, the necessary tasks for complying with the control objectives are self-explanatory. Therefore, it is classified as relatively high level, aiming to be generically complete but not specific.

AVAILABILITY

COBIT 4.1 is a framework and is readily accessible for complimentary electronic download from the ITGI or ISACA web sites, *www.itgi.org* or *www.isaca.org/cobit*. COBIT Online® can be purchased at *www.isaca.org/cobitonline*. COBIT Online allows users to customise a version of COBIT for their own enterprise, then store and manipulate that version as desired. Online, real-time surveys and benchmarking are offered. The print version of COBIT 4.1 can be purchased from the ISACA Bookstore, *www.isaca.org/bookstore*.

COBIT PROCESSES ADDRESSED



Note: The chart is not a comparison; this is COBIT itself.

INFORMATION CRITERIA ADDRESSED

Information Criteria
+ Effectiveness
+ Efficiency
+ Confidentiality
+ Integrity
+ Availability
+ Compliance
+ Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

Note: The chart is not a comparison; this is COBIT itself.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

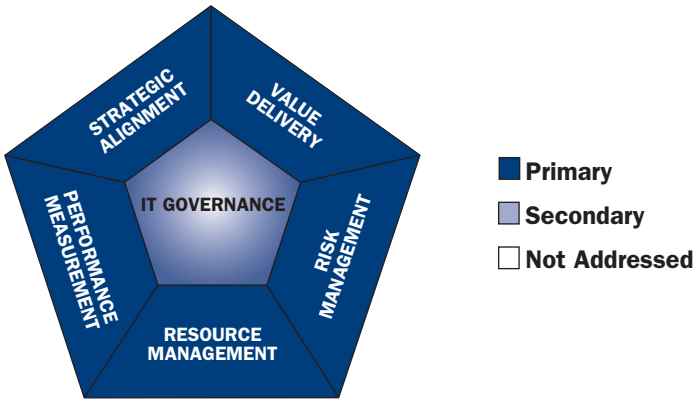
IT RESOURCES CONCERNED

IT Resources
+ Applications
+ Information
+ Infrastructure
+ People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

Note: The chart is not a comparison; this is CobiT itself.

IT GOVERNANCE FOCUS AREAS ADDRESSED



DESCRIPTION OF THE GUIDANCE AND ITS CONTENT

Enterprise governance (the system by which organisations are governed and controlled) and IT governance (the system by which the organisation's IT is governed and controlled) are, from a CobiT point of view, highly related. Enterprise governance is inadequate without IT governance and *vice versa*. IT can extend and influence the performance of the organisation, but IT has to be subject to adequate governance. On the other hand, business processes require information from the IT processes, and this interrelationship has to be governed as well.

In this subject matter, the plan-do-check-act (PDCA) cycle becomes evident. The concept of the PDCA cycle is usually used in structured problem-solving and continuous improvement processes. The PDCA cycle is also known as the Deming cycle or the Deming wheel of a continuous improvement process. Both the information needed (enterprise governance) and the information delivered (IT governance) have to be planned with measurable and constructive indicators (plan). The information and, possibly, information systems have to be implemented, delivered and used (do). The outcome of the information delivered and used is measured against the indicators defined in the planning phase (check). Deviation is investigated and corrective action is taken (act).

Considering these interdependencies, it is apparent that the IT processes are not an end in themselves; instead, they are a means to an end that is highly integrated with the management of business processes.

ITGI has defined IT governance as follows:

> *IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives.*[9]

IT GOVERNANCE USING CobiT

IT governance is the responsibility of executives and the board of directors, and consists of the leadership, organisational structures and processes that ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives.

[9] ITGI, CobiT *Quickstart, 2nd Edition*, 2007, p.8

© 2007 IT Governance Institute. All rights reserved.

CobiT supports IT governance by providing a framework to ensure that:
- IT is aligned with the business
- IT enables the business and maximises benefits
- IT resources are used responsibly
- IT risks are managed appropriately

Performance measurement is essential for IT governance, is supported by CobiT, and includes setting and monitoring measurable objectives of what IT processes need to deliver (process outcome) and how they deliver it (process capability and performance).

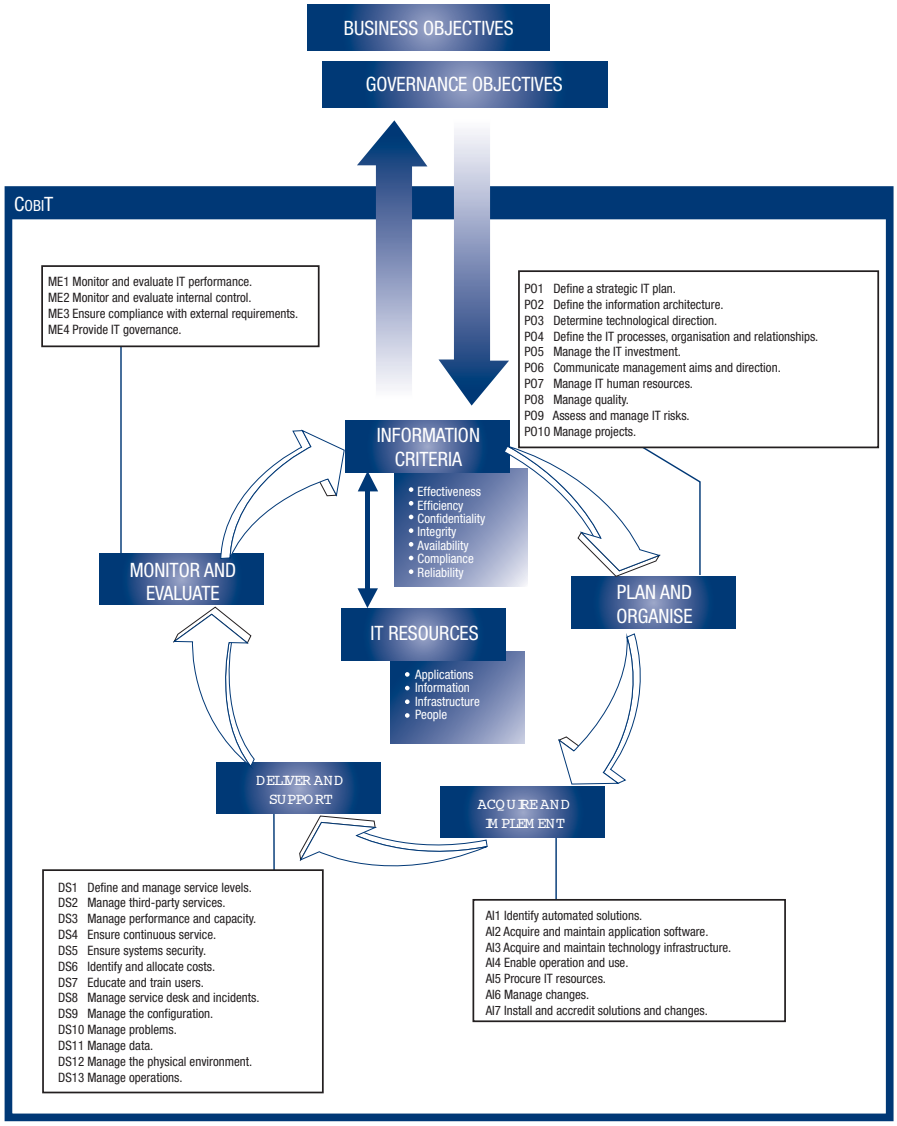
THE CobiT IT PROCESSES

The processes are grouped into four domains, as indicated in **figure 3**.

Any service delivered by IT and all services provided to the core processes have to be integrated into the IT service life cycle, as indicated in **figure 3**. Plans and organisational structures already developed can be adopted, depending on the significance of each service, rather than developing a new plan for the IT service. Services are subsequently implemented, and all necessary precautions for ongoing service, delivery and monitoring are to be considered.

From the IT governance point of view, single services are merely in the background. The focus must be on the PDCA cycle discussed previously, for the sum of services delivered by and with IT.

Figure 3—CobiT IT Processes Defined Within the Four Domains



© 2007 IT Governance Institute. All rights reserved.

Each process is described by using the following information:
• A process description
• Control objectives
• Information criteria affected by the process
• IT resources used by the process
• IT governance focus areas
• Inputs and outputs
• A Responsible, Accountable, Consulted and Informed (RACI) chart
• Goals and metrics

INFORMATION CRITERIA

To satisfy business objectives, information needs to conform to certain control criteria, which CobiT refers to as business requirements for information. Based on the broader quality, fiduciary and security requirements, seven distinct, certainly overlapping, information criteria are defined as follows:
• **Effectiveness** deals with information being relevant and pertinent to the business process as well as being delivered in a timely, correct, consistent and usable manner.
• **Efficiency** concerns the provision of information through the optimal (most productive and economical) use of resources.
• **Confidentiality** concerns the protection of sensitive information from unauthorised disclosure.
• **Integrity** relates to the accuracy and completeness of information as well as to its validity in accordance with business values and expectations.
• **Availability** relates to information being available when required by the business process—now and in the future. Availability also concerns the safeguarding of necessary resources and associated capabilities.
• **Compliance** deals with complying with those laws, regulations and contractual arrangements to which the business process is subject, i.e., externally imposed business criteria as well as internal policies.
• **Reliability** relates to the provision of appropriate information for management to operate the entity and exercise its fiduciary and governance responsibilities.

IT RESOURCES

Following the CobiT definition, the resources used by IT are identified as follows:
• **Applications** are automated user systems and manual procedures that process the information.
• **Information** is the data in all their forms—input, processed and output by the information systems in whatever form is used by the business.
• **Infrastructure** is the technology and facilities (hardware, operating systems, database management systems, networking, multimedia, etc., and the environment that houses and supports the facilities) that enable the processing of the applications.
• **People** are the personnel required to plan, organise, acquire, implement, deliver, support, monitor and evaluate the information systems and services. People may be internal, outsourced or contracted as required.

MATURITY MODELS

Maturity modelling for management and control over IT processes is based on a method of self-evaluation by the organisation. A maturity model has been defined for each of the 34 CobiT IT processes, providing an incremental measurement scale from 0, non-existent, through 5, optimised. Using the maturity models developed for each IT process, management can identify:
• The actual performance of the enterprise—Where the enterprise is today
• The current status of the industry—The comparison
• The enterprise's target for improvement—Where the enterprise wants to be

The maturity attributes list the characteristics of how IT processes are managed and describes how they evolve from a non-existent to an optimised process. These attributes can be used for more comprehensive assessment, gap analysis and improvement planning. The maturity attributes are:
• Awareness and communication
• Policies, plans and procedures
• Tools and automation
• Skills and expertise
• Responsibility and accountability
• Goal setting and measurement

© 2007 IT Governance Institute. All rights reserved.

CobiT CUBE

The previously mentioned components (IT processes, business requirements of information, and resources) are three-dimensional, thus illustrating the IT function. These dimensions, as shown in **figure 4**, represent the CobiT cube.

The CobiT components interrelate as shown in **figure 5**.

The IT processes and control objectives, activity goals, key performance indicators (KPIs), key goal indicators (KGIs) and maturity models are documented in CobiT 4.1.

For more information, refer to the appendix, CobiT and Related Products.

FURTHER REFERENCES

Internet	
ISACA	*www.isaca.org/cobit*
ITGI	*www.itgi.org*

Figure 4—CobiT Cube

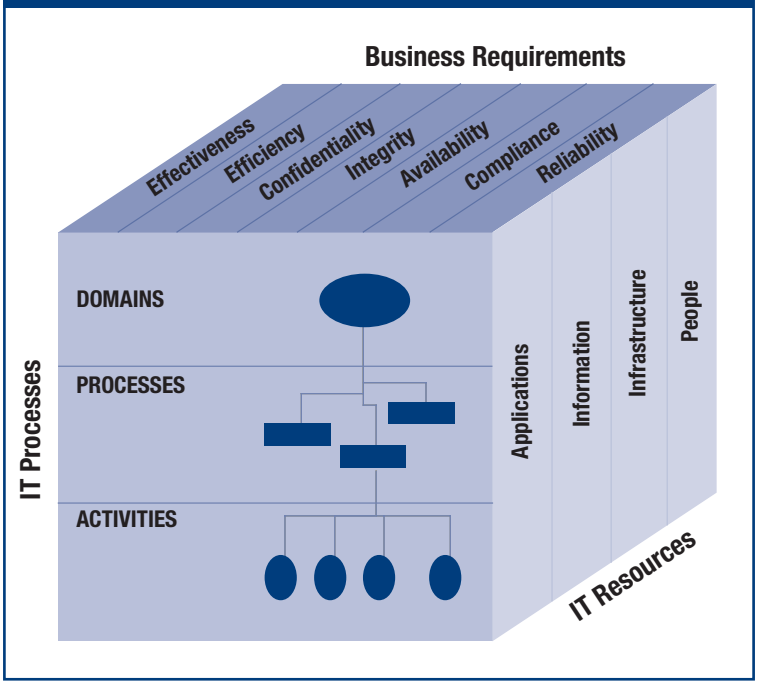
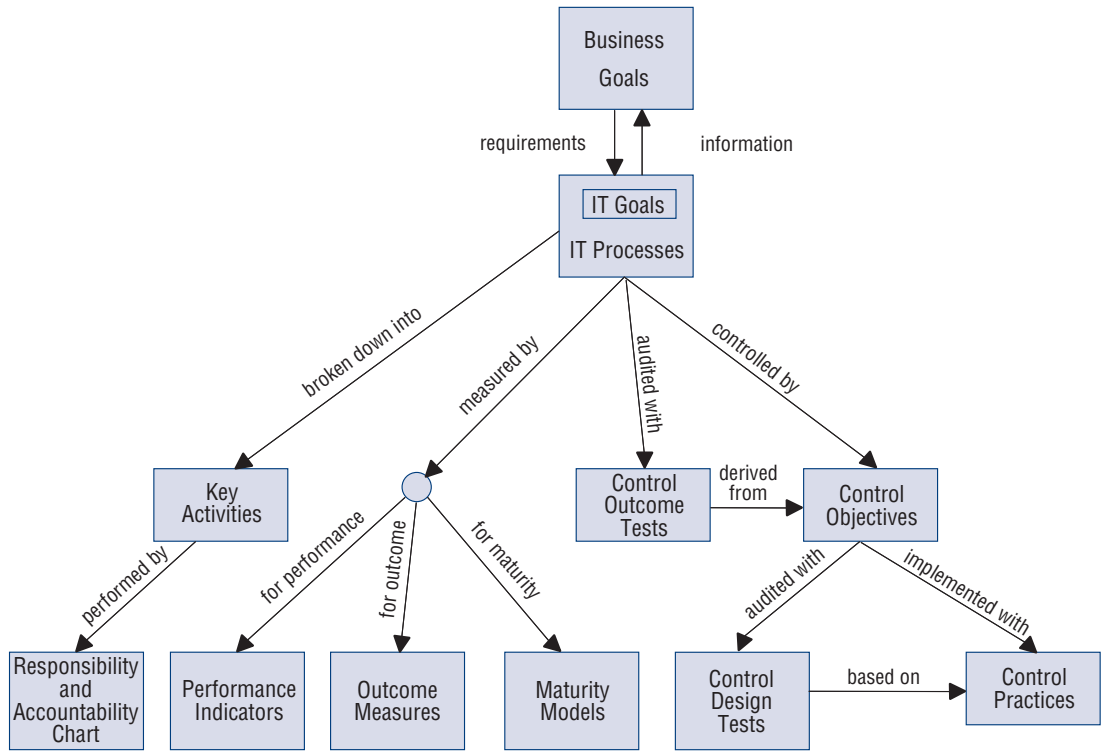


Figure 5—Interrelationships of CobiT Components



Source: CobiT 4.1, Figure 4—Interrelationships of CobiT Components, p. 8

© 2007 IT Governance Institute. All rights reserved.

4. NIST SP800-53 OVERVIEW

DOCUMENT TAXONOMY

The US NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all US federal agency operations and assets. The explicit goal is to assist federal agencies in implementing the Federal Information Security Management Act (FISMA) of 2002 and in managing cost-effective programmes to protect their information and information systems. The security controls defined in SP800-53 and recommended for use by organisations in protecting their information systems should be employed in conjunction with, and as part of, a well-defined information security programme.

ISSUER

SP800 series documents have been issued since 1991. SP800-53, *Recommended Security Controls for Federal Information Systems,* was first issued in February 2005, after a period of public discussion. The document was developed and has been issued under the authority of FISMA, P.L. 107-347.

GOAL OF THE GUIDANCE

The purpose of SP800-53 is to provide guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the federal government. The guidelines apply to all components of an information system that process, store or transmit federal information. The guidelines have been developed to help achieve more secure information systems within the federal government by:

- Facilitating a more consistent, comparable and repeatable approach for selecting and specifying security controls for information systems
- Providing a recommendation for minimum security controls for information systems categorised in accordance with Federal Information Processing Standards (FIPS) 199, *Standards for Security Categorization of Federal Information and Information Systems*
- Promoting a dynamic, extensible catalogue of security controls for information systems to meet the demands of changing requirements and technologies
- Creating a foundation for the development of assessment methods and procedures for determining security control effectiveness

BUSINESS DRIVERS FOR IMPLEMENTING THE GUIDANCE, INCLUDING TYPICAL SITUATIONS

The standard provides for mandatory controls applicable to all federal information systems other than those systems designated as national security systems. As such, the standard serves a diverse federal audience of information systems and information security professionals including:

- Individuals with information systems and information security management and oversight responsibilities (e.g., chief information officers [CIOs], senior agency information security officers [ISOs], authorising officials)
- Individuals with information systems development responsibilities (e.g., programme and project managers)
- Individuals with information security implementation and operational responsibilities (e.g., information systems owners, information owners, information systems security officers)
- Individuals with information systems and information security assessment and monitoring responsibilities (e.g., auditors, inspectors general, evaluators, certification agents [CAs])

Compliance with the controls is measured using auditor guidance available in SP800-53A, Draft Special Publication 800-53A, *Guide for Assessing the Security Controls in Federal Information Systems* (*http://csrc.nist.gov/publications/drafts.html#sp800-53A*).

Because the selection and employment of appropriate security controls for an information system are important tasks that can have major implications on the operations and assets of an organisation, commercial entities may find the use of this baseline will provide guidance on adequate controls for protecting systems that support the operation and assets of the organisation.

RELATED RISKS OF NOT IMPLEMENTING THE GUIDANCE

For a federal agency, FISMA compliance in the form of aggregate scores is public information. Significant funding penalties can occur from non-compliance.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

TARGET AUDIENCE

The primary and secondary audiences are indicated in **figure 6**.

Figure 6—Chart of SP800-53 Audiences

Activities	Functions: Primary (P), secondary (S) to the pertinence of NIST SP800-53 to the particular audience										
	Chief Executive Officer (CEO)	Chief Financial Officer (CFO)	Business Executive	Chief Information Officer (CIO)	Business Process Owner	Head of Operations	Chief Architect	Head of Development	Head of IT Administration	Project Management Office (PMO)	Compliance, Audit, Risk and Security
NIST SP800-53	S	–	–	P	S	P	P	P	P	S	P

An additional secondary audience is information systems security officers, and additional primary audiences include:
- Senior agency information officers
- Designated authorising officers
- Inspector general

TIMELINESS

The core content of NIST SP800-53 is under continuous revision through public discussion, with a commitment to a biennial review and update cycle. Rev 1 contains relatively modest changes in a few notable areas from previous public draft versions of this publication:
- There have been several additions to the security control catalogue, reflecting new controls and control enhancements to provide users with greater choices in supplementing their security control baselines.
- There have been some minor additions to the security control baselines reflecting an increased need for protection within federal information systems and to better align the minimum security controls with current federal policy and recommended security practices.
- There have been some changes to the tailoring guidance for security control baselines reflecting environmental considerations and the application of compensating controls.
- Chapters two and three have been expanded to include guidance on implementing security controls in external environments and responding to information systems incidents.
- There have been two new appendices added to the publication providing;
  – A two-way crosswalk from the security controls in SP800-53 to the NIST suite of security standards and guidelines
  – Initial guidance on the application of SP800-53 to industrial control systems

Enhancements to SP800-53 at the time of this publication include SP800-53A, a 300-page document providing explicit control assessment criteria for the controls documented in SP800-53.

CERTIFICATION OPPORTUNITIES

No certification opportunities are available at time of publication.

CIRCULATION

The standard is mandatory for US federal systems that are not national security systems.

COMPLETENESS

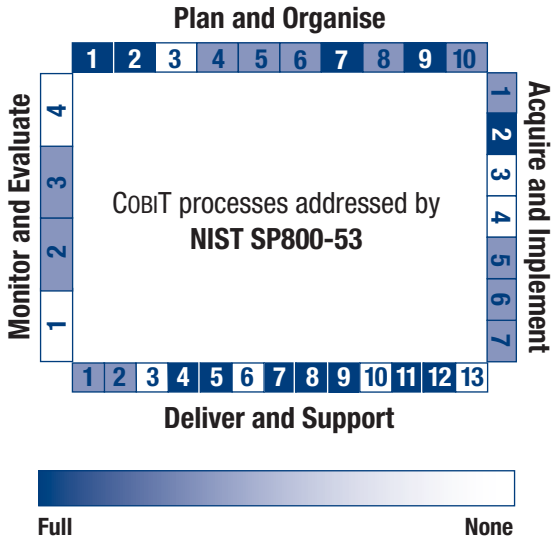
The SP800-53 criteria are designed to provide technically sound and broadly applicable sets of controls for information systems. The criteria are intended to be sufficiently rich to satisfy the breadth and depth of security requirements derived from laws, executive orders, directives, policies, regulations and organisational needs, to ensure the confidentiality, integrity and availability of the information being processed, stored or transmitted. Whilst intended to be cost-effective, unlike COBIT it does not address financial issues. However, its catalogue of security controls is intended to demonstrate compliance with a variety of governmental, organisational or institutional security requirements, facilitating consistent and repeatable control design and measured effectiveness in a consistent and repeatable manner.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

AVAILABILITY

The standard is readily available from the NIST web site. The document notes that it has been prepared for use by federal agencies, and may be used by non-governmental organisations on a voluntary basis. It is not subject to copyright.

COBIT PROCESSES ADDRESSED



INFORMATION CRITERIA ADDRESSED

Information Criteria	
o	Effectiveness
-	Efficiency
+	Confidentiality
+	Integrity
+	Availability
+	Compliance
o	Reliability

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

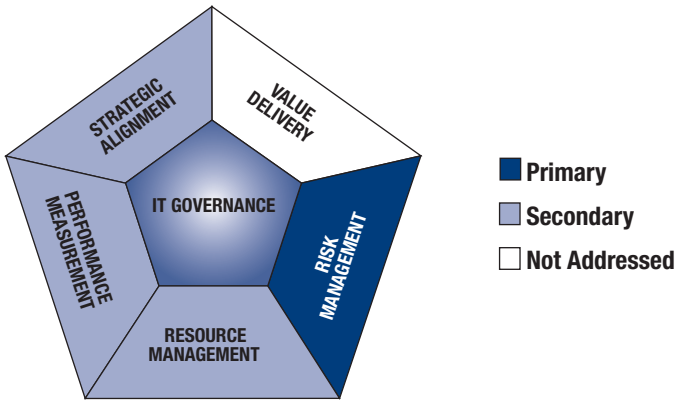
IT RESOURCES CONCERNED

IT Resources	
o	Applications
+	Information
+	Infrastructure
+	People

(+) Frequently addressed
(o) Moderately addressed
(-) Not or rarely addressed

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

IT GOVERNANCE FOCUS AREAS ADDRESSED



DESCRIPTION OF GUIDANCE AND ITS CONTENT

The primary focus of NIST SP800-53 is on selection, implementation and assurance requirements of specific security controls as part of an effective information security programme. The intent is to establish a normative baseline for risk management for federal information processing systems. The guidance integrates with the other, extensive and often extremely detailed, standards and guidelines published under the Special Publications and Federal Information Processing Standards series.

After introductory material, the guidance establishes the fundamental concepts associated with security control selection and specification, including:
- Structural components and security family organisation
- Baseline controls
- Use of controls in organisationwide information security programmes
- Use of controls in external environments
- Assurance principles for control effectiveness
- Ongoing maintenance of the controls and control baselines

The guidance next studies the process for selecting and specifying security controls. This is based upon a high-water mark impact approach, described in FIPS 199. It also describes how to determine additional controls, and how to update the selected controls as part of a continuous monitoring programme.

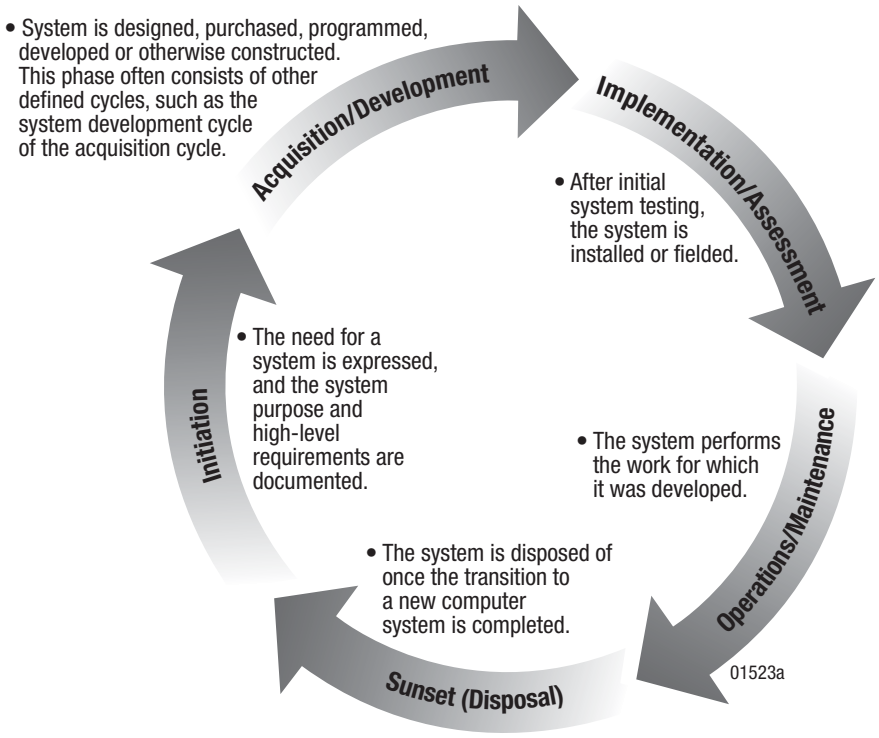
This guidance provides detailed security control selection and specification data, including explicit definitions and terms, assurance requirements, a security catalogue, and also relationships between various NIST standards and controls and associated control frameworks.

The NIST approach is very system/programme-centric, and follows an explicitly designed security life cycle, as shown in **figure 7**.

Considering the life cycle shown in **figure 7**, the service delivery and IT processes are, in some sense, an end; the framework is designed to maximise 'the extent to which someone who relies on a system can have confidence that the system meets its specifications, i.e., that the system does what it claims to do and does not perform unwanted functions'—a formal definition of trust. It is not intended as a comprehensive IT framework.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

Figure 7—NIST Security Life Cycle



The NIST SP800-53 Framework

The security controls in the security control catalogue are organised in a tree-like structure. The first tier separates into three general classes of security controls:

- **Technical**—Direct controls primarily implemented and executed by the information system through mechanisms contained in hardware, software or firmware components of the system
- **Managerial**—Indirect controls that focus on the management of risk and the management of information systems security
- **Operational**—Direct controls that are primarily implemented and executed by people (as opposed to systems)

These are then broken into a total of 17 control families corresponding to these three classes.

The NIST SP800-53 Control Families

Figure 8 summarises the classes and families in the security control catalogue and associated family identifiers.

Management Guidelines

The NIST SP800-53 document should be considered, not by itself, but in the context of the full library of NIST Special Publications and Federal Information Processing Standards. For example, the authority document that mandates the use of the catalogue from SP800-53 comes from FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*, and states: 'Federal agencies must meet the minimum security requirements as defined herein through the use of the security controls in accordance with NIST Special Publication 800-53, *Recommended Security Controls for Federal Information Systems*, as amended'.

Other elements in the SP800 library address topics ranging from broad management issues, such as security planning, security engineering principles, control life cycle issues, integrating security into the capital planning programme, and security awareness and training, to focused, technical specifications such as allowed block encryption modes, key management, Domain Name System (DNS) deployment, radio-frequency identification (RFID) schema, and cell phone forensics.

Of particular note is SP800-100, *Information Security Handbook: A Guide for Managers*, a comprehensive guide that 'summarizes and augments a number of existing NIST standards and guidance documents and provides additional information on related topics. Such documents are referenced within appropriate subchapters'.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

Figure 8—NIST Security Control Classes, Families and Identifiers

Class	Family	Identifier
Management	Risk Assessment	RA
Management	Planning	PL
Management	System and Services Acquisition	SA
Management	Certification, Accreditation, and Security Assessments	CA
Operational	Personnel Security	PS
Operational	Physical and Environmental Protection	PE
Operational	Contingency Planning	CP
Operational	Configuration Management	CM
Operational	Maintenance	MA
Operational	System and Information Integrity	SI
Operational	Media Protection	MP
Operational	Incident Response	IR
Operational	Awareness and Training	AT
Technical	Identification and Authentication	IA
Technical	Access Control	AC
Technical	Audit and Accountability	AU
Technical	System and Communications Protection	SC

Maturity Models

SP800-53A describes maturity models for information systems security control environments, linking them to impact assessments derived from the guidance from FIPS 199. Maturity modelling is based over both the presence and configuration of explicit, auditable criteria as well as language based upon conventional Capability Maturity Model (CMM) approaches. The maturity model has three (successful) levels of increasing rigour:

- Security controls in place; no obvious errors
- Security controls correctly implemented; operating as intended
- Security controls consistently applied on an ongoing basis with continuous improvement

Explicit language in the assessment provides for a determination of process maturity levels.

Control Practices

Control practices were developed for NIST SP800-53 programmatically as part of the FISMA Implementation Project (*http://csrc.nist.gov/sec-cert/*). Input came from a variety of sources including NIST SP800-26, *Security Self-Assessment Guide for Information Technology Systems*, US Department of Defense (DoD) Policy 8500, Director of Central Intelligence Directive (DCID) 6/3, ISO/IEC 17799, US Government Accountability Office (GAO) Federal Information System Controls Audit Manual (FISCAM), and US Health and Human Services (HHS) Centers for Medicare and Medicaid Services (CMS) Core Security Requirements; and these sources are subject to extensive public review by security professionals. The control practices provide a common baseline with a high level of detail to ensure consistent, effective control implementation across federal entities.

Audit Guidelines

To achieve the desired goals and objectives, and to provide consistent reporting and oversight to the American public, each federal entity must audit its procedures constantly and consistently, its reporting status quarterly and the overall programme assessment annually. The audit guidelines in NIST SP800-53A describe actual assessment activities to be performed by external auditors, identifying roles, responsibilities, mechanisms for assessment and appropriate metrics. Other NIST guidelines (NIST SP800-26, *Security Self-assessment Guide for Information Technology Systems*, and NIST SP800-80, *Guide for Developing Performance Metrics for Information Security*) provide a wealth of information for internal assessments.

© 2007 IT Governance Institute. All rights reserved.

Relationship to COBIT and the Federal Enterprise Architecture

As can be clearly seen in the graphic illustrating, COBIT processes addressed, the coverage mapping between NIST SP800-53 controls and the COBIT controls and processes shows a great deal of overlap in some areas, and no overlap at all in others. The objectives of the two documents are fairly different. COBIT intends to describe the generally accepted good practices for IT governance, control and assurance, with the framework addressing a broad spectrum of IT processes. However, NIST SP800-53 is intended to provide a security control catalogue, establishing consistency and auditability across various US federal enterprises. NIST SP800-53 is thus narrower and more targeted in many areas than COBIT, and NIST can be more focused because of its more specific purpose.

FURTHER REFERENCES

Internet	
NIST SP800-53	*http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf*
FISMA Implementation Project	*http://csrc.nist.gov/sec-cert/*

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

5. HIGH-LEVEL MAPPING

OVERVIEW

This section contains the result of the mapping of objectives as stated in NIST SP800-53 to the IT processes of COBIT; an overview of the results can be found in **figure 9**. A copy of NIST SP800-53 can be obtained from NIST at *http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf*.

Figure 9—NIST SP800-53 Processes Mapped to High-level COBIT Processes

COBIT 4.1 Processes and Domains	1	2	3	4	5	6	7	8	9	10	11	12	13
Plan and Organise	+	+	-	o	o	o	+	o	+	o			
Acquire and Implement	o	+	-	-	o	o	o						
Deliver and Support	o	o	-	+	+	-	o	+	+	-	+	+	-
Monitor and Evaluate	-	o	o	-									
Process Controls	-	o	-	o	+	-							
Application Controls	o	o	o	o	o	+							

(+) Significant match (more than two objectives were mapped to a COBIT process)
(o) Minor match (one or two objectives were mapped)
(-) Unrelated focus (no objective was mapped)
(\) No COBIT IT process exists.

COVERAGE OF IT GOVERNANCE FOCUS AREAS

Figure 10 lists the coverage of IT governance focus areas.

Figure 10—Coverage of IT Governance Focus Areas

Focus Area	Contribution of COBIT	Contribution of NIST SP800-53
Strategic alignment	Requirements of this focus area can be covered by implementing the COBIT processes. Processes with a primary impact on this focus area are: • PO1 Define a strategic IT plan • PO2 Define the information architecture • PO6 Communicate management aims and direction • PO7 Manage IT human resources • PO8 Manage quality • PO9 Assess and manage IT risks • PO10 Manage projects • AI1 Identify automated solutions • AI2 Acquire and maintain application software • DS1 Define and manage service levels • ME3 Ensure compliance with external requirements • ME4 Provide IT governance • AC4 Processing integrity and validity • AC6 Transaction authentication and integrity The processes ensure that the IT-enabled initiatives are planned and organised in a structured manner and initiated appropriately. In addition, the delivery of IT services meets the business and regulatory requirements and enables the management and the business to oversee service development and service delivery.	Requirements of this focus area can be partially covered by implementing various NIST SP800-53 security controls. The control families with a primary impact on this focus area are: • CM—Configuration management • PL—Planning • PS—Personnel security • RA—Risk assessment • SA—System and services acquisition • SI—System and information integrity The processes are specifically focused on security but clearly add to assurances that IT-enabled initiatives are planned and organised in a structured manner and initiated appropriately. The emphasis on configuration management is particularly applicable in that organisations know their IT environment in order to ensure it is well controlled and secure, and addresses the issue of strategic alignment of IT to the business needs.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

Figure 10—Coverage of IT Governance Focus Areas (cont.)

Focus Area	Contribution of CobiT	Contribution of NIST SP800-53
Value delivery	Requirements of this focus area can be covered by implementing the CobiT processes. Processes with a primary impact on this focus area are: • PO5 Manage the IT investment • AI1 Identify automated solutions • AI2 Acquire and maintain application software • AI4 Enable operation and use • AI6 Manage changes • AI7 Install and accredit solutions and changes • DS1 Define and manage service levels • DS2 Manage third-party services • DS4 Ensure continuous service • DS7 Educate and train users • DS8 Manage service desk and incidents • DS9 Manage the configuration • DS10 Manage problems • DS11 Manage data • ME2 Monitor and evaluate internal control • ME4 Provide IT governance • AC4 Processing integrity and validity • AC6 Transaction authentication and integrity The processes ensure that IT-enabled business initiatives deliver value to the business by proper planning of the implementation, delivery of knowledge to ensure beneficial usage of services and providing a proper support for the services required in line with the business requirements.	Requirements of this focus area can be partially covered by implementing various NIST SP800-53 security controls. The control families with a primary impact on this focus area are: • AT—Awareness and training • CA—Certification, accreditation and security assessments • CM—Configuration management • CP—Contingency planning • MA—Maintenance • IR—Incident response • SA—System and services acquisition • SI—System and information integrity The processes address value delivery by emphasising security over the IT environment. Without adequate security, the delivery of value to the organisation is negatively impacted. The emphasis is to ensure that the maximum value can be achieved by security enabling business needs. Security can be a value-add, not just a way to mitigate risk.
Risk management	Requirements of this focus area can be covered by implementing the CobiT processes. Processes with a primary impact on this focus area are: • PO4 Define the IT processes, organisation and relationships • PO6 Communicate management aims and direction • PO9 Assess and manage IT risks • DS2 Manage third-party services • DS4 Ensure continuous service • DS5 Ensure systems security • DS11 Manage data • DS12 Manage the physical environment • ME2 Monitor and evaluate internal control • ME3 Ensure compliance with external requirements • ME4 Provide IT governance • AC4 Processing integrity and validity • AC6 Transaction authentication and integrity These processes ensure that risks are identified and managed in a way that enables business and top management to understand the relevance of IT-related risks, implications on business risks and the adequacy of measures to control risks.	Requirements of this focus area can be partially covered by implementing various NIST SP800-53 security controls. The control families with a primary impact on this focus area are: • AC—Access control • AU—Audit and accountability • CA—Certification, accreditation, and security assessments • CP—Contingency planning • IA—Identification and authentication • IR—Incident response • MP—Media protection • PE—Physical and environmental protection • PL—Planning • PS—Personnel security • RA—Risk assessment • SA—System and services acquisition • SC—System and communication protection • SI—System and information integrity Those processes are very much risk-oriented to ensure that security risks are identified and managed by business, IT and top management of organisations—so that management understands the relevance of security-related risks, the implications of these risks on the business, and the adequacy of measures to control security risks.

© 2007 IT Governance Institute. All rights reserved.

Figure 10—Coverage of IT Governance Focus Areas (cont.)		
Focus Area	**Contribution of CobiT**	**Contribution of NIST SP800-53**
Resource management	Requirements of this focus area can be covered by implementing the CobiT processes. Processes with a primary impact on this focus area are: • PO2 Define the information architecture • PO3 Determine technological direction • PO4 Define the IT processes, organisation and relationships • PO7 Manage IT human resources • AI3 Acquire and maintain technology infrastructure • AI5 Procure IT resources • DS1 Define and manage service levels • DS3 Manage performance and capacity • DS6 Identify and allocate costs • DS9 Manage the configuration • DS11 Manage data • DS13 Manage operations • ME4 Provide IT governance The processes are responsible to ensure IT is able to provide resources required to deliver the services by focusing on planning and managing resources as applications, infrastructure, information and people.	Requirements of this focus area can be partially covered by implementing various NIST SP800-53 security controls. The control families with a primary impact on this focus area are: • CM—Configuration management • MP—Media protection • PS—Personnel security • SA—System and services acquisition • SI—System and information integrity The processes are responsible for ensuring that IT is able to provide resources required to deliver the security services by focusing on planning and managing resources related to applications, infrastructure, information and people.
Performance measurement	Requirements of this focus area can be covered by implementing the CobiT processes. Processes with a primary impact on this focus area are: • DS1 Define and manage service levels • ME1 Monitor and evaluate IT performance • ME4 Provide IT governance The processes ensure that the other focus areas (i.e., strategic alignment, value delivery, risk management and resource management) will achieve their desired outcomes. This creates the opportunity to take timely corrective measures, if needed.	Requirements of this focus area are not covered in NIST SP800-53. This is not unusual, as research has shown that performance measurement is the least addressed of the five IT governance focus areas by other standards/guidance.

COMBINATION OF CobiT AND NIST SP800-53

NIST SP800-53 should be used in conjunction with CobiT to provide more detailed guidance in the area of security, as identified in this mapping publication. NIST is complementary to CobiT and, therefore, should be used with CobiT, just as other similar standards (e.g., ISO/IEC 17799:2005) are mapped to and used with CobiT.

CobiT, on the other hand, provides guidance in the entire realm of the governance of enterprise IT to ensure that the enterprise's IT sustains and extends the organisation's strategies and objectives. CobiT addresses security to ensure adequate governance of the enterprise's IT security; however, CobiT does not provide the detailed security guidance that is provided in NIST SP800-53.

Both CobiT and NIST SP800-53 are controls that are oriented to be very compatible from the security perspective. Because there are no differences in concepts, there are no conflicts between the two publications.

RECOMMENDATIONS FOR USE

NIST SP800-53 is a security-related technical standard issued by NIST. It is one of NIST's SP800-series of reports 'providing research, guidelines, and outreach efforts in information systems security, and its collaborative activities with industry, government, and academic organizations'. Although this is a US federal government standard, it is applicable for all organisations interacting with the US federal government. More important, the standards included in NIST are good security practices for all organisations and therefore need to be looked at and used from that perspective.

© 2007 IT Governance Institute. All rights reserved.

6. Detailed Mapping

As stated previously, the detailed mapping consists of the information requirements of NIST SP800-53 mapped to each CobiT control objective. The structure follows the domains, processes and control objectives of CobiT.

The coverage of the mapped information requirements is noted in four different levels:
- E—The requirements stated in NIST SP800-53 **exceed** the requirement of CobiT. Therefore, NIST SP800-53 should be seen as the primary source for further information and guidance to improve the process or control objective.
- C—The requirements of the control objective are **covered** by the mapped requirements of the guidance in NIST SP800-53.
- A—Some aspects of the control objectives are **addressed** by NIST SP800-53, but the requirements of the control objective are not covered completely.
- N/A—There is **no match** between the requirements of CobiT and NIST SP800-53.

Each CobiT control objective number and title is listed in tables as in the example in **figure 11**.

Figure 11—Example of Detailed Mapping of NIST SP800-53 With CobiT

Control Objective Example	NIST SP800-53 Coverage
Control objective number and title	E, C, A or N/A

Legend: (E) Exceeded
(C) Complete coverage
(A) Some aspects addressed
(N/A) Not addressed

The description of the CobiT control objective is provided to give an overview of the aim of the specific part of CobiT.

Note: Mapping cannot always be one-to-one because the CobiT control objectives operate at a higher level, and the detail of SP800-53 is much closer to the level of detail of the CobiT control practices.

OVERVIEW

NIST SP800-53 Rev 1 is presented in numbered, outline form, broken into 17 families and multiple controls per family. Controls have a reference statement, expanded guidance and control enhancements for environments where the risk suggests a more controlled environment. References provided are at the level of detail of the reference statement.

Figure 12 gives a qualitative overview of the coverage.

Figure 12—NIST SP800-53 Processes Mapped to High-level CobiT Processes

CobiT 4.1 Processes and Domains													
	1	2	3	4	5	6	7	8	9	10	11	12	13
Plan and Organise	+	+	-	o	o	o	+	o	+	o			
Acquire and Implement	o	+	-	-	o	o	o						
Deliver and Support	o	o	-	+	+	-	o	+	+	-	+	+	-
Monitor and Evaluate	-	o	o	-									
Process Controls	-	o	-	o	+	-							
Application Controls	o	o	o	o	o	+							

(+) Significant match
(o) Minor match
(-) Unrelated focus
(\) No CobiT control process exists.

© 2007 IT Governance Institute. All rights reserved.

PLAN AND ORGANISE

PO1 Define a Strategic IT Plan

PO1.1 *IT value management* states: 'Work with the business to ensure that the enterprise portfolio of IT-enabled investments contains programmes that have solid business cases. Recognise that there are mandatory, sustaining and discretionary investments that differ in complexity and degree of freedom in allocating funds. IT processes should provide effective and efficient delivery of the IT components of programmes and early warning of any deviations from plan, including cost, schedule or functionality, which might impact the expected outcomes of the programmes. IT services should be executed against equitable and enforceable service level agreements (SLAs). Accountability for achieving the benefits and controlling the costs is clearly assigned and monitored. Establish fair, transparent, repeatable and comparable evaluation of business cases including financial worth, the risk of not delivering a capability and the risk of not realising the expected benefits'.

This was mapped with SA-2 Allocation of Resources, which requires the organisation to determine, document and allocate, as part of its capital planning and investment control process, the resources required to adequately protect the information system. Whilst focused on security aspects, this addresses planning for effective management.

PO1.3 *Assessment of current capability and performance* states: 'Assess the current capability and performance of solution and service delivery to establish a baseline against which future requirements can be compared. Define performance in terms of IT's contribution to business objectives, functionality, stability, complexity, costs, strengths and weaknesses'.

This was mapped with CA-7 Continuous Monitoring, which requires the organisation to monitor the security controls in the information system on an ongoing basis. Again, whilst focused on security controls, baselining is a precursor to continuous monitoring.

PO1.4 *IT strategic plan* states: 'Create a strategic plan that defines, in co-operation with the relevant stakeholders, how IT goals will contribute to the enterprise's strategic objectives and related costs and risks. It should include how IT will support IT-enabled investment programmes, IT services and IT assets. IT should define how the objectives will be met, the measurements to be used and the procedures to obtain formal sign-off from the stakeholders. The IT strategic plan should cover investment/operational budget, funding sources, sourcing strategy, acquisition strategy, and legal and regulatory requirements. The strategic plan should be sufficiently detailed to allow the definition of tactical IT plans'.

PO1.4 was mapped with:
- PL-2 System Security Plan, which requires the organisation to develop and implement a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organisation review and approve the plan.
- PL-3 System Security Plan Update, which requires the organisation to review the security plan for the information system based on the organisation-defined frequency, at least annually, and revise the plan to address system/organisational changes or problems identified during plan implementation or security control assessments

Because the US federal process has a formal sign-off from designated accrediting authorities, rather than stakeholders, the concept is slightly different, but the underlying goals are similar.

PO1.6 *IT portfolio management* states: 'Actively manage, with the business, the portfolio of IT-enabled investment programmes required to achieve specific strategic business objectives by identifying, defining, evaluating, prioritising, selecting, initiating, managing and controlling programmes. This should include clarifying desired business outcomes, ensuring that programme objectives support achievement of the outcomes, understanding the full scope of effort required to achieve the outcomes, assigning clear accountability with supporting measures, defining projects within the programme, allocating resources and funding, delegating authority, and commissioning required projects at programme launch'.

This was mapped with CM-2 Baseline Configuration and System Component Inventory, which requires the organisation to develop, document, and maintain a current baseline configuration of the information system, an inventory of the systems' constituent components, and the relevant ownership information.

PO2 Define the Information Architecture

PO2.1 *Enterprise information architecture model* states: 'Establish and maintain an enterprise information model to enable applications development and decision-supporting activities, consistent with IT plans as described in PO1. The model should facilitate the optimal creation, use and sharing of information by the business in a way that maintains integrity and is flexible, functional, cost-effective, timely, secure and resilient to failure'.

© 2007 IT Governance Institute. All rights reserved.

This was mapped with:
- CM-1 Configuration Management Policy and Procedures, which requires the organisation to develop, disseminate, and periodically review/update:
  - A formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls
- CM-2 Baseline Configuration and System Component Inventory, which requires the organisation to develop, document, and maintain a current baseline configuration of the information system, an inventory of the systems' constituent components, and relevant ownership information

PO2.3 *Data classification scheme* states: 'Establish a classification scheme that applies throughout the enterprise, based on the criticality and sensitivity (e.g., public, confidential, top secret) of enterprise data. This scheme includes details about data ownership; definition of appropriate security levels and protection controls; and a brief description of data retention and destruction requirements, criticality and sensitivity. It should be used as the basis for applying controls such as access controls, archiving or encryption'.

This was mapped with:
- AC-3 Access Enforcement, which requires the information system to enforce assigned authorisations for controlling access to the system in accordance with applicable policy
- AC-15 Automated Marking, which requires the information system to mark output using standard naming conventions to identify any special dissemination, handling or distribution instructions
- AC-16 Automated Labeling, which requires the information system to appropriately label information in storage, in process and in transmission

PO2.4 *Integrity management* states: 'Define and implement procedures to ensure integrity and consistency of all data stored in electronic form, such as databases, data warehouses and data archives'.

This was mapped with:
- SI-1 System and Information Integrity Policy and Procedures, which requires the organisation to develop, disseminate, and periodically review/update:
  - A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls
- SI-4 Information System Monitoring Tools and Techniques, which requires the organisation to employ tools and techniques to monitor events on the information system, detect attacks, and provide identification of unauthorised use of the system
- SI-7 Software and Information Integrity, which requires the information system to detect and protect against unauthorised changes to software and information
- SI-10 Information Accuracy, Completeness, Validity and Authenticity, which requires the information system to check information for accuracy, completeness, validity and authenticity

Because the NIST SP800-53 is a security catalogue, it is explicit about the specific integrity mechanisms that must be applied.

PO4 Define the IT Processes, Organisation and Relationships

PO4.6 *Establishment of roles and responsibilities* states: 'Establish and communicate roles and responsibilities for IT personnel and end users that delineate between IT personnel and end-user authority, responsibilities and accountability for meeting the organisation's needs'.

This was mapped with PS-1 Personnel Security Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
- A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
- Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls

PO4.10 *Supervision* states: 'Implement adequate supervisory practices in the IT function to ensure that roles and responsibilities are properly exercised to assess whether all personnel have sufficient authority and resources to execute their roles and responsibilities, and to generally review KPIs'.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

This was mapped with AC-13 Supervision and Review—access control, which requires the organisation to supervise and review the activities of users with respect to the enforcement and usage of information systems access controls.

While more terse, the NIST standard is actually more restrictive, in that it requires formal access authorisations and an enforcement process.

PO4.11 *Segregation of duties* states: 'Implement a division of roles and responsibilities that reduces the possibility for a single individual to compromise a critical process. Make sure that personnel are performing only authorised duties relevant to their respective jobs and positions'.

This was mapped with:
- AC-5 Separation of Duties, which requires the information system to enforce separation of duties through assigned access authorisations
- AC-6 Least Privilege, which requires the information system to enforce the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks

While more terse, the NIST standard is actually more restrictive in that it requires formal access authorisations and an enforcement process.

PO4.13 *Key IT personnel* states: 'Define and identify key IT personnel (e.g., replacements/backup personnel), and minimise reliance on a single individual performing a critical job function'.

This was mapped with PS-2 Position Categorisation, which requires the organisation to assign a risk designation to all positions and establish screening criteria for individuals filling those positions. The organisation reviews and revises position risk designations based on the organisation-defined frequency.

The goals here are similar. To identify critical job functions, position categorisations must be established. Whilst minimisation of single points of failures is not explicitly stated in PS-2, such reliances would be covered under business continuity controls, explicitly covered elsewhere.

PO4.14 *Contracted staff policies and procedures* states: 'Ensure that consultants and contract personnel who support the IT function know and comply with the organisation's policies for the protection of the organisation's information assets such that they meet agreed-upon contractual requirements'.

This was mapped with PS-7 Third-Party Personnel Security, which requires the organisation to establish personnel security requirements, including security roles and responsibilities for third-party providers, and monitor provider compliance to ensure adequate security.

PO5 Manage the IT Investment

PO5.2 *Prioritisation within IT budget* states: 'Implement a decision-making process to prioritise the allocation of IT resources for operations, projects and maintenance to maximise IT's contribution to optimising the return on the enterprise's portfolio of IT-enabled investment programmes and other IT services and assets'.

This was mapped with SA-2 Allocation of Resources, which requires the organisation to determine, document and allocate, as part of its capital planning and investment control process, the resources required to adequately protect the information system. Whilst focused on security aspects, this addresses planning for effective management.

PO6 Communicate Management Aims and Direction

PO6.5 *Communication of IT objectives and direction* states, 'Communicate awareness and understanding of business and IT objectives and direction to appropriate stakeholders and users throughout the enterprise'.

This was mapped with PL-4 Rules of Behavior, which requires the organisation to establish and make readily available to all information system users a set of rules that describes their responsibilities and expected behavior with regard to information and information system usage. The organisation receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorising access to the information system and its resident information.

© 2007 IT Governance Institute. All rights reserved.

PO7 Manage IT Human Resources

PO7.3 *Staffing of roles* states: 'Define, monitor and supervise roles, responsibilities and compensation frameworks for personnel, including the requirement to adhere to management policies and procedures, the code of ethics, and professional practices. The level of supervision should be in line with the sensitivity of the position and extent of responsibilities assigned'.

This was mapped with:
- PS-1 Personnel Security Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls
- PS-2 Position Categorisation, which requires the organisation to assign a risk designation to all positions and establish screening criteria for individuals filling those positions. The organisation reviews and revises position risk designations based on the organisation-defined frequency.

PO7.4 *Personnel training* states: 'Provide IT employees with appropriate orientation when hired and ongoing training to maintain their knowledge, skills, abilities, internal controls and security awareness at the level required to achieve organisational goals'.

This was mapped with:
- AT-2 Security Awareness, which requires the organisation to ensure that all users (including managers and senior executives) receive basic information systems security awareness training before authorising access to the system, when required by system changes, and based on the organisation-defined frequency, at least annually thereafter.
- AT-3 Security Training, which requires the organisation to identify personnel with significant information systems security roles and responsibilities, document those roles and responsibilities, and provide appropriate information systems security training before authorising access to the system, when required by system changes, and based on the organisation-defined frequency thereafter.

PO7.6 *Personnel clearance procedures* states: 'Include background checks in the IT recruitment process. The extent and frequency of periodic reviews of these checks depend on the sensitivity and/or criticality of the function and should be applied for employees, contractors and vendors'.

This was mapped with PS-3 Personnel Screening, which requires the organisation to screen individuals requiring access to organisational information and information systems before authorising access.

PO7.8 *Job change and termination* states: 'Take expedient actions regarding job changes, especially job terminations. Knowledge transfer should be arranged, responsibilities reassigned and access rights removed such that risks are minimised and continuity of the function is guaranteed'.

This was mapped with:
- PS-4 Personnel Termination, which requires that when employment is terminated, the organisation terminates information system access, conducts exit interviews, ensures the return of all organisational information system-related property (e.g., keys, identification cards, building passes), and ensures that appropriate personnel have access to official records created by the terminated employee that are stored on organisational information systems.
- PS-5 Personnel Transfer, which requires the organisation to review information systems/facilities access authorisations when personnel are reassigned or transferred to other positions within the organisation and initiates appropriate actions (e.g., reissuing keys, identification cards, building passes; closing old accounts and establishing new accounts; and changing system access authorisations).

PO8 Manage Quality

PO8.3 *Development and acquisition standards* states: 'Adopt and maintain standards for all development and acquisition that follow the life cycle of the ultimate deliverable, and include sign-off at key milestones based on agreed-upon sign-off criteria. Consider software coding standards; naming conventions; file formats; schema and data dictionary design standards; user interface standards; interoperability; system performance efficiency; scalability; standards for development and testing; validation against requirements; test plans; and unit, regression and integration testing'.

This was mapped with SA-3 Life Cycle Support, which requires the organisation to manage the information system using a system development life cycle methodology that includes information security considerations.

The supplementary guidance for SA-3 points to NIST SP800-64, which describes specifications, standards and other requirements as part of the life cycle process. NIST SP800-64 is primarily focused on security considerations.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

PO9 Assess and Manage IT Risks

PO9.1 *IT risk management framework* states: 'Establish an IT risk management framework that is aligned to the organisation's (enterprise's) risk management framework'.

This was mapped with RA-1 Risk Assessment Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
- A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
- Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls

The supplemental guidance for this control points to NIST SP800-30 and NIST SP800-12 for frameworks for assessment and policy, respectively. In addition, NIST SP800-39, *Managing Risk from Information from Information Systems: An Organisational Perspective* (Initial Public Draft) has recently been issued to describe NIST's Risk Management Framework. This publication provides guidance on important information security issues including:
- Organisationwide perspectives on managing risk from information systems
- Risk-based protection strategies
- Trustworthiness of information systems and trust relationships among organisations
- Strategic considerations for managing risk related to the operation and use of information systems
- Use of the risk executive function

In addition to the above issues, SP800-39 provides information on applying the steps of the Risk Management Framework to the phases of the system development life cycle to help ensure that information security is tightly integrated into the mission and business functions of organisations.

PO9.2 *Establishment of risk context* states: 'Establish the context in which the risk assessment framework is applied to ensure appropriate outcomes. This should include determining the internal and external context of each risk assessment, the goal of the assessment and the criteria against which risks are evaluated'.

This was mapped with RA-2 Security Categorisation, which requires the organisation to categorise the information system and the information processed, stored or transmitted by the system in accordance with FIPS 199, and document the results (including supporting rationale) in the system security plan. Designated senior-level officials within the organisation review and approve the security categorisations.

FIPS 199 establishes formal contexts for evaluation of risk. It promotes the use of analysis based on confidentiality, integrity and availability requirements and mandates a high-water mark risk categorisation based on these three elements. Thus, contexts are formally determined and placed into external categories, which are not determinable by the individual system owners, although the choice of categorisation is made by the system owners.

PO9.3 *Event identification* states: 'Identify events (an important, realistic threat that exploits a significant applicable vulnerability) with a potential negative impact on the goals or operations of the enterprise, including business, regulatory, legal, technology, trading partner, human resources and operational aspects. Determine the nature of the impact and maintain this information. Record and maintain relevant risks in a risk registry'.

This was mapped with:
- RA-3 Risk Assessment, which requires the organisation to conduct assessments of the risk and magnitude of harm that could result from the unauthorised access, use, disclosure, disruption, modification or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties)
- RA-5 Vulnerability Scanning, which requires the organisation to scan for vulnerabilities in the information system based on the organisation-defined frequency or when significant new vulnerabilities potentially affecting the system are identified and reported. This is also part of the FIPS 199 risk calculation.

PO9.4 *Risk assessment* states: 'Assess, on a recurrent basis, the likelihood and impact of all identified risks, using qualitative and quantitative methods. The likelihood and impact associated with inherent and residual risk should be determined individually, by category and on a portfolio basis'.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

This was mapped with:
- RA-3 Risk Assessment, which requires the organisation to conduct assessments of the risk and magnitude of harm that could result from the unauthorised access, use, disclosure, disruption, modification or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties)
- RA-4 Risk Assessment Update, which requires the organisation to update the risk assessment based on the organisation-defined frequency or, whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system.

Note that risk assessments are required by the US government as part of the certification process (on a triennial cycle). The methods mandated for risk assessment have varied over time, but have generally used a mix of qualitative and quantitative methods.

PO9.5 *Risk response* states: 'Develop and maintain a risk response process designed to ensure that cost-effective controls mitigate exposure to risks on a continuing basis. The risk response process should identify risk strategies such as avoidance, reduction, sharing or acceptance; determine associated responsibilities; and consider risk tolerance levels'.

This was mapped with:
- IR-1 Incident Response Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls
- IR-4 Incident Handling, which requires the organisation to implement an incident-handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery.

PO9.6 *Maintenance and monitoring of a risk action plan* states: 'Prioritise and plan the control activities at all levels to implement the risk responses identified as necessary, including identification of costs, benefits and responsibility for execution. Obtain approval for recommended actions and acceptance of any residual risks, and ensure that committed actions are owned by the affected process owner(s). Monitor execution of the plans, and report on any deviations to senior management'.

This was mapped with:
- IR-1 Incident Response Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls
- IR-4 Incident Handling, which requires the organisation to implement an incident-handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery

PO10 Manage Projects

PO10.12 *Project planning of assurance methods* states: 'Identify assurance tasks required to support the accreditation of new or modified systems during project planning, and include them in the integrated project plan. The tasks should provide assurance that internal controls and security features meet the defined requirements'.

This was mapped with CA-1 Certification, Accreditation, and Security Assessment Policies and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
- Formal, documented security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
- Formal, documented procedures to facilitate the implementation of the security assessment and certification; accreditation policies; and associated assessment, certification and accreditation controls

ACQUIRE AND IMPLEMENT

AI1 Identify Automated Solutions

AI1.1 *Definition and maintenance of business functional and technical requirements* states: 'Identify, prioritise, specify and agree on business functional and technical requirements covering the full scope of all initiatives required to achieve the expected outcomes of the IT-enabled investment programme'.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

This was mapped with RA-3 Risk Assessment, which requires the organisation to conduct assessments of the risk and magnitude of harm that could result from the unauthorised access, use, disclosure, disruption, modification or destruction of information and information systems that support the operations and assets of the agency (including information and information systems managed/operated by external parties).

AI2 Acquire and Maintain Application Software

AI2.3 *Application control and auditability* states: 'Implement business controls, where appropriate, into automated application controls such that processing is accurate, complete, timely, authorised and auditable'.

This was mapped with:
- AU-2 Auditable Events, which requires the information system to generate audit records for events based on the organisation-defined auditable events
- SI-10 Information Accuracy, Completeness, Validity and Authenticity, which requires the information system to check information for accuracy, completeness, validity and authenticity

AI2.4 *Application security and availability* states: 'Address application security and availability requirements in response to identified risks and in line with the organisation's data classification, information architecture, information security architecture and risk tolerance'.

This was mapped with:
- AC-3 Access Enforcement, which requires the information to system to enforce assigned authorisations for controlling access to the system in accordance with applicable policy
- IA-2 User Identification and Authentication, which requires the information system to uniquely identify and authenticate users (or processes acting on behalf of users)
- SA-4 Acquisitions, which requires the organisation to include security requirements and/or security specifications, either explicitly or by reference, in information systems acquisition contracts based on an assessment of risk
- SA-8 Security Engineering Principles, which requires the organisation to design and implement the information system using security engineering principles
- SC-2 Application Partitioning, which requires the information system to separate user functionality (including user interface services) from information systems management functionality
- SI-7 Software and Information Integrity, which requires the information system to detect and protect against unauthorised changes to software and information
- SI-10 Information, Accuracy, Completeness, Validity and Authenticity, which requires the information system to check information for accuracy, completeness, validity and authenticity

AI2.5 *Configuration and implementation of acquired application software* states: 'Configure and implement acquired application software to meet business objectives'.

This was mapped with SA-1 System and Services Acquisition Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
- A formal, documented system and services acquisition policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
- Formal, documented procedures to facilitate the implementation of the system and services acquisition policy and associated system and services acquisition controls

The US Federal Acquisition Regulations have significant additional requirements on acquired applications.

AI2.7 *Development of application software* states: 'Ensure that automated functionality is developed in accordance with design specifications, development and documentation standards, QA requirements and approval standards. Ensure that all legal and contractual aspects are identified and addressed for application software developed by third parties'.

This was mapped with SA-3 Life Cycle Support, which requires the organisation to manage the information system using a system development life cycle methodology that includes information security considerations.

The supplementary guidance for SA-3 points to NIST SP800-64, which describes specifications, standards and other requirements as part of the life cycle process. NIST SP800-64 is focused primarily on security considerations.

AI2.8 *Software quality assurance* states: 'Develop, resource and execute a software QA plan to obtain the quality specified in the requirements definition and the organisation's quality policies and procedures'.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

This was mapped with SA-11 Developer Security Testing, which requires the information systems developer to create a security test and evaluation plan, implement the plan, and document the results. This mandates security assurance, but would generally be integrated with QA requirements.

AI2.10 *Application software maintenance* states: 'Develop a strategy and plan for the maintenance of software applications'.

This was mapped with MA-2 Periodic Maintenance, which requires the organisation to schedule, perform and document routine preventive and regular maintenance on the components of the information system in accordance with manufacturer or vendor specifications and/or organisational requirements.

AI5 Procure IT Resources

AI5.1 *Procurement control* states: 'Develop and follow a set of procedures and standards that is consistent with the business organisation's overall procurement process and acquisition strategy to acquire IT-related infrastructure, facilities, hardware, software and services needed by the business'.

This was mapped with SA-1 System and Services Acquisition Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
- A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
- Formal, documented procedures to facilitate the implementation of the system

AI5.4 *IT resources acquisition* states: 'Protect and enforce the organisation's interests in all acquisition contractual agreements, including the rights and obligations of all parties in the contractual terms for the acquisition of software, development resources, infrastructure and services'.

This was mapped with SA-4 Acquisitions, which requires the organisation to include security requirements and/or security specifications, either explicitly or by reference, in information systems acquisition contracts based on an assessment of risk.

AI6 Manage Changes

AI6.1 *Change standards and procedures* states: 'Set up formal change management procedures to handle, in a standardised manner, all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms'.

This was mapped with:
- CM-1 Configuration Management Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls
- CM-3 Configuration Change Control, which requires the organisation to document and control changes to the information system. Appropriate organisational officials approve information system changes in accordance with organisational policies and procdures.

AI6.3 *Emergency changes*, states, 'Establish a process for defining, raising, testing, documenting, assessing and authorising emergency changes that do not follow the established change process'.

This was mapped with CM-3 Configuration Change Control, which requires the organisation to document and control changes to the information system. Appropriate organisational officials approve information system changes in accordance with organisational policies and procedures.

AI7 Install and Accredit Solutions and Changes

AI7.7 *Final acceptance test* states: 'Ensure that business process owners and IT stakeholders evaluate the outcome of the testing process as determined by the test plan. Remediate significant errors identified in the testing process, having completed the suite of tests identified in the test plan and any necessary regression tests. Following evaluation, approve promotion to production'.

© 2007 IT Governance Institute. All rights reserved.

This was mapped with:
- CA-4 Security Certification, which requires the organisation to conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system
- CA-6 Security Accreditation, which requires the organisation to authorise (i.e., accredit) the information system for processing before beginning operations and update the authorisation based on the organisation-defined frequency, at least every three years, or when there is a significant change to the system. A senior organisational official signs and approves the security accreditation.

DELIVER AND SUPPORT

DS1 Define and Manage Service Levels

DS1.6 *Review of service level agreements and contracts* states: 'Regularly review SLAs and underpinning contracts (UCs) with internal and external service providers to ensure that they are effective and up to date and that changes in requirements have been taken into account'.

This was mapped with SA-9 External Information System Services, which requires the organisation to ensure that third-party providers of outsourced information system services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance and established SLAs. The organisation monitors security control compliance.

Again, the NIST guidance focuses on security issues rather than on more general quality issues, but the goals are similar.

DS2 Manage Third-party Services

DS2.2 *Supplier relationship management* states: 'Formalise the supplier relationship management process for each supplier. The relationship owners should liaise on customer and supplier issues and ensure the quality of the relationship based on trust and transparency (e.g., through SLAs)'.

This was mapped with PS-7 Third-Party Personnel Security, which requires the organisation to establish personnel security requirements, including security roles and responsibilities for third-party providers, and monitor provider compliance to ensure adequate security.

Again, the NIST guidance focuses on security issues rather than on more general quality issues, but the goals are similar.

DS2.3 *Supplier risk management* states: 'Identify and mitigate risks relating to suppliers' ability to continue effective service delivery in a secure and efficient manner on a continual basis. Ensure that contracts conform to universal business standards in accordance with legal and regulatory requirements. Risk management should further consider non-disclosure agreements (NDAs), escrow contracts, continued supplier viability, conformance with security requirements, alternative suppliers, penalties and rewards, etc.'.

This was mapped with SA-9 External Information System Services, which requires the organisation to ensue that third-party providers of outsourced information systems services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance and established SLAs. The organisation monitors security control compliance.

DS4 Ensure Continuous Service

DS4.1 *IT continuity framework* states: 'Develop a framework for IT continuity to support enterprisewide business continuity management using a consistent process. The objective of the framework should be to assist in determining the required resilience of the infrastructure and to drive the development of disaster recovery and IT contingency plans. The framework should address the organisational structure for continuity management, covering the roles, tasks and responsibilities of internal and external service providers, their management and their customers; and the planning processes that create the rules and structures to document, test and execute the disaster recovery and IT contingency plans. The plan should also address items such as the identification of critical resources, noting key dependencies, the monitoring and reporting of the availability of critical resources, alternative processing, and the principles of backup and recovery'.

This was mapped with:
- CP-1 Contingency Planning Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

- CP-6 Alternate Storage Sites, which requires the organisation to identify an alternate storage site and initiate necessary agreements to permit the storage of information systems backup information
- CP-7 Alternate Processing Sites, which requires the organisation to identify an alternate processing site and initiate necessary agreements to permit the resumption of information systems operations for critical mission/business functions within the organisation-defined time period when the primary processing capabilities are unavailable
- CP-8 Telecommunications Services, which requires the organisation to identify primary and alternate telecommunications services to support the information system and initiate necessary agreements to permit the resumption of system operations for critical mission/business functions within the organisation-defined time period when the primary telecommunications capabilities are unavailable

The NIST guidance requires more explicit controls to be present in the continuity solution.

DS4.2 *IT continuity plans* states: 'Develop IT continuity plans based on the framework and designed to reduce the impact of a major disruption on key business functions and processes. The plans should be based on risk understanding of potential business impacts and address requirements for resilience, alternative processing and recovery capability of all critical IT services. The plans should also cover usage guidelines, roles and responsibilities, procedures, communication processes, and the testing approach'.

This was mapped with:
- CP-2 Contingency Plan, which requires the organisation to develop and implement a contingency plan for the information system, addressing contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. Designated officials within the organisation review and approve the contingency plan and distribute copies of the plan to key contingency personnel.
- CP-4 Contingency Plan Testing, which requires the organisation to test the contingency plan for the information system based on the organisation-defined frequency, using organisation-defined tests and exercises to determine the plan's effectiveness and the organisation's readiness to execute the plan. Appropriate officials within the organisation review the contingency plan test results and initiate corrective actions.
- CP-9 Information System Backup, which requires the organisation to conduct backups of user-level and system-level information (including system state information) contained in the information system based on the organisation-defined frequency and protect backup information whilst in transit and at the storage location

The NIST guidance seems to cover the CobiT control objective with more explicit language.

DS4.4 *Maintenance of the IT continuity plan* states: 'Encourage IT management to define and execute change control procedures to ensure that the IT continuity plan is kept up to date and continually reflects actual business requirements. Communicate changes in procedures and responsibilities clearly and in a timely manner'.

This was mapped with CP-5 Contingency Plan Update, which requires the organisation to review the contingency plan for the information system based on the organisation-defined frequency, at least annually, and revise the plan to address system/organisational changes or problems encountered during plan implementation, execution or testing.

DS4.5 *Testing of the IT continuity plan* states: 'Test the IT continuity plan on a regular basis to ensure that IT systems can be effectively recovered, shortcomings are addressed and the plan remains relevant. This requires careful preparation, documentation, reporting test results and, according to the results, implementation of an action plan. Consider the extent of testing recovery of single applications to integrated testing scenarios to end-to-end testing and integrated vendor testing'.

This was mapped with CP-4 Contingency Plan Testing, which requires the organisation to test the contingency plan for the information system based on the organisation-defined frequency, using organisation-defined tests and exercises to determine the plan's effectiveness and the organisation's readiness to execute the plan. Appropriate officials within the organisation review the contingency plan test results and initiate corrective actions.

DS4.6 *IT continuity plan training* states: 'Provide all concerned parties with regular training sessions regarding the procedures and their roles and responsibilities in case of an incident or disaster. Verify and enhance training according to the results of the contingency tests'.

This was mapped with CP-3 Contingency Training, which requires the organisation to train personnel in their contingency roles and responsibilities with respect to the information system and provide refresher training based on the organisation-defined frequency, at least annually.

© 2007 IT Governance Institute. All rights reserved.

DS4.8 *IT services recovery and resumption* states: 'Plan the actions to be taken for the period when IT is recovering and resuming services. This may include activation of backup sites, initiation of alternative processing, customer and stakeholder communication, and resumption procedures. Ensure that the business understands IT recovery times and the necessary technology investments to support business recovery and resumption needs'.

This was mapped with:
- CP-7 Alternate Processing Sites, which requires the organisation to identify an alternate processing site and initiate necessary agreements to permit the resumption of information systems operations for critical mission/business functions within the organisation-defined time period when the primary processing capabilities are unavailable
- CP-10 Information System Recovery and Reconstitution, which requires the organisation to employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure

DS4.9 *Offsite backup storage* states: 'Store offsite all critical backup media, documentation and other IT resources necessary for IT recovery and business continuity plans. Determine the content of backup storage in collaboration between business process owners and IT personnel. Management of the offsite storage facility should respond to the data classification policy and the enterprise's media storage practices. IT management should ensure that offsite arrangements are periodically assessed, at least annually, for content, environmental protection and security. Ensure compatibility of hardware and software to restore archived data, and periodically test and refresh archived data'.

This was mapped with:
- CP-6 Alternate Storage Sites, which requires the organisation to identify an alternate storage site and initiate necessary agreements to permit the storage of information systems backup information
- CP-9 Information System Backup, which requires the organisation to conduct backups of user-level and system-level information (including system state information) contained in the information system based on the organisation-defined frequency and protect backup information whilst in transit and at the storage location

DS5 Ensure Systems Security

DS5.2 *IT security plan* states: 'Translate business, risk and compliance requirements into an overall IT security plan, taking into consideration the IT infrastructure and the security culture. Ensure that the plan is implemented in security policies and procedures together with appropriate investments in services, personnel, software and hardware. Communicate security policies and procedures to stakeholders and users'.

This was mapped with:
- PL-1 Security Planning Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls
- PL-2 System Security Plan, which requires the organisation to develop and implement a security plan for the information system that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Designated officials within the organisation review and approve the plan.
- PL-4 Rules of Behaviour, which requires the organisation to establish and make readily available to all information systems users a set of rules that describes their responsibilities and expected behaviour with regard to information and information systems usage. The organisation receives signed acknowledgement from users indicating that they have read, understand and agree to abide by the rules of behaviour, before authorising access to the information system and its resident information.
- SC-1 System and Communications Protection Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls.

Formal security planning has been required as part of the certification process for US federal systems for several decades. In particular, the supplementary guidance to PL-2 points to SP800-18, *Guide for Developing Security Plans for Federal Information Systems*.

DS5.3 *Identity management* states: 'Ensure that all users (internal, external and temporary) and their activity on IT systems (business application, IT environment, system operations, development and maintenance) are uniquely identifiable. Enable user identities via authentication mechanisms. Confirm that user access rights to systems and data are in line with defined and documented business needs and that job requirements are attached to user identities. Ensure that user access rights are requested by user management, approved by

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

system owners and implemented by the security-responsible person. Maintain user identities and access rights in a central repository. Deploy cost-effective technical and procedural measures, and keep them current to establish user identification, implement authentication and enforce access rights'.

This was mapped with:
- IA-1 Identification and Authentication Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls
- IA-2 User Identification and Authentication, which requires the information system to uniquely identify and authenticate users (or processes acting on behalf of users)
- IA-4 Identifier Management, which requires the organisation to manage user identifiers by:
  - Uniquely identifying each user
  - Verifying the identity of each user
  - Receiving authorisation to issue a user identifier from an appropriate organisation official
  - Ensuring that the user identifier is issued to the intended party
  - Disabling the user identifier after the organisation-defined time period of inactivity
  - Archiving user identifiers

Centralisation of user identities and access rights (mentioned in the CobiT control objectives) is not required by NIST guidance, but is usually implemented as a matter of efficiency. In addition, US Homeland Security Presidential Directive/HSPD-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, mandates that all US federal agencies use a government-wide standard form of identification for the federal government's employees and contractors. This policy is intended to enhance security, increase government efficiency, reduce identity fraud and protect personal privacy. It requires the use of this identification for gaining physical access to federally controlled facilities and logical access to federally controlled information systems.

DS5.4 *User account management* states: 'Address requesting, establishing, issuing, suspending, modifying and closing user accounts and related user privileges with a set of user account management procedures. Include an approval procedure outlining the data or system owner granting the access privileges. These procedures should apply for all users, including administrators (privileged users) and internal and external users, for normal and emergency cases. Rights and obligations relative to access to enterprise systems and information should be contractually arranged for all types of users. Perform regular management review of all accounts and related privileges'.

This was mapped with:
- AC-2 Account Management, which requires the organisation to manage information systems accounts, including establishing, activating, modifying, reviewing, disabling and removing accounts. The organisation reviews information systems accounts based on the organisation-defined frequency, at least annually.
- IA-4 Identifier Management, which requires the organisation to manage user identifiers by:
  - Uniquely identifying each user
  - Verifying the identity of each user
  - Receiving authorisation to issue a user identifier from an appropriate organisation official
  - Ensuring that the user identifier is issued to the intended party
  - Disabling user identifier after the organisation-defined time period of inactivity
  - Archiving user identifiers
- PS-6 Access Agreements, which requires the organisation to complete appropriate access agreements for individuals requiring access to organisational information and information systems, before authorising access, and review/update the agreements

DS5.5 *Security testing, surveillance and monitoring* states: 'Test and monitor the IT security implementation in a proactive way. IT security should be reaccredited in a timely manner to ensure that the approved enterprise's information security baseline is maintained. A logging and monitoring function will enable the early prevention and/or detection and subsequent timely reporting of unusual and/or abnormal activities that may need to be addressed'.

This was mapped with:
- AU-6 Audit Monitoring, Analysis, and Reporting, which requires the organisation to regularly review/analyse information system audit records for indications of inappropriate or unusual activity, investigate suspicious activity or suspected violations, report findings to appropriate officials, and take necessary actions.

© 2007 IT Governance Institute. All rights reserved.

- CA-2 Security Assessments, which requires the organisation to conduct an assessment of the security controls in the information system based on the organisation-defined frequency, at least annually, to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for the system
- CA-6 Security Accreditation, which requires the organisation to authorise (i.e., accredit) the information system for processing before operations and update the authorisation based on the organisation-defined frequency, at least every three years or when there is a significant change to the system. A senior organisational official signs and approves the security accreditation.
- CA-7 Continuous Monitoring, which requires the organisation to monitor the security controls in the information system on an ongoing basis.
- CM-4 Monitoring Configuration Changes, which requires the organisation to monitor changes to the information system, conducting security impact analyses to determine the effects of the changes
- RA-5 Vulnerability Scanning, which requires the organisation to scan for vulnerabilities in the information system based on the organisation-defined frequency or when significant new vulnerabilities potentially affecting the system are identified and reported. This is also part of the FIPS 199 risk calculation.
- SI-4 Information System Monitoring Tools and Techniques, which requires the organisation to employ tools and techniques to monitor events on the information system, detect attacks and provide identification of unauthorised use of the system

DS5.6 *Security incident definition* states: 'Clearly define and communicate the characteristics of potential security incidents so that they can be properly classified and treated by the incident and problem management process'.

This was mapped with:
- IR-1 Incident Response Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls
- IR-6 Incident Reporting, which requires the organisation to promptly report incident information to appropriate authorities

DS5.7 *Protection of security technology* states: 'Make security-related technology resistant to tampering, and do not disclose security documentation unnecessarily'.

This was mapped with:
- PE-4 Access Control for Transmission Medium, which requires the organisation to control physical access to information system distribution and transmission lines within organisational facilities to prevent accidental damage, eavesdropping, in-transit modifications, disruption, or physical tampering
- SA-5 Information System Documentation, which requires the organisation to ensure that adequate documentation for the information system is available, protected when required, and distributed to authorised personnel
- SC-3 Security Function Isolation, which requires the information system to isolate security functions from non-security functions

The COBIT control seems to imply a broader non-tampering requirement. The US federal perspective does not require any particular level of tamper resistance.

DS5.8 *Cryptographic key management* states: 'Determine that policies and procedures are in place to organise the generation, change, revocation, destruction, distribution, certification, storage, entry, use and archiving of cryptographic keys to ensure the protection of keys against modification and unauthorised disclosure'.

This was mapped with:
- SC-12 Cryptographic Key Establishment and Management, which requires the information system to employ automated mechanisms with supporting procedures or manual procedures for cryptographic key establishment and key management
- SC-13 Use of Validated Cryptography, which requires that when cryptography is employed within the information system, the cryptography to comply with applicable federal laws, directives, policies, regulations, standards, and guidance, including FIPS 140-2 (as amended), which requires the system to perform all cryptographic operations (including key generation) using FIPS 140-2 validated cryptographic modules operating in approved modes of operation

The supplemental guidance to SC-12 points to NIST SP800-56 and NIST SP800-57 on key establishment and key management.

DS5.9 *Malicious software prevention, detection and correction* states: 'Put preventive, detective and corrective measures in place (especially up-to-date security patches and virus control) across the organisation to protect information systems and technology from malware (e.g., viruses, worms, spyware, spam)'.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

This was mapped with:
- SC-18 Mobile Code, which requires the organisation to:
  - Establish usage restrictions and implementation guidance for mobile code technologies based on the potential to cause damage to the information system if used maliciously
  - Document, monitor, and control the use of mobile code within the information system. Appropriate organisational officials authorise the use of mobile code.
- SI-3 Malicious Code Protection, which requires the information system to implement malicious code protection
- SI-7 Software and Information Integrity, which requires the information system to detect and protect against unauthorised changes to software and information
- SI-8 Spam Protection, which requires the information system to implement spam protection

DS5.10 *Network security* states: 'Use security techniques and related management procedures (e.g., firewalls, security appliances, network segmentation and intrusion detection) to authorise access and control information flows from and to networks'.

This was mapped with:
- AC-4 Information Flow Enforcement, which requires the information system to enforce assigned authorisations for controlling the flow of information within the system and amongst interconnected systems in accordance with applicable policy
- SC-7 Boundary Protection, which requires the information system to monitor and control communications at the external boundary of the information system and at key internal boundaries within the system
- SI-4 Information System Monitoring Tools and Techniques, which requires the organisation to employ tools and techniques to monitor events on the information system, detect attacks and provide identification of unauthorised use of the system

DS5.11 *Exchange of sensitive data* states: 'Exchange sensitive transaction data only over a trusted path or medium with controls to provide authenticity of content, proof of submission, proof of receipt and non-repudiation of origin'.

This was mapped with:
- AU-10 Nonrepudiation, which requires the information system to provide the capability to determine whether a given individual took a particular action (e.g., created information, sent a message, approved information [e.g., to indicate concurrence or sign a contract] or received a message)
- SC-9 Transmission Confidentiality, which requires the information system to protect the confidentiality of transmitted information
- SC-11 Trusted Path, which requires the information system to establish a trusted communications path between the user and the following security functions of the system: based on organisation-defined security functions to include at a minimum, information system authentication and reauthentication
- SC-16 Transmission of Security Parameters, which requires the information system to reliably associate security parameters with information exchanged amongst information systems
- SC-23 Session Authenticity, which requires the information system to provide mechanisms to protect the authenticity of communications sessions

DS7 Educate and Train Users

DS7.1 *Identification of education and training needs* states: 'Establish and regularly update a curriculum for each target group of employees considering:
- Current and future business needs and strategy
- Value of information as an asset
- Corporate values (ethical values, control and security culture, etc.)
- Implementation of new IT infrastructure and software (i.e., packages, applications)
- Current and future skills, competence profiles and certification and/or credentialing needs as well as required reaccreditation
- Delivery methods (e.g., classroom, web-based), target group size, accessibility and timing'

This was mapped with AT-1 Security Awareness and Training Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
- A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment and co-ordination amongst organisational entities and compliance
- Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls

The NIST guidance focuses exclusively on security training.

© 2007 IT Governance Institute. All rights reserved.

DS7.2 *Delivery of training and education* states: 'Based on the identified education and training needs, identify target groups and their members, efficient delivery mechanisms, teachers, trainers and mentors. Appoint trainers and organise timely training sessions. Record registration (including prerequisites), attendance and training session performance evaluations'.

This was mapped with:
- AT-3 Security Training, which requires the organisation to identify personnel with significant information systems security roles and responsibilities, document those roles and responsibilities, and provide appropriate information system security training before authorising access to the system, when required by system changes, and based on the organisation-defined frequency thereafter
- AT-4 Security Training Records, which requires the organisation to document and monitor individual information systems security training activities, including basic security awareness training and specific information systems security training

The NIST guidance focuses exclusively on security training.

DS8 Manage Service Desk and Incidents

DS8.1 *Service desk* states: 'Establish a service desk function, which is the user interface with IT, to register, communicate, dispatch and analyse all calls, reported incidents, service requests and information demands. There should be monitoring and escalation procedures based on agreed-upon service levels relative to the appropriate SLA that allow classification and prioritisation of any reported issue as an incident, service request or information request. Measure end users' satisfaction with the quality of the service desk and IT services'.

This was mapped with IR-7 Incident Response Assistance, which requires the organisation to provide an incident response support resource that offers advice and assistance to users of the information system for the handling and reporting of security incidents. The support resource is an integral part of the organisation's incident response capability.

Because the NIST guidance is focused only on security issues, the only help desk features are associated with support to security incidents.

DS8.2 *Registration of customer queries* states: 'Establish a function and system to allow logging and tracking of calls, incidents, service requests and information needs. It should work closely with such processes as incident management, problem management, change management, capacity management and availability management. Incidents should be classified according to a business and service priority and routed to the appropriate problem management team where necessary. Customers should be kept informed of the status of their queries'.

This was mapped with:
- IR-1 Incident Response Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls
- IR-4 Incident Handling, which requires the organisation to implement an incident-handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery
- IR-5 Incident Monitoring, which requires the organisation to track and document information systems security incidents on an ongoing basis

Because the NIST guidance is focused only on security issues, the only help desk features are associated with support to security incidents.

DS8.4 *Incident closure* states: 'Establish procedures for the timely monitoring of clearance of customer queries. When the incident has been resolved, ensure that the service desk records the resolution steps, and confirm that the action taken has been agreed to by the customer. Also record and report unresolved incidents (known errors and workarounds) to provide information for proper problem management'.

This was mapped with IR-5 Incident Monitoring, which requires the organisation to track and document information systems security incidents on an ongoing basis.

Because the NIST guidance is focused only on security issues, the only help desk features are associated with support to security incidents.

DS9 Manage the Configuration

DS9.1 *Configuration repository and baseline* states: 'Establish a supporting tool and a central repository to contain all relevant information on configuration items. Monitor and record all assets and changes to assets. Maintain a baseline of configuration items for every system and service as a checkpoint to which to return after changes'.

© 2007 IT Governance Institute. All rights reserved.

This was mapped with:
- CM-1 Configuration Management Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls
- CM-2 Baseline Configuration and System Component Inventory, which requires the organisation to develop, document, and maintain a current baseline configuration of the information system, an inventory of the systems' constituent components, and the relevant ownership information

DS9.2 *Identification and maintenance of configuration items* states: 'Establish configuration procedures to support management and logging of all changes to the configuration repository. Integrate these procedures with change management, incident management and problem management procedures'.

This was mapped with CM-3 Configuration Change Control, which requires that the organisation to document and control changes to the information system. Appropriate organisational officials approve information systems changes in accordance with organisational policies and procedures.

DS9.3 *Configuration integrity review* states: 'Periodically review the configuration data to verify and confirm the integrity of the current and historical configuration. Periodically review installed software against the policy for software usage to identify personal or unlicensed software or any software instances in excess of current license agreements. Report, act on and correct errors and deviations'.

This was mapped with:
- CM-4 Monitoring Configuration Changes, which requires the organisation to monitor changes to the information system, conducting security impact analyses to determine the effects of the changes
- SA-6 Software Usage Restrictions, which requires the organisation to comply with software usage restrictions
- SA-7 User Installed Software, which requires the organisation to enforce explicit rules governing the installation of software by users.

The supplemental guidance to SA-6 is quite explicit about personal or unlicensed software. Software and associated documentation are used in accordance with contract agreements and copyright laws. For software and associated documentation protected by quantity licences, the organisation employs tracking systems to control copying and distribution. The organisation controls and documents the use of publicly accessible peer-to-peer file sharing technology to ensure that this capability is not used for the unauthorised distribution, display, performance or reproduction of copyrighted work.

DS11 Manage Data

DS11.1 *Business requirements for data management* states: 'Verify that all data expected for processing are received and processed completely, accurately and in a timely manner, and all output is delivered in accordance with business requirements. Support restart and reprocessing needs'.

This was mapped with:
- MP-1 Media Protection Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls
- SI-10 Information Accuracy, Completeness, Validity and Authenticity, which requires the information system to check information for accuracy, completeness, validity and authenticity
- SI-12 Information Output Handling and Retention, which requires the organisation to handle and retain output from the information system in accordance with applicable laws, executive orders, directives, policies, regulations, standards and operational requirements

DS11.2 *Storage and retention arrangements* states: 'Define and implement procedures for effective and efficient data storage, retention and archiving to meet business objectives, the organisation's security policy and regulatory requirements'.

This was mapped with MP-4 Media Storage, which requires the organisation to physically control and securely store information systems media within controlled areas.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

DS11.4 *Disposal* states: 'Define and implement procedures to ensure that business requirements for protection of sensitive data and software are met when data and hardware are disposed or transferred'.

This was mapped with:
- MP-5 Media Transport, which requires the organisation to control information media (paper and digital) during transport and restrict the pickup, receipt, transfer and delivery of such media to authorised personnel
- MP-6 Media Sanitisation and Disposal, which requires the organisation to sanitise information systems media, both digital and non-digital, prior to disposal or release for reuse

DS11.5 *Backup and restoration* states: 'Define and implement procedures for backup and restoration of system, application, data and documentation in line with business requirements and the continuity plan'.

This was mapped with:
- CP-9 Information System Backup, which requires the organisation to conduct backups of user-level and system-level information (including system state information) contained in the information system based on the organisation-defined frequency and protect backup information whilst in transit and at the storage location
- CP-10 Information System Recovery and Reconstitution, which requires the organisation to employ mechanisms with supporting procedures to allow the information system to be recovered and reconstituted to a known secure state after a disruption or failure

DS11.6 *Security requirements for data management* states: 'Define and implement policies and procedures to identify and apply security requirements applicable to the receipt, processing, storage and output of data to meet business objectives, the organisation's security policy and regulatory requirements'.

This was mapped with:
- AC-1 Access Control Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls
- AC-3 Access Enforcement, which requires the information system to enforce assigned authorisations for controlling access to the system in accordance with applicable policy
- AC-15 Automated Marking, which requires the information system to mark output using standard naming conventions to identify any special dissemination, handling or distribution instructions
- AC-16 Automated Labelling, which requires the information system to appropriately label information in storage, in process and in transmission
- MP-1 Media Protection Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls
- MP-2 Media Access, which requires the organisation to ensure that only authorised users have access to information in printed form or on digital media removed from the information system.
- MP-3 Media Labeling, which requires the organisation to affix external labels to removable information storage media and information system output indicating the distribution limitations and handling caveats of the information. The organisation exempts the following specific types of media or hardware components from labeling so long as they remain within a secure environment: based on the organisation-defined list of media types and hardware components.
- MP-4 Media Storage, which requires the organisation to physically control and securely store information system media, both paper and digital, based on the highest FIPS 199 security category of the information recorded on the media
- MP-5 Media Transport, which requires the organisation to control information system media (paper and digital) during transport and restrict the pickup, receipt, transfer and delivery of such media to authorised personnel.
- MP-6 Media Sanitation and Disposal, which requires the organisation to control information system media (paper and digital) during transport and restrict the pickup, receipt, transfer and delivery of such media to authorised personnel
- SI-10 Information Accuracy, Completeness, Validity and Authenticity, which requires the information system to check information for accuracy, completeness, validity and authenticity
- SI-12 Information Output Handing and Retention, which requires the organisation to handle and retain output from the information system in accordance with organisational policy and operational requirements

© 2007 IT Governance Institute. All rights reserved.

DS12 Manage the Physical Environment

DS12.1 *Site selection and layout* states: 'Define and select the physical sites for IT equipment to support the technology strategy linked to the business strategy. The selection and design of the layout of a site should take into account the risk associated with natural and man-made disasters, whilst considering relevant laws and regulations, such as occupational health and safety regulations'.

This was mapped with:
- PE-1 Physical and Environmental Protection Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
- PE-18 Location of Information System Components, which requires the organisation to position information systems components within the facility to minimise potential damage from physical and environmental hazards and to minimise the opportunity for unauthorised access

DS12.2 *Physical security measures* states: 'Define and implement physical security measures in line with business requirements to secure the location and the physical assets. Physical security measures must be capable of effectively preventing, detecting and mitigating risks relating to theft, temperature, fire, smoke, water, vibration, terror, vandalism, power outages, chemicals or explosives'.

This was mapped with:
- PE-3 Physical Access Control, which requires the organisation to control all physical access points (including designated entry/exit points) to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and verify individual access authorisations before granting access to the facility. The organisation controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organisation's assessment of risk.
- PE-4 Access Control for Transmission Medium, which requires the organisation to control physical access to information systems distribution and transmission lines within organisational facilities to prevent accidental damage, eavesdropping, in-transit modification, description or physical tampering
- PE-5 Access Control for Display Medium, which requires the organisation to control physical access to information systems devices that display information to prevent unauthorised individuals from observing the display output
- PE-16 Delivery and Removal, which requires the organisation to authorise and control information system-related items entering and exiting the facility and maintains appropriate records of those items
- PE-19 Information Leakage, which requires the organisation to protect the information system from information leakage due to electromagnetic signal emanations

DS12.3 *Physical access* states: 'Define and implement procedures to grant, limit and revoke access to premises, buildings and areas according to business needs, including emergencies. Access to premises, buildings and areas should be justified, authorised, logged and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party'.

This was mapped with:
- PE-2 Physical Access Authorisations, which requires the organisation to develop and keep current a list of personnel with authorised access to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) and issue appropriate authorisation credentials (e.g., badges, identification cards, smart cards). Designated officials within the organisation review and approve the access list and authorisation credentials based on the organisation-defined frequency, at least annually
- PE-6 Monitoring Physical Access, which requires the organisation to monitor physical access to the information system to detect and respond to physical security incidents
- PE-7 Visitor Control, which requires the organisation to control physical access to the information system by authenticating visitors before authorising access to the facility where the information system resides (other than areas designated as publicly accessible)
- PE-8 Access Records, which requires the organisation to maintain visitor access records to the facility where the information system resides (except for those areas within the facility officially designated as publicly accessible) that include:
  - Name and organisation of the person visiting
  - Signature of the visitor
  - Form of identification
  - Date of access
  - Time of entry and departure
  - Purpose of visit
  - Name and organisation of person visited

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

DS12.4 *Protection against environmental factors* states: 'Design and implement measures for protection against environmental factors. Install specialised equipment and devices to monitor and control the environment'.

This was mapped with:
- PE-9 Power Equipment and Power Cabling, which requires the organisation to protect power equipment and power cabling for the information system from damage and destruction
- PE-10 Emergency Shutoff, which requires for specific locations within a facility containing concentrations of information systems resources, the organisation to provide the capability of shutting off power to any information systems component that may be malfunctioning or threatened without endangering personnel by requiring them to approach the equipment
- PE-11 Emergency Power, which requires the organisation to provide a short-term uninterruptible power supply to facilitate an orderly shutdown of the information system in the event of a primary power source loss
- PE-12 Emergency Lighting, which requires the organisation to employ and maintain automatic emergency lighting that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes
- PE-13 Fire Protection, which requires the organisation to employ and maintain fire suppression and detection devices/systems that can be activated in the event of a fire
- PE-14 Temperature and Humidity Controls, which requires the organisation to regularly maintain within acceptable levels, and monitor the temperature and humidity within the facility where the information system resides
- PE-15 Water Damage Protection, which requires the organisation to protect the information system from water damage resulting from broken plumbing lines or other sources of water leakage by ensuring that master shut-off valves are accessible, working properly and known to key personnel

DS12.5 *Physical facilities management* states: 'Manage facilities, including power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines'.

This was mapped with PE-1 Physical and Environmental Protection Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
- A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
- Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls

MONITOR AND EVALUATE

ME2 Monitor and Evaluate Internal Control

ME2.7 *Remedial actions* states: 'Identify, initiate, track and implement remedial actions arising from control assessments and reporting'.

This was mapped with CA-5 Plan of Action and Milestones, which requires the organisation to develop and update, based on the organisation-defined frequency, a plan of action and milestones for the information system that document the organisation's planned, implemented and evaluated remedial actions to correct deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system.

ME3 Ensure Compliance With External Requirements

ME3.1 *Identification of external legal, regulatory and contractual compliance requirements* states: 'Identify, on a continuous basis, local and international laws, regulations, and other external requirements that must be complied with for incorporation into the organisation's IT policies, standards, procedures and methodologies'.

This was mapped with SA-9 External Information System Services, which requires the organisation to ensure that third-party providers of outsourced information systems services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance and established SLAs. The organisation monitors security control compliance.

ME3.3 *Evaluation of compliance with external requirements* states: 'Confirm compliance of IT policies, standards, procedures and methodologies with legal and regulatory requirements'.

This was mapped with SA-9 External Information System Services, which requires the organisation to ensure that third-party providers of outsourced information systems services employ adequate security controls in accordance with applicable federal laws, directives, policies, regulations, standards, guidance and established SLAs. The organisations monitors security control compliance.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

PROCESS CONTROL OBJECTIVES

PC2 Process Ownership states: 'Assign an owner for each IT process, and clearly define the roles and responsibilities of the process owner. Include, for example, responsibility for process design, interaction with other processes, accountability for the end results, measurement of process performance and the identification of improvement opportunities'.

This was mapped with AU-1 Audit and Accountability Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
- A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
- Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls

PC4 Roles and Responsibilities states: 'Define the key activities and end deliverables of the process. Assign and communicate unambiguous roles and responsibilities for effective and efficient execution of the key activities and their documentation as well as accountability for the process end deliverables'.

This was mapped with PL-4 Rules of Behaviour, which requires the organisation to establish and make readily available to all information systems users a set of rules that describes their responsibilities and expected behaviour with regard to information and information systems usage. The organisation receives signed acknowledgement from users indicating that they have read, understand and agree to abide by the rules of behaviour, before authorising access to the information system and its resident information.

PC5 Policy, Plans and Procedures states: 'Define and communicate how all policies, plans and procedures that drive an IT process are documented, reviewed, maintained, approved, stored, communicated and used for training. Assign responsibilities for each of these activities and, at appropriate times, review whether they are executed correctly. Ensure that the policies, plans and procedures are accessible, correct, understood and up to date'.

This was mapped with:
- AC-1 Access Control Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented access control policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the access control policy and associated access controls
- AT-1 Security Awareness and Training Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented security awareness and training policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the security awareness and training policy and associated security awareness and training controls
- AU-1 Audit and Accountability Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls
- CA-1 Certification, Accreditation, and Security Assessment Policies and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - Formal, documented security assessment and certification and accreditation policies that address purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the security assessment and certification and accreditation policies and associated assessment, certification, and accreditation controls
- CM-1 Configuration Management Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

- CP-1 Contingency Planning Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented contingency planning policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the contingency planning policy and associated contingency planning controls
- IA-1 Identification and Authentication Policy and Procedures, which requires organisation to develop, disseminate and periodically review/update:
  - A formal, documented identification and authentication policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls
- IR-1 Incident Response Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented incident response policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the incident response policy and associated incident response controls
- MA-1 System Maintenance Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented information system maintenance policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the information system maintenance policy and associated system maintenance controls
- MP-1 Media Protection Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented media protection policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the media protection policy and associated media protection controls
- PE-1 Physical and Environmental Protection Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls
- PL-1 Security Planning Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented security planning policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the security planning policy and associated security planning controls
- PS-1 Personnel Security Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented personnel security policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the personnel security policy and associated personnel security controls
- RA-1 Risk Assessment Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls
- SA-1 System and Services Acquisition Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented system and services acquisition policy that includes information security considerations and that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the system
- SC-1 System and Communications Protection Policy and Procedures, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented system and communications protection policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance
  - Formal, documented procedures to facilitate the implementation of the system and communications protection policy and associated system and communications protection controls
- SI-1 System and Information Integrity, which requires the organisation to develop, disseminate and periodically review/update:
  - A formal, documented system and information integrity policy that addresses purpose, scope, roles, responsibilities, management commitment, co-ordination amongst organisational entities and compliance

© 2007 IT Governance Institute. All rights reserved.

– Formal, documented procedures to facilitate the implementation of the system and information integrity policy and associated system and information integrity controls

APPLICATION CONTROL OBJECTIVES

AC1 Source Data Preparation and Authorisation states: 'Ensure that source documents are prepared by authorised and qualified personnel following established procedures, taking into account adequate segregation of duties regarding the origination and approval of these documents. Errors and omissions can be minimised through good input form design. Detect errors and irregularities so they can be reported and corrected'.

This was mapped with SI-9 Information Input Restrictions, which requires the organisation to restrict the information input to the information system to authorised personnel only.

AC2 Source Data Collection and Entry states: 'Establish that data input is performed in a timely manner by authorised and qualified staff. Correction and resubmission of data that were erroneously input should be performed without compromising original transaction authorisation levels. Where appropriate for reconstruction, retain original source documents for the appropriate amount of time'.

This was mapped with:
- SI-9 Information Input Restrictions, which requires the organisation to restrict the information input to the information system to authorised personnel only
- AC-15 Automated Marking, which requires the information system to mark output using standard naming conventions to identify any special dissemination handling or distribution instructions.

AC3 Accuracy, Completeness and Authenticity Checks states: Ensure that transactions are accurate, complete and valid. Validate data that were input, and edit or send back for correction as close to the point of origination as possible.

This was mapped with SI-10 Information Accuracy, Completeness, Validity and Authenticity, which requires the information system to check information for accuracy, completeness, validity and authenticity.

AC4 Processing Integrity and Validity states: 'Maintain the integrity and validity of data throughout the processing cycle. Detection of erroneous transactions does not disrupt the processing of valid transactions'.

This was mapped with SI-10 Information Accuracy, Completeness, Validity and Authenticity, which requires the information system to check information for accuracy, completeness, validity and authenticity.

AC5 Output Review, Reconciliation and Error Handling states: 'Establish procedures and associated responsibilities to ensure that output is handled in an authorised manner, delivered to the appropriate recipient, and protected during transmission; that verification, detection and correction of the accuracy of output occurs; and that information provided in the output is used'.

This was mapped with:
- SI-11 Error Handling, which requires the information system to identify and handle error conditions in an expeditious manner
- SI-12 Information Output Handling and Retention, which requires the organisation to handle and retain output from the information system in accordance with organisational policy and operational requirements.

AC6 Transaction authentication and integrity states: 'Before passing transaction data between internal applications and business/operational functions (in or outside the enterprise), check the data for proper addressing, authenticity of origin and integrity of content. Maintain authenticity and integrity during transmission or transport'.

This was mapped with:
- AU-10 Nonrepudiation, which requires the information system to provide the capability to determine whether a given individual took a particular action
- SC-8 Transmission Integrity, which requires the information system to protect the integrity of transmitted information
- SC-9 Transmission Confidentiality, which requires the information system to protect the confidentiality of transmitted information
- SC-11 Trusted Path, which requires the information system to establish a trusted communications path between the user and the following security functions of the system: based on organisation-defined security functions to include at a minimum, information system authentication and reauthentication
- SC-23 Session Authenticity, which requires the information system to provide mechanisms to protect the authenticity of communications sessions
- SI-10 Information Accuracy, Completeness, Validity and Authenticity, which requires the information system to check information for accuracy, completeness, validity and authenticity

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

RESULT

Figure 13—Detailed Mapping of NIST SP800-53 With CobiT

CobiT 4.1 Control Objective		NIST SP800-53	
		Coverage	Requirements
PO1	**Define a strategic IT plan.**		
PO1.1	IT value management	A	SA-2
PO1.2	Business-IT alignment	N/A	
PO1.3	Assessment of current capability and performance	A	CA-7
PO1.4	IT strategic plan	A	PL-2, PL-3
PO1.5	IT tactical plans	N/A	
PO1.6	IT portfolio management	A	CM-2
PO2	**Define the information architecture.**		
PO2.1	Enterprise information architecture model	A	CM-1, CM-2
PO2.2	Enterprise data dictionary and data syntax rules	N/A	
PO2.3	Data classification scheme	A	AC-3, AC-15, AC-16
PO2.4	Integrity management	C	SI-1, SI-4, SI-7, SI-10
PO3	**Determine technological direction.**		
PO3.1	Technological direction planning	N/A	
PO3.2	Technical infrastructure plan	N/A	
PO3.3	Monitor future trends and regulations	N/A	
PO3.4	Technology standards	N/A	
PO3.5	IT architecture board	N/A	
PO4	**Define the IT processes, organisation and relationships.**		
PO4.1	IT process framework	N/A	
PO4.2	IT strategy committee	N/A	
PO4.3	IT steering committee	N/A	
PO4.4	Organisational placement of the IT function	N/A	
PO4.5	IT organisational structure	N/A	
PO4.6	Establishment of roles and responsibilities	A	PS-1
PO4.7	Responsibility for IT quality assurance	N/A	
PO4.8	Responsibility for risk, security and compliance	N/A	
PO4.9	Data and system ownership	N/A	
PO4.10	Supervision	A	AC-13
PO4.11	Segregation of duties	A	AC-5, AC-6
PO4.12	IT staffing	N/A	
PO4.13	Key IT personnel	A	PS-2
PO4.14	Contracted staff policies and procedures	A	PS-7
PO4.15	Relationships	N/A	
PO5	**Manage the IT investment.**		
PO5.1	Financial management framework	N/A	
PO5.2	Prioritisation within IT budget	A	SA-2
PO5.3	IT budgeting	N/A	
PO5.4	Cost management	N/A	
PO5.5	Benefit management	N/A	

© 2007 IT Governance Institute. All rights reserved.

Figure 13—Detailed Mapping of NIST SP800-53 With CobiT (cont.)

CobiT 4.1 Control Objective		NIST SP800-53 Coverage	NIST SP800-53 Requirements
PO6	**Communicate management aims and direction.**		
PO6.1	IT policy and control environment	N/A	
PO6.2	Enterprise IT risk and control framework	N/A	
PO6.3	IT policies management	N/A	
PO6.4	Policy, standards and procedures rollout	N/A	
PO6.5	Communication of IT objectives and direction	A	PL-4
PO7	**Manage IT human resources.**		
PO7.1	Personnel recruitment and retention	N/A	
PO7.2	Personnel competencies	N/A	
PO7.3	Staffing of roles	A	PS-1, PS-2
PO7.4	Personnel training	A	AT-2, AT-3
PO7.5	Dependence upon individuals	N/A	
PO7.6	Personnel clearance procedures	A	PS-3
PO7.7	Employee job performance evaluation	N/A	
PO7.8	Job change and termination	A	PS-4, PS-5
PO8	**Manage quality.**		
PO8.1	Quality management system	N/A	
PO8.2	IT standards and quality practices	N/A	
PO8.3	Development and acquisition standards	A	SA-3
PO8.4	Customer focus	N/A	
PO8.5	Continuous improvement	N/A	
PO8.6	Quality measurement, monitoring and review	N/A	
PO9	**Assess and manage IT risks.**		
PO9.1	IT risk management alignment	A	RA-1
PO9.2	Establishment of risk context	A	RA-2
PO9.3	Event identification	A	RA-3, RA-5
PO9.4	Risk assessment	A	RA-3, RA-4
PO9.5	Risk response	C	IR-1, IR-4
PO9.6	Maintenance and monitoring of a risk action plan	E	IR-1, IR-4
PO10	**Manage projects.**		
PO10.1	Programme management framework	N/A	
PO10.2	Project management framework	N/A	
PO10.3	Project management approach	N/A	
PO10.4	Stakeholder commitment	N/A	
PO10.5	Project scope statement	N/A	
PO10.6	Project phase initiation	N/A	
PO10.7	Integrated project plan	N/A	
PO10.8	Project resources	N/A	
PO10.9	Project risk management	N/A	
PO10.10	Project quality plan	N/A	
PO10.11	Project change control	N/A	
PO10.12	Project planning of assurance methods	A	CA-1
PO10.13	Project performance measurement, reporting and monitoring	N/A	
PO10.14	Project closure	N/A	

© 2007 IT Governance Institute. All rights reserved.

Figure 13—Detailed Mapping of NIST SP800-53 With CobiT (cont.)			
CobiT 4.1 Control Objective		NIST SP800-53	
		Coverage	Requirements
AI1	**Identify automated solutions.**		
AI1.1	Definition and maintenance of business functional and technical requirements	A	RA-3
AI1.2	Risk analysis report	N/A	
AI1.3	Feasibility study and formulation of alternative courses of action	N/A	
AI1.4	Requirements and feasibility decision and approval	N/A	
AI2	**Acquire and maintain application software.**		
AI2.1	High-level design	N/A	
AI2.2	Detailed design	N/A	
AI2.3	Application control and auditability	A	AU-2, SI-10
AI2.4	Application security and availability	C	AC-3, IA-2, SA-4, SA-8, SC-2, SI-7, SI-10
AI2.5	Configuring and implementation of acquired application software	A	SA-1
AI2.6	Major upgrades to existing systems	N/A	
AI2.7	Development of application software	A	SA-3
AI2.8	Software quality assurance	A	SA-11
AI2.9	Applications requirements management	N/A	
AI2.10	Application software maintenance	A	MA-2
AI3	**Acquire and maintain technology infrastructure.**		
AI3.1	Technological infrastructure acquisition plan	N/A	
AI3.2	Infrastructure resource protection and availability	N/A	
AI3.3	Infrastructure maintenance	N/A	
AI3.4	Feasibility test environment	N/A	
AI4	**Enable operation and use.**		
AI4.1	Planning for operational solutions	N/A	
AI4.2	Knowledge transfer to business management	N/A	
AI4.3	Knowledge transfer to end users	N/A	
AI4.4	Knowledge transfer to operations and support staff	N/A	
AI5	**Procure IT resources.**		
AI5.1	Procurement control	A	SA-1
AI5.2	Supplier contract management	N/A	
AI5.3	Supplier selection	N/A	
AI5.4	IT resources acquisition	A	SA-4
AI6	**Manage changes.**		
AI6.1	Change standards and procedures	A	CM-1, CM-3
AI6.2	Impact assessment, prioritisation and authorisation	N/A	
AI6.3	Emergency changes	A	CM-3
AI6.4	Change status tracking and reporting	N/A	
AI6.5	Change closure and documentation	N/A	

© 2007 IT Governance Institute. All rights reserved.

Figure 13—Detailed Mapping of NIST SP800-53 With CobiT (cont.)

CobiT 4.1 Control Objective		NIST SP800-53 Coverage	NIST SP800-53 Requirements
AI7	**Install and accredit solutions and changes.**		
AI7.1	Training	N/A	
AI7.2	Test plan	N/A	
AI7.3	Implementation plan	N/A	
AI7.4	Test environment	N/A	
AI7.5	System and data conversion	N/A	
AI7.6	Testing of changes	N/A	
AI7.7	Final acceptance test	A	CA-4, CA-6
AI7.8	Promotion to production	N/A	
AI7.9	Post-implementation review	N/A	
DS1	**Define and manage service levels.**		
DS1.1	Service level management framework	N/A	
DS1.2	Definition of services	N/A	
DS1.3	Service level agreements	N/A	
DS1.4	Operating level agreements	N/A	
DS1.5	Monitoring and reporting of service level achievements	N/A	
DS1.6	Review of service level agreements and contracts	A	SA-9
DS2	**Manage third-party services.**		
DS2.1	Identification of all supplier relationships	N/A	
DS2.2	Supplier relationship management	A	PS-7
DS2.3	Supplier risk management	A	SA-9
DS2.4	Supplier performance monitoring	N/A	
DS3	**Manage performance and capacity.**		
DS3.1	Performance and capacity planning	N/A	
DS3.2	Current performance and capacity	N/A	
DS3.3	Future performance and capacity	N/A	
DS3.4	IT resources availability	N/A	
DS3.5	Monitoring and reporting	N/A	
DS4	**Ensure continuous service.**		
DS4.1	IT continuity framework	E	CP-1, CP-6, CP-7, CP-8
DS4.2	IT continuity plans	C	CP-2, CP-4, CP-9
DS4.3	Critical IT resources	N/A	
DS4.4	Maintenance of the IT continuity plan	C	CP-5
DS4.5	Testing of the IT continuity plan	C	CP-4
DS4.6	IT continuity plan training	C	CP-3
DS4.7	Distribution of the IT continuity plan	N/A	
DS4.8	IT services recovery and resumption	C	CP-7, CP-10
DS4.9	Offsite backup storage	C	CP-6, CP-9
DS4.10	Post-resumption review	N/A	

© 2007 IT Governance Institute. All rights reserved.

Figure 13—Detailed Mapping of NIST SP800-53 With CobiT (cont.)

CobiT 4.1 Control Objective		NIST SP800-53 Coverage	NIST SP800-53 Requirements
DS5	**Ensure systems security.**		
DS5.1	Management of IT security	N/A	
DS5.2	IT security plan	E	PL-1, PL-2, PL-4, SC-1
DS5.3	Identity management	C	IA-1, IA-2, IA-4
DS5.4	User account management	C	AC-2, IA-4, PS-6
DS5.5	Security testing, surveillance and monitoring	E	AU-6, CA-2, CA-6, CA-7, CM-4, RA-5, SI-4
DS5.6	Security incident definition	E	IR-1, IR-6
DS5.7	Protection of security technology	C	PE-4, SA-5, SC-3
DS5.8	Cryptographic key management	C	SC-12, SC-13
DS5.9	Malicious software prevention, detection and correction	C	SC-18, SI-3, SI-7, SI-8
DS5.10	Network security	C	AC-4, SC-7, SI-4
DS5.11	Exchange of sensitive data	E	AU-10, SC-9, SC-11, SC-16, SC-23
DS6	**Identify and allocate costs.**		
DS6.1	Definition of services	N/A	
DS6.2	IT accounting	N/A	
DS6.3	Cost modelling and charging	N/A	
DS6.4	Cost model maintenance	N/A	
DS7	**Educate and train users.**		
DS7.1	Identification of education and training needs	A	AT-1
DS7.2	Delivery of training and education	A	AT-3, AT-4
DS7.3	Evaluation of training received	N/A	
DS8	**Manage service desk and incidents.**		
DS8.1	Service desk	A	IR-7
DS8.2	Registration of customer queries	A	IR-1, IR-4, IR-5
DS8.3	Incident escalation	N/A	
DS8.4	Incident closure	A	IR-5
DS8.5	Reporting and trend analysis	N/A	
DS9	**Manage the configuration.**		
DS9.1	Configuration repository and baseline	C	CM-1, CM-2
DS9.2	Identification and maintenance of configuration items	C	CM-3
DS9.3	Configuration integrity review	C	CM-4, SA-6, SA-7
DS10	**Manage problems.**		
DS10.1	Identification and classification of problems	N/A	
DS10.2	Problem tracking and resolution	N/A	
DS10.3	Problem closure	N/A	
DS10.4	Integration of configuration, incident and problem management	N/A	
DS11	**Manage data.**		
DS11.1	Business requirements for data management	C	MP-1, SI-10, SI-12
DS11.2	Storage and retention arrangements	C	MP-4
DS11.3	Media library management system	N/A	
DS11.4	Disposal	C	MP-5, MP-6
DS11.5	Backup and restoration	C	CP-9, CP-10
DS11.6	Security requirements for data management	E	AC-1, AC-3, AC-15, AC-16, MP-1, MP-2, MP-3, MP-4, MP-5, MP-6, SI-10, SI-12

© 2007 IT Governance Institute. All rights reserved.

Figure 13—Detailed Mapping of NIST SP800-53 With CobiT (cont.)

CobiT 4.1 Control Objective		NIST SP800-53 Coverage	NIST SP800-53 Requirements
DS12	**Manage the physical environment.**		
DS12.1	Site selection and layout	C	PE-1, PE-18
DS12.2	Physical security measures	E	PE-3, PE-4, PE-5, PE-16, PE-19
DS12.3	Physical access	C	PE-2, PE-6, PE-7, PE-8
DS12.4	Protection against environmental factors	E	PE-9, PE-10, PE-11, PE-12, PE-13, PE-14, PE-15
DS12.5	Physical facilities management	A	PE-1
DS13	**Manage operations.**		
DS13.1	Operations procedures and instructions	N/A	
DS13.2	Job scheduling	N/A	
DS13.3	IT infrastructure monitoring	N/A	
DS13.4	Sensitive documents and output devices	N/A	
DS13.5	Preventive maintenance for hardware	N/A	
ME1	**Monitor and evaluate IT performance.**		
ME1.1	Monitoring approach	N/A	
ME1.2	Definition and collection of monitoring data	N/A	
ME1.3	Monitoring method	N/A	
ME1.4	Performance assessment	N/A	
ME1.5	Board and executive reporting	N/A	
ME1.6	Remedial actions	N/A	
ME2	**Monitor and evaluate internal control.**		
ME2.1	Monitoring of internal control framework	N/A	
ME2.2	Supervisory review	N/A	
ME2.3	Control exceptions	N/A	
ME2.4	Control self-assessment	N/A	
ME2.5	Assurance of internal control	N/A	
ME2.6	Internal control at third parties	N/A	
ME2.7	Remedial actions	A	CA-5
ME3	**Ensure compliance with external requirements.**		
ME3.1	Identification of external legal, regulatory and contractual compliance requirements	N/A	SA-9
ME3.2	Optimisation of response to external requirements	N/A	
ME3.3	Evaluation of compliance with external requirements	N/A	SA-9
ME3.4	Positive assurance of compliance	N/A	
ME3.5	Integrated reporting	N/A	
ME4	**Provide IT governance.**		
ME4.1	Establishment of an IT governance framework	N/A	
ME4.2	Strategic alignment	N/A	
ME4.3	Value delivery	N/A	
ME4.4	Resource management	N/A	
ME4.5	Risk management	N/A	
ME4.6	Performance measurement	N/A	
ME4.7	Independent assurance	N/A	

© 2007 IT Governance Institute. All rights reserved.

Figure 13—Detailed Mapping of NIST SP800-53 With CobiT (cont.)

CobiT 4.1 Control Objective		NIST SP800-53 Coverage	NIST SP800-53 Requirements
PC	**Process Control Objectives**		
PC1	Process goals and objectives	N/A	
PC2	Process ownership	A	AU-1
PC3	Process repeatability	N/A	
PC4	Roles and responsibilities	A	PL-4
PC5	Policy, plans and procedures	C	AC-1, AT-1, AU-1, CA-1, CM-1, CP-1, IA-1, IR-1, MA-1, MP-1, PE-1, PL-1, PS-1, RA-1, SA-1, SC-1, SI-1
PC6	Process performance improvement	N/A	
AC	**Application Controls Objectives**		
AC1	Source data preparation and authorisation	A	SI-9
AC2	Source data collection and entry	A	SI-9, AC-15
AC3	Accuracy, completeness and authenticity checks	A	SI-10
AC4	Processing integrity and validity	A	SI-10
AC5	Output review, reconciliation and error handling	A	SI-11, SI-12
AC6	Transaction authentication and integrity	E	AU-10, SC-8, SC-9, SC-11, SC-23, SI-10

Legend: (E) Exceeded
(C) Complete coverage
(A) Some aspects are addressed.
(N/A) Not addressed

© 2007 IT Governance Institute. All rights reserved.

7. REFERENCES

IT Governance Institute, COBIT 4.1, USA, 2007

National Institute of Standards and Technology, Computer Security Division, Information Technology Laboratory, USA:
• FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*
• FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems*
• SP800-18, *Guide for Developing Security Plans for Federal Information Systems*
• SP800-26, *Security Self-Assessment Guide for Information Technology Systems*
• SP800-30, *Risk Management Guide for Information Technology Systems*
• SP800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems*
• SP800-39, *Managing Risks from Information Systems: An Organizational Perspective* (Initial Public Draft)
• SP800-53 Rev 1, *Recommended Security Controls for Federal Information Systems*
• SP800-53A, *Guide for Assessing the Security Controls in Federal Information Systems, Second Public Draft*
• SP800-60, *Guide for Mapping Types of Information and Information Systems to Security Categories*
• SP800-70, *Security Configuration Checklists Program for IT Products*
• SP800-80, *Guide for Developing Performance Metrics for Information Security*
• SP800-100, *Information Security Handbook: A Guide for Managers*

Paulk, M.C.; *et al*; 'Capability Maturity Model℠ for Software', CMU/SEI-93-TR-24, Carnegie Mellon University, Software Engineering Institute, USA, 1993

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

APPENDIX—COBIT AND RELATED PRODUCTS

The COBIT framework, in versions 4.1 and higher, includes all of the following:
- Framework—Explains how COBIT organises IT governance, management and control objectives and good practices by IT domains and processes, and links them to business requirements
- Process descriptions—Include 34 IT processes covering the IT responsibility areas from beginning to end
- Control objectives—Provide generic best practice management objectives for IT processes
- Management guidelines—Offer tools to help assign responsibility, measure performance, and benchmark and address gaps in capability
- Maturity models—Provide profiles of IT processes describing possible current and future states

In the years since its inception, COBIT's core content has continued to evolve, and the number of COBIT-based derivative works has increased. Following are the publications currently derived from COBIT:
- *Board Briefing on IT Governance, 2nd Edition*—Designed to help executives understand why IT governance is important, what its issues are and what their responsibility is for managing it
- COBIT® Online—Allows users to customise a version of COBIT for their own enterprise, then store and manipulate that version as desired. It offers online, real-time surveys, frequently asked questions, benchmarking and a discussion facility for sharing experiences and questions.
- *COBIT® Control Practices: Guidance to Achieve Control Objectives for Successful IT Governance, 2nd Edition*—Provides guidance on the risks to be avoided and value to be gained from implementing a control objective, and instruction on how to implement the objective. Control practices are strongly recommended for use with the *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*.
- *IT Assurance Guide: Using COBIT®*—Provides guidance on how COBIT can be used to support a variety of assurance activities and offers suggested testing steps for all the COBIT IT processes and control objectives. It replaces the information in the *Audit Guidelines* for auditing and self-assessment against the control objectives in COBIT® 4.1.
- *IT Control Objectives for Sarbanes-Oxley: The Role of IT in the Design and Implementation of Internal Control Over Financial Reporting, 2nd Edition*—Provides guidance on how to assure compliance for the IT environment based on the COBIT control objectives
- *IT Governance Implementation Guide: Using COBIT® and Val IT™, 2nd Edition*—Provides a generic road map for implementing IT governance using COBIT and Val IT resources and a supporting tool kit
- *COBIT® Quickstart, 2nd Edition*—Provides a baseline of control for the smaller organisation and a possible first step for the larger enterprise
- *COBIT® Security Baseline: An Information Security Survival Kit, 2nd Edition*—Focuses on essential steps for implementing information security within the enterprise
- COBIT Mappings—Currently posted at *www.isaca.org/downloads*:
  - *Aligning COBIT, ITIL and ISO 17799 for Business Benefit*
  - *COBIT® Mapping: Mapping of CMMI for Development V1.2 With COBIT 4.0*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2000 With COBIT, 2nd Edition*
  - *COBIT® Mapping: Mapping of ISO/IEC 17799:2005 With COBIT 4.0*
  - *COBIT® Mapping: Mapping of ITIL With COBIT 4.0*
  - *COBIT® Mapping: Mapping of PMBOK With COBIT 4.0*
  - *COBIT® Mapping: Mapping of PRINCE2 With COBIT 4.0*
  - *COBIT® Mapping: Mapping of SEI's CMM for Software With COBIT 4.0*
  - *COBIT® Mapping: Mapping of TOGAF 8.1 With COBIT 4.0*
  - *COBIT® Mapping: Overview of International IT Guidance, 2nd Edition*
- *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition*—Presents information security in business terms and contains tools and techniques to help uncover security-related problems

Val IT is the umbrella term used to describe the publications and future additional products and activities addressing the Val IT framework.

Current Val IT-related publications are:
- *Enterprise Value: Governance of IT Investments—The Val IT™ Framework*, which explains how an enterprise can extract optimal value from IT-enabled investments and is based on the COBIT framework. It is organised into:
  - Three processes—Value Governance, Portfolio Management and Investment Management
  - IT key management practices—Essential management practices that positively influence the achievement of the desired result or purpose of a particular activity. They support the Val IT processes and play roughly the same role as COBIT's control objectives.
- *Enterprise Value: Governance of IT Investments—The Business Case*, which focuses on one key element of the investment management process
- *Enterprise Value: Governance of IT Investments—The ING Case Study*, which describes how a global financial services company manages a portfolio of IT investments in the context of the Val IT framework

For the most complete and up-to-date information on COBIT, Val IT and related products, case studies, training opportunities, newsletters and other framework-specific information, visit *www.isaca.org/cobit* and *www.isaca.org/valit*.

© 2007 IT GOVERNANCE INSTITUTE. ALL RIGHTS RESERVED.

LEADING THE IT GOVERNANCE COMMUNITY

3701 ALGONQUIN ROAD, SUITE 1010
ROLLING MEADOWS, IL 60008 USA
PHONE: +1.847.660.5700
FAX: +1.847.253.1443
E-MAIL: *info@itgi.org*
WEB SITE: *www.itgi.org*

ISBN 978-1-60420-034-8