ISACA®
Trust in, and value from, information systems

COBIT® 5

for Information Security

PREVIEW VERSION

COBIT® 5

AN ISACA® FRAMEWORK

The following pages provide a preview of the information contained in *COBIT 5 for Information Security*. The publication provides guidance to help IT and Security professionals understand, utilize, implement and direct important information-security related activities and make more informed decisions.

COBIT 5 for Information Security is a major strategic evolution of COBIT 5—the only business framework for the governance and management of enterprise IT. This evolutionary version incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems.

To purchase *COBIT 5 for Information Security*, visit www.isaca.org/cobit5info-sec

Not a member? Learn the value of ISACA membership. Additional information is available at www.isaca.org/membervalue.

ISACA®
With more than 100,000 constituents in 180 countries, ISACA (*www.isaca.org*) is a leading global provider of knowledge, certifications, community, advocacy and education on information systems (IS) assurance and security, enterprise governance and management of IT, and IT-related risk and compliance. Founded in 1969, the nonprofit, independent ISACA hosts international conferences, publishes the *ISACA® Journal*, and develops international IS auditing and control standards, which help its constituents ensure trust in, and value from, information systems. It also advances and attests IT skills and knowledge through the globally respected Certified Information Systems Auditor® (CISA®), Certified Information Security Manager® (CISM®), Certified in the Governance of Enterprise IT® (CGEIT®) and Certified in Risk and Information Systems Control™ (CRISC™) designations.

ISACA continually updates and expands the practical guidance and product family based on the COBIT framework. COBIT helps IT professionals and enterprise leaders fulfill their IT governance and management responsibilities, particularly in the areas of assurance, security, risk and control, and deliver value to the business.

Disclaimer
ISACA has designed this publication, *COBIT® 5 for Information Security* (the 'Work'), primarily as an educational resource for security professionals. ISACA makes no claim that use of any of the Work will assure a successful outcome. The Work should not be considered inclusive of all proper information, procedures and tests or exclusive of other information, procedures and tests that are reasonably directed to obtaining the same results. In determining the propriety of any specific information, procedure or test, security professionals should apply their own professional judgement to the specific circumstances presented by the particular systems or information technology environment.

ISACA
3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008 USA
Phone: +1.847.253.1545
Fax: +1.847.253.1443
Email: *info@isaca.org*
Web site: *www.isaca.org*

Feedback: *www.isaca.org/cobit*
Participate in the ISACA Knowledge Center: *www.isaca.org/knowledge-center*
Follow ISACA on Twitter: *https://twitter.com/ISACANews*
Join the COBIT conversation on Twitter: #COBIT
Join ISACA on LinkedIn: ISACA (Official), *http://linkd.in/ISACAOfficial*
Like ISACA on Facebook: *www.facebook.com/ISACAHQ*

COBIT® 5 for Information Security
ISBN 978-1-60420-255-7
Printed in the United States of America
1

Table of Contents

List of Figures

EXECUTIVE SUMMARY

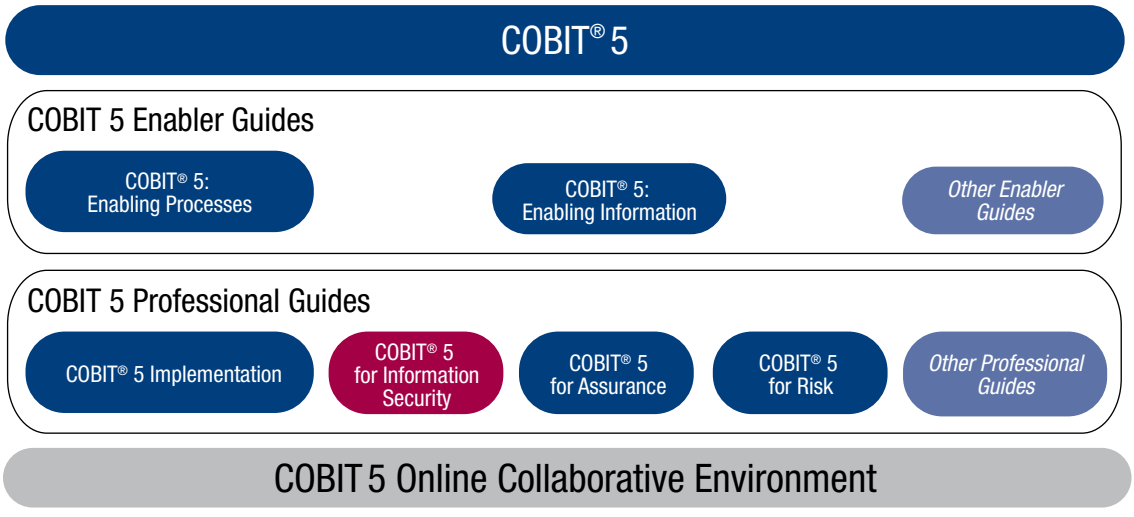
Introduction

Information is a key resource for all enterprises and, from the time information is created to the moment it is destroyed, technology plays a significant role. Technology is increasingly advanced and has become pervasive in enterprises and the social, public and business environments.

COBIT 5 provides a comprehensive framework that assists enterprises in achieving their objectives for the governance and management of enterprise IT. Simply stated, it helps enterprises create optimal value from information technology (IT) by maintaining a balance between realising benefits and optimising risk levels and resource use. COBIT 5 enables IT to be governed and managed in a holistic manner for the entire enterprise, taking into account the full end-to-end business and IT functional areas of responsibility, considering the IT-related interests of internal and external stakeholders.

COBIT 5 for Information Security, highlighted in **figure 1**, builds on the COBIT 5 framework in that it focusses on information security and provides more detailed and more practical guidance for information security professionals and other interested parties at all levels of the enterprise (see **figure 2**).

Figure 1—COBIT 5 Product Family

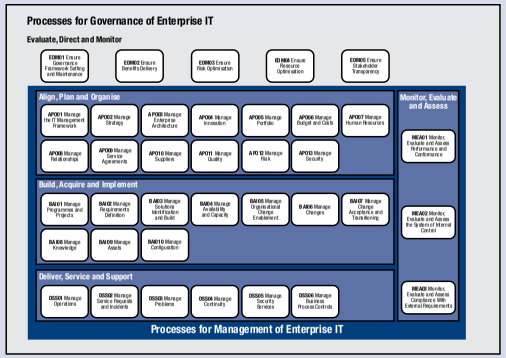


Drivers

In COBIT 5, the processes APO13 *Manage security*, DSS04 *Manage continuity* and DSS05 *Manage security services* provide basic guidance on how to define, operate and monitor a system for general security management. However, the assumption made in this publication is that information security is pervasive throughout the entire enterprise, with information security aspects in every activity and process performed. Therefore, *COBIT 5 for Information Security* provides the next generation of ISACA's guidance on the enterprise governance and management of information security.

The major drivers for the development of *COBIT 5 for Information Security* include:
- The need to describe information security in an enterprise context including:
  - The full end-to-end business and IT functional responsibilities of information security
  - All aspects that lead to effective governance and management of information security, such as organisational structures, policies and culture
  - The relationship and link of information security to enterprise objectives
- An ever-increasing need for the enterprise to:
  - Maintain information risk at an acceptable level and to protect information against unauthorised disclosure, unauthorised or inadvertent modifications, and possible intrusions.
  - Ensure that services and systems are continuously available to internal and external stakeholders, leading to user satisfaction with IT engagement and services.
  - Comply with the growing number of relevant laws and regulations as well as contractual requirements and internal policies on information and systems security and protection, and provide transparency on the level of compliance.
  - Achieve all of the above while containing the cost of IT services and technology protection.

Figure 2—COBIT 5 as it Relates to Information Security



Section II, Chapter 3
Detailed Guidance: Appendix B

Information Security-specific Organisational Structures

- Chief information security officer (CISO)
- Information security steering committee (ISSC)
- Information security manager (ISM)
- Other related roles and structures

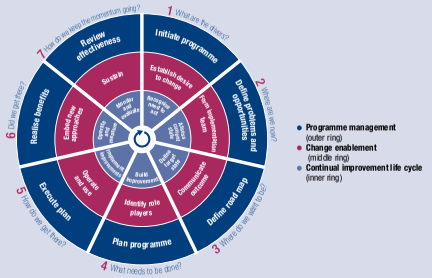
Section II, Chapter 4
Detailed Guidance: Appendix C

Desired Information Security-specific Culture, Ethics and Behaviour

- Information security is practiced in daily operations.
- People respect the policies and principles.
- People are provided with sufficient and detailed guidance, and are encouraged to participate in and challenge the current situation.
- Everyone is accountable for protection.
- Stakeholders identify and respond to threats to the enterprise.
- Management proactively supports and anticipates innovations.
- Business management engages in continuous cross-functional collaboration.
- Executive management recognises the business value.

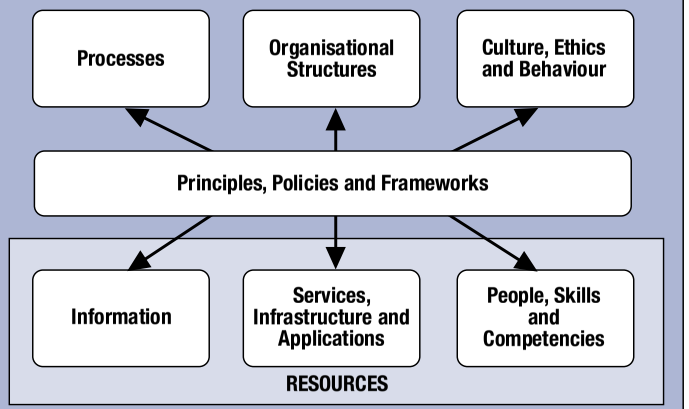
Section II, Chapter 5
Detailed Guidance: Appendix D

Adapting *COBIT 5 for Information Security* to the Environment

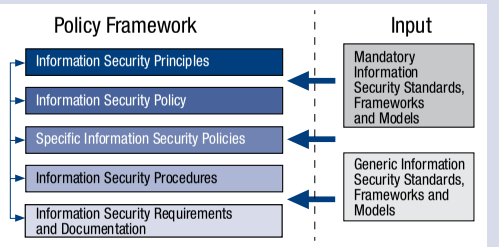


Section III

COBIT 5 ENABLERS



Information Security-specific Principles, Policies and Frameworks



Section II, Chapter 2
Detailed Guidance: Appendix A

Information Security-specific Information Types

- Information security strategy
- Information security budget
- Information security plan
- Policies
- Information security requirements
- Awareness material
- Information security review reports
- Information risk profile
- Information security dashboard

Section II, Chapter 6
Detailed Guidance: Appendix E

Information Security-specific Services, Infrastructure and Applications

- Provide a security architecture.
- Provide security awareness.
- Provide secure development.
- Provide security assessments.
- Provide adequately secured and configured systems.
- Provide user access and access rights.
- Provide adequate protection against external attacks and intrusion attempts.
- Provide adequate incident response.
- Provide security testing.
- Provide monitoring and alert services.

Section II, Chapter 7
Detailed Guidance: Appendix F

Information Security-specific People, Skills and Competencies

- Information security govenance
- Information security strategy formulation
- Information risk management
- Information security architecture development
- Information security operations
- Information assessment and testing and compliance

Section II, Chapter 8
Detailed Guidance: Appendix G

- The need to connect to, and, where relevant, align with, other major frameworks and standards in the marketplace. The (non-exhaustive) mapping (**appendix H**) will help stakeholders understand how various frameworks, good practices and standards are positioned relative to each other and how they can be used together and complement each other under the umbrella of *COBIT 5 for Information Security*.
- The need to link together all major ISACA research, frameworks and guidance, with a primary focus on the Business Model for Information Security (BMIS) and COBIT, but also considering Val IT, Risk IT, the IT Assurance Framework (ITAF), the publication titled *Board Briefing on IT Governance* and the Taking Governance Forward (TGF) resource.

In addition to these major drivers for the development of *COBIT 5 for Information Security* is the fact that information security is essential in the day-to-day operations of enterprises. Breaches in information security can lead to a substantial impact within the enterprise through, for example, financial or operational damages. In addition, the enterprise can be exposed to external impacts such as reputational or legal risk, which can jeopardise customer or employee relations or even endanger the survival of the enterprise.

The need for stronger, better and more systematic approaches for information security is illustrated in the following examples:
- A national critical infrastructure depends on information systems, and successful intrusions can result in a significant impact to economies or human safety.
- Non-public financial information can be used for economic gain.
- Disclosure of confidential information can generate embarrassment to enterprises, cause damage to reputations or jeopardise business relations.
- Intrusion in commercial networks, for example, to obtain credit card or other payment-related data, can lead to substantial reputational and financial damage due to fines, as well as increased scrutiny from regulatory bodies.
- Industrial espionage can enable trade secrets to be imitated and increase competition for manufacturing enterprises.
- Leakage of national or military intelligence can result in damage to political relationships.
- Personal data leaks can result in financial loss and unnecessary efforts to rebuild an individual's financial reputation.
- Significant unplanned costs (both financial and operational) related to containing, investigating and remediating security breaches can impact any enterprise that has suffered a breach.

Benefits

Using *COBIT 5 for Information Security* brings a number of information security-related capabilities to the enterprise, which can result in a number of enterprise benefits such as:
- Reduced complexity and increased cost-effectiveness due to improved and easier integration of information security standards, good practices and/or sector-specific guidelines
- Increased user satisfaction with information security arrangements and outcomes
- Improved integration of information security in the enterprise
- Informed risk decisions and risk awareness
- Improved prevention, detection and recovery
- Reduced (impact of) information security incidents
- Enhanced support for innovation and competitiveness
- Improved management of costs related to the information security function
- Better understanding of information security

These benefits are obtained by leveraging the *COBIT 5 for Information Security* capabilities shown in **figure 3**.

Figure 3—*COBIT 5 for Information Security* Capabilities	
***COBIT 5 for Information Security* Capability**	**Description**
Up-to-date view on governance	*COBIT 5 for Information Security* provides the most up-to-date view on information security governance and management through alignment with COBIT 5, International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 38500 and other IT governance initiatives. During the development of *COBIT 5 for Information Security*, the most important guidance and standards were analysed. *COBIT 5 for Information Security* aligns with other major frameworks, standards and models in the marketplace, such as the ISO/IEC 27000 series, the Information Security Forum (ISF) Standard of Good Practice, and BMIS. Additionally, ISACA's information security governance offerings, *Information Security Governance: Guidance for Information Security Managers* and *Information Security Governance: Guidance for Boards of Directors and Executive Management, 2nd Edition* were analysed during the development of *COBIT 5 for Information Security*.
Clear distinction between governance and management	COBIT 5 clarifies the roles of governance and management and provides a clear distinction between them, with a revised process model reflecting this distinction and showing how they relate to each other.
End-to-end view	*COBIT 5 for Information Security* is a process model that integrates both business and IT functional responsibilities. It provides a clear distinction between information security governance and information security management practices, outlining responsibilities at various levels of the enterprise, encompassing all process steps from the beginning to the end.
Holistic guidance	The *COBIT 5 for Information Security* framework brings together comprehensive and holistic guidance on information security. Holistic means that attention is paid not only to processes, but to all enablers, including information, structures, culture, policies and their interdependence.

COBIT 5 for Information Security is based on the COBIT 5 framework, from which all information security-relevant information has been filtered and complemented with more detailed and specific guidance, therefore ensuring consistency with the COBIT 5 product architecture. COBIT 5 starts from stakeholder expectations and concerns related to enterprise IT. All guidance can be related back to stakeholder issues, and thus information security assists to support the mission of the business and achievement of business goals.

Target Audience

COBIT 5 for Information Security is intended for all stakeholders of information security. Chief information security officers (CISOs), information security managers (ISMs) and other information security professionals are the most obvious target audience. However, information security is the responsibility of all stakeholders of the enterprise, including all staff members, and other stakeholders, including third parties. Therefore, this publication may be of interest to all stakeholders in the enterprise.

Conventions Used and Overview

COBIT 5 for Information Security refers to a number of enablers such as roles and job titles, committees and boards, processes, and policies. The unique characteristics of each enterprise will cause these enablers to be used in many different ways to provide information security in an optimal manner. *COBIT 5 for Information Security* uses guidance and examples to provide a pervasive view that explains each concept of COBIT 5 from an information security perspective.

To guide the reader through the vast collection of information, *COBIT 5 for Information Security* follows a set structure consisting of three sections and eight appendices.

Each section contains several chapters. Within a chapter, as required, signposting is used to guide the reader throughout the explanation. In addition, blue and grey information boxes are used:
- A blue box calls out attention points relevant for information security.
- A grey box highlights material that is given to link the information with other relevant items. The sections also refer to the appendices for more specific information.

Each section and its interconnections with other sections is described as follows:
- **Section I**—Elaborates on **information security** and describes briefly how the COBIT 5 architecture can be tailored to information security-specific needs. This section provides a conceptual baseline that is followed throughout the rest of the publication.
- **Section II**—Elaborates on **the use of COBIT 5 enablers for implementing information security**. Governance of enterprise IT is systemic and supported by a set of enablers. In this section, the concept of the security-specific enablers is introduced and explained using practical examples. Detailed guidance regarding these enablers is provided in the appendices.
- **Section III**—Elaborates on how **to adapt *COBIT 5 for Information Security* to the enterprise environment**. This section contains guidance on how information security initiatives can be implemented and contains a mapping with other standards and frameworks in the area of information security and *COBIT 5 for Information Security*.

The **appendices** contain detailed guidance based on the enablers introduced in section II:
- **Appendix A**—Detailed guidance regarding the principles, policies and frameworks enabler
- **Appendix B**—Detailed guidance regarding the processes enabler
- **Appendix C**—Detailed guidance regarding the organisational structures enabler
- **Appendix D**—Detailed guidance regarding the culture, ethics and behaviour enabler
- **Appendix E**—Detailed guidance regarding the information enabler
- **Appendix F**—Detailed guidance regarding the services, infrastructure and applications enabler
- **Appendix G**—Detailed guidance regarding the people, skills and competencies enabler
- **Appendix H**—Detailed mappings of *COBIT 5 for Information Security* to other information security standards

The **Acronyms** and **Glossary** sections clarify the abbreviations and terms used exclusively in this publication. For standardised terms, please refer to the ISACA Glossary of Terms located at *www.isaca.org/Glossary*.

Section I. Information Security

Chapter 1
Information Security Defined

ISACA defines information security as something that:

> *Ensures that within the enterprise, information is protected against disclosure to unauthorised users (confidentiality), improper modification (integrity) and non-access when required (availability).*

- Confidentiality means preserving authorised restrictions on access and disclosure, including means for protecting privacy and proprietary information.
- Integrity means guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.
- Availability means ensuring timely and reliable access to and use of information.

Although several other definitions of the term exist, this definition provides the very basics of information security as it covers the confidentiality, integrity and availability (CIA) concept. It is important to note that while the CIA concept is globally accepted, there are broader uses of the term 'integrity' in the wider business context. COBIT 5 covers this term in the information enabler as information goals of completeness and accuracy. *COBIT 5 for Information Security* is limited to the security view of this term and builds on this definition to describe how information security can be applied in real life, taking into account the COBIT 5 principles.

Information security is a business enabler that is strictly bound to stakeholder trust, either by addressing business risk or by creating value for an enterprise, such as competitive advantage. At a time when the significance of information and related technologies is increasing in every aspect of business and public life, the need to mitigate information risk, which includes protecting information and related IT assets from ever-changing threats, is constantly intensifying. Increasing regulation within the business landscape adds to the awareness of the board of directors of the criticality of information security for information and IT-related assets.

The preceding pages provide a preview of the information contained in *COBIT 5 for Information Security*. The publication provides guidance to help IT and Security professionals understand, utilize, implement and direct important information-security related activities and make more informed decisions.

COBIT 5 for Information Security is a major strategic evolution of COBIT 5—the only business framework for the governance and management of enterprise IT. This evolutionary version incorporates the latest thinking in enterprise governance and management techniques, and provides globally accepted principles, practices, analytical tools and models to help increase the trust in, and value from, information systems.

To purchase *COBIT 5 for Information Security*, visit www.isaca.org/cobit5info-sec

Not a member? Learn the value of ISACA membership. Additional information is available at www.isaca.org/membervalue.