

# COBIT<sup>®</sup>



*for Information Security*

PREVIEW VERSION

**COBIT**<sup>®</sup>   
AN ISACA<sup>®</sup> 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](http://www.isaca.org/cobit5info-sec)

**Not a member?** Learn the value of ISACA membership. Additional information is available at [www.isaca.org/membervalue](http://www.isaca.org/membervalue).

## ISACA<sup>®</sup>

With more than 100,000 constituents in 180 countries, ISACA ([www.isaca.org](http://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<sup>®</sup> 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<sup>®</sup> (CISA<sup>®</sup>), Certified Information Security Manager<sup>®</sup> (CISM<sup>®</sup>), Certified in the Governance of Enterprise IT<sup>®</sup> (CGEIT<sup>®</sup>) and Certified in Risk and Information Systems Control<sup>™</sup> (CRISC<sup>™</sup>) 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<sup>®</sup> 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.

## Copyright

© 2012 ISACA. All rights reserved. For usage guidelines, see [www.isaca.org/COBITuse](http://www.isaca.org/COBITuse).

## 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](mailto:info@isaca.org)  
Web site: [www.isaca.org](http://www.isaca.org)

Feedback: [www.isaca.org/cobit](http://www.isaca.org/cobit)

Participate in the ISACA Knowledge Center: [www.isaca.org/knowledge-center](http://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](http://www.facebook.com/ISACAHQ)

*COBIT<sup>®</sup> 5 for Information Security*

ISBN 978-1-60420-255-7

Printed in the United States of America

1

TABLE OF CONTENTS

<b>List of Figures</b> .....	11
<b>Executive Summary</b> .....	13
Introduction .....	13
Drivers .....	13
Benefits .....	15
Target Audience .....	16
Conventions Used and Overview .....	16
<b>Section I. Information Security</b> .....	19
<b>Chapter 1. Information Security Defined</b> .....	19
<b>Chapter 2. COBIT 5 Principles</b> .....	21
2.1 Overview .....	21
2.2 Principle 1. Meeting Stakeholder Needs .....	21
2.3 Principle 2. Covering the Enterprise End-to-end .....	22
2.4 Principle 3. Applying a Single, Integrated Framework .....	22
2.5 Principle 4. Enabling a Holistic Approach .....	23
2.6 Principle 5. Separating Governance From Management .....	23
<b>Section II. Using COBIT 5 Enablers for Implementing Information Security in Practice</b> .....	25
<b>Chapter 1. Introduction</b> .....	25
1.1 The Generic Enabler Model .....	25
1.2 Enabler Performance Management .....	26
1.3 <i>COBIT 5 for Information Security</i> and Enablers .....	26
<b>Chapter 2. Enabler: Principles, Policies and Frameworks</b> .....	27
2.1 Principles, Policies and Framework Model .....	27
2.2 Information Security Principles .....	29
2.3 Information Security Policies .....	29
2.4 Adapting Policies to the Enterprise’s Environment .....	30
2.5 Policy Life Cycle .....	31
<b>Chapter 3. Enabler: Processes</b> .....	33
3.1 The Process Model .....	33
3.2 Governance and Management Processes .....	34
3.3 Information Security Governance and Management Processes .....	34
3.4 Linking Processes to Other Enablers .....	35
<b>Chapter 4. Enabler: Organisational Structures</b> .....	37
4.1 Organisational Structures Model .....	37
4.2 Information Security Roles and Structures .....	38
4.3 Accountability Over Information Security .....	39
<b>Chapter 5. Enabler: Culture, Ethics and Behaviour</b> .....	41
5.1 Culture Model .....	41
5.2 Culture Life Cycle .....	42
5.3 Leadership and Champions .....	42
5.4 Desirable Behaviour .....	43
<b>Chapter 6. Enabler: Information</b> .....	45
6.1 Information Model .....	45
6.2 Information Types .....	46
6.3 Information Stakeholders .....	46
6.4 Information Life Cycle .....	47
<b>Chapter 7. Enabler: Services, Infrastructure and Applications</b> .....	49
7.1 Services, Infrastructure and Applications Model .....	49
7.2 Information Security Services, Infrastructure and Applications .....	50
<b>Chapter 8. Enabler: People, Skills and Competencies</b> .....	51
8.1 People, Skills and Competencies Model .....	51
8.2 Information Security-related Skills and Competencies .....	52

<b>Section III. Adapting <i>COBIT 5 for Information Security</i> to the Enterprise Environment</b> .....	53
<b>Chapter 1. Introduction</b> .....	53
<b>Chapter 2. Implementing Information Security Initiatives</b> .....	55
2.1. Considering the Enterprise’s Information Security Context.....	55
2.2. Creating the Appropriate Environment.....	55
2.3. Recognising Pain Points and Trigger Events.....	56
2.4. Enabling Change.....	56
2.5. A Life Cycle Approach.....	57
<b>Chapter 3. Using <i>COBIT 5 for Information Security</i> to Connect Other Frameworks, Models, Good Practices and Standards</b> .....	59
<b>Appendices</b>	
<b>Appendix A. Detailed Guidance: Principles, Policies and Frameworks Enabler</b> .....	61
A.1 Information Security Principles.....	61
A.2 Information Security Policy.....	63
A.3 Specific Information Security Policies Driven by the Information Security Function.....	63
A.4 Specific Information Security Policies Driven by Other Functions Within the Enterprise.....	65
<b>Appendix B. Detailed Guidance: Processes Enabler</b> .....	67
B.1 Evaluate, Direct and Monitor (EDM).....	69
B.2 Align, Plan and Organise (APO).....	81
B.3 Build, Acquire and Implement (BAI).....	115
B.4 Deliver, Service and Support (DSS).....	141
B.5 Monitor, Evaluate and Assess (MEA).....	159
<b>Appendix C. Detailed Guidance: Organisational Structures Enabler</b> .....	169
C.1 Chief Information Security Officer.....	169
C.2 Information Security Steering Committee.....	171
C.3 Information Security Manager.....	172
C.4 Enterprise Risk Management Committee.....	174
C.5 Information Custodians/Business Owners.....	174
<b>Appendix D. Detailed Guidance: Culture, Ethics and Behaviour Enabler</b> .....	175
D.1 Behaviours.....	175
D.2 Leadership.....	176
<b>Appendix E. Detailed Guidance: Information Enabler</b> .....	179
E.1 Information Security Stakeholders Template.....	179
E.2 Information Security Strategy.....	181
E.3 Information Security Budget.....	182
E.4 Information Security Plan.....	183
E.5 Policies.....	184
E.6 Information Security Requirements.....	184
E.7 Awareness Material.....	184
E.8 Information Security Review Reports.....	185
E.9 Information Security Dashboard.....	186
<b>Appendix F. Detailed Guidance: Services, Infrastructure and Applications Enabler</b> .....	189
F.1 Security Architecture.....	189
F.2 Security Awareness.....	191
F.3 Secure Development.....	192
F.4 Security Assessments.....	192
F.5 Adequately Secured and Configured Systems, Aligned With Security Requirements and Security Architecture.....	193
F.6 User Access and Access Rights in Line With Business Requirements.....	194
F.7 Adequate Protection Against Malware, External Attacks and Intrusion Attempts.....	196
F.8 Adequate Incident Response.....	197
F.9 Security Testing.....	198
F.10 Monitoring and Alert Services for Security-related Events.....	199

**Appendix G. Detailed Guidance: People, Skills and Competencies Enabler** ..... 201

    G.1 Information Security Governance ..... 201

    G.2 Information Security Strategy Formulation ..... 202

    G.3 Information Risk Management..... 203

    G.4 Information Security Architecture Development ..... 203

    G.5 Information Security Operations ..... 204

    G.6 Information Assessment and Testing and Compliance ..... 205

**Appendix H. Detailed Mappings**..... 207

**Acronyms** ..... 215

**Glossary** ..... 217

## LIST OF FIGURES

<b>Figure 1</b> —COBIT 5 Product Family.....	13
<b>Figure 2</b> —COBIT 5 as it Relates to Information Security.....	14
<b>Figure 3</b> —COBIT 5 for Information Security Capabilities .....	16
<b>Figure 4</b> —COBIT 5 Principles .....	21
<b>Figure 5</b> —COBIT 5 Goals Cascade Overview .....	22
<b>Figure 6</b> —COBIT 5 Enabler: Systemic Model With Interacting Enablers.....	23
<b>Figure 7</b> —COBIT 5 Process Reference Model.....	24
<b>Figure 8</b> —COBIT 5 Enablers: Generic .....	25
<b>Figure 9</b> —COBIT 5 Enabler: Principles, Policies and Frameworks.....	27
<b>Figure 10</b> —Policy Framework .....	28
<b>Figure 11</b> —COBIT 5 Enabler: Processes .....	33
<b>Figure 12</b> —COBIT 5 Enabler: Organisational Structures .....	37
<b>Figure 13</b> —Information Security-specific Roles/Structures.....	38
<b>Figure 14</b> —Advantages and Disadvantages of Potential Paths for Information Security Reporting.....	39
<b>Figure 15</b> —COBIT 5 Enabler: Culture, Ethics and Behaviour.....	41
<b>Figure 16</b> —COBIT 5 Enabler: Information .....	45
<b>Figure 17</b> —Example Stakeholders for Information Security-related Information (Small/Medium Enterprise).....	47
<b>Figure 18</b> —COBIT 5 Enabler: Services, Infrastructure and Applications .....	49
<b>Figure 19</b> —COBIT 5 Enabler: People, Skills and Competencies.....	51
<b>Figure 20</b> —Information Security Skills/Competencies .....	52
<b>Figure 21</b> —The Seven Phases of the Implementation Life Cycle.....	57
<b>Figure 22</b> —Information Security Principles.....	61
<b>Figure 23</b> —Specific Information Security Policies Driven by Other Functions Within the Organisation: Scope.....	65
<b>Figure 24</b> —COBIT 5 Process Reference Model.....	67
<b>Figure 25</b> —CISO: Mandate, Operating Principles, Span of Control and Authority Level.....	169
<b>Figure 26</b> —CISO: High-level RACI Chart With Key Practices .....	170
<b>Figure 27</b> —CISO: Inputs and Outputs .....	170
<b>Figure 28</b> —ISSC: Composition .....	171
<b>Figure 29</b> —ISSC: Mandate, Operating Principles, Span of Control and Authority Level.....	171
<b>Figure 30</b> —ISSC: High-level RACI Chart .....	172
<b>Figure 31</b> —ISSC: Inputs and Outputs .....	172
<b>Figure 32</b> —ISM: Mandate, Operating Principles, Span of Control and Authority Level.....	172
<b>Figure 33</b> —ISM: High-level RACI Chart.....	173
<b>Figure 34</b> —ISM: Inputs and Outputs.....	173
<b>Figure 35</b> —ERM Committee: Composition.....	174
<b>Figure 36</b> —ERM Committee: High-level RACI Chart.....	174
<b>Figure 37</b> —Information Custodians/Business Owners: High-level RACI Chart.....	174
<b>Figure 38</b> —Information Related to Stakeholders for Information Security Template .....	180
<b>Figure 39</b> —Plan Services: Description of the Service Capability .....	189
<b>Figure 40</b> —Plan Services: Attributes.....	190
<b>Figure 41</b> —Plan Services: Goals .....	190
<b>Figure 42</b> —Security Awareness Services: Description of the Service Capability.....	191
<b>Figure 43</b> —Security Awareness Services: Attributes .....	191
<b>Figure 44</b> —Security Awareness Services: Goals.....	191
<b>Figure 45</b> —Secure Development Services: Description of the Service Capability .....	192
<b>Figure 46</b> —Secure Development Services: Attributes .....	192
<b>Figure 47</b> —Secure Development Services: Goals .....	192
<b>Figure 48</b> —Security Assessment Services: Description of the Service Capability.....	192
<b>Figure 49</b> —Security Assessment Services: Attributes .....	193
<b>Figure 50</b> —Security Assessment Services: Goals.....	193
<b>Figure 51</b> —Adequately Secured Systems Services: Description of the Service Capability.....	193
<b>Figure 52</b> —Adequately Secured Systems Services: Attributes .....	194
<b>Figure 53</b> —Adequately Secured Systems Services: Goals .....	194
<b>Figure 54</b> —User Access and Access Rights Services: Description of the Service Capability .....	194
<b>Figure 55</b> —User Access and Access Rights Services: Attributes.....	195
<b>Figure 56</b> —User Access and Access Rights Services: Goals.....	196
<b>Figure 57</b> —Protection Against Malware and Attacks Services: Description of the Service Capability.....	196

**Figure 58**—Protection Against Malware and Attacks Services: Attributes ..... 197

**Figure 59**—Protection Against Malware and Attacks Services: Goals ..... 197

**Figure 60**—Incident Response Services: Description of the Service Capability ..... 197

**Figure 61**—Incident Response Services: Attributes ..... 198

**Figure 62**—Incident Response Services: Goals ..... 198

**Figure 63**—Security Testing Services: Description of the Service Capability ..... 198

**Figure 64**—Security Testing Services: Attributes ..... 198

**Figure 65**—Security Testing Services: Goals ..... 199

**Figure 66**—Information Security Monitoring/Improvement Services: Description of the Service Capability ..... 199

**Figure 67**—Information Security Monitoring/Improvement Services: Attributes ..... 199

**Figure 68**—Information Security Monitoring/Improvement Services: Goals ..... 200

**Figure 69**—Information Security Governance: Experience, Education and Qualifications ..... 201

**Figure 70**—Information Security Governance: Knowledge, Technical Skills and Behavioural Skills ..... 201

**Figure 71**—Information Security Strategy Formulation: Experience, Education and Qualifications ..... 202

**Figure 72**—Information Security Strategy Formulation: Knowledge, Technical Skills and Behavioural Skills ..... 202

**Figure 73**—Information Security Strategy Formulation: Related Role/Structure ..... 202

**Figure 74**—Information Risk Management: Experience, Education and Qualifications ..... 203

**Figure 75**—Information Risk Management: Knowledge, Technical Skills and Behavioural Skills ..... 203

**Figure 76**—Information Security Architecture Development: Experience, Education and Qualifications ..... 203

**Figure 77**—Information Security Architecture Development: Knowledge, Technical Skills and Behavioural Skills ..... 204

**Figure 78**—Information Security Architecture Development: Related Role/Structure ..... 204

**Figure 79**—Information Security Operations: Experience, Education and Qualifications ..... 204

**Figure 80**—Information Security Operations: Knowledge, Technical Skills and Behavioural Skills ..... 205

**Figure 81**—Information Security Operations: Related Role/Structure ..... 205

**Figure 82**—Information Security Auditing and Compliance: Experience, Education and Qualifications ..... 205

**Figure 83**—Information Security Auditing and Compliance: Knowledge, Technical Skills and Behavioural Skills ..... 205

**Figure 84**—Mapping of *COBIT 5 for Information Security* to Related Standards ..... 208



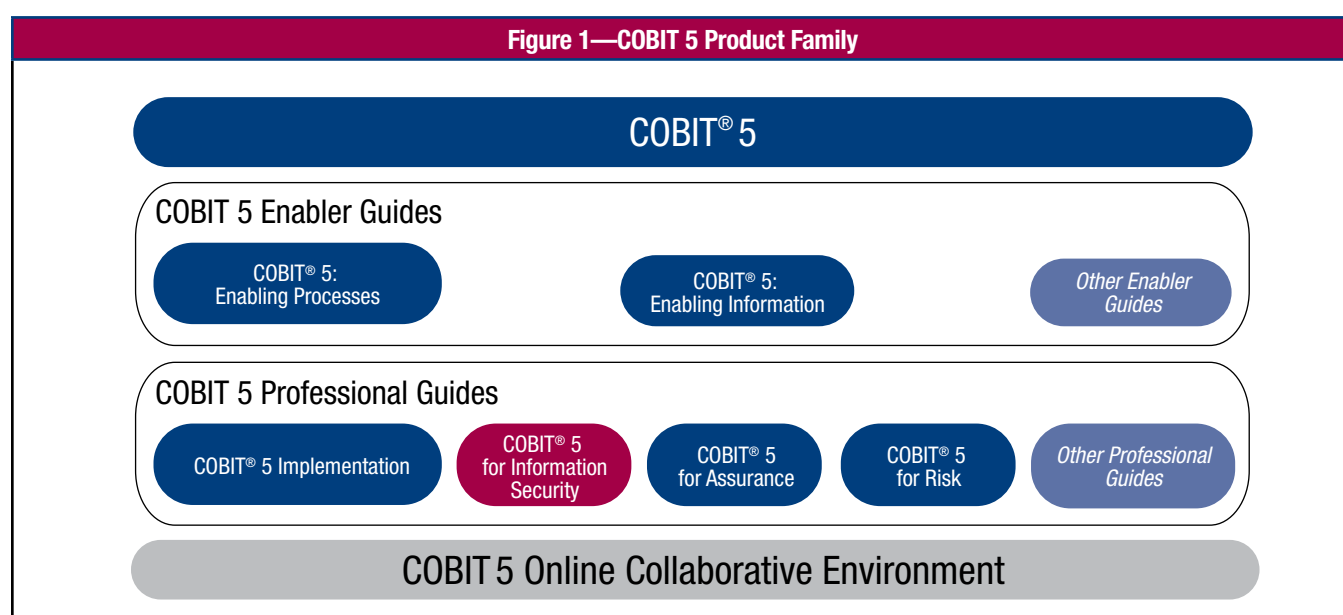
## EXECUTIVE SUMMARY

### 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**).



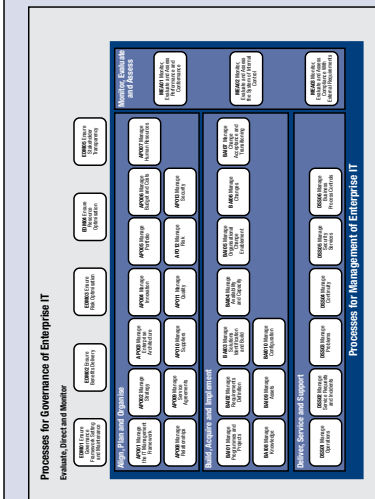
### Drivers

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**

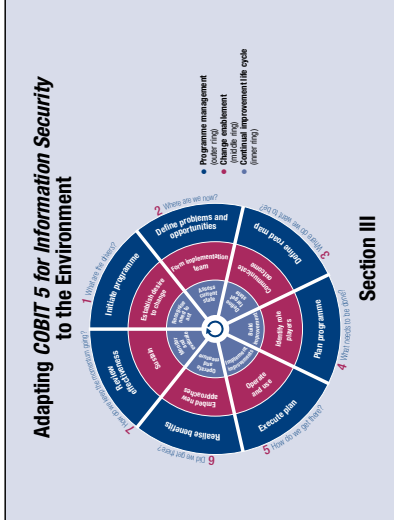
- Chief information security officer (CISO)
- Information security steering committee (ISSC)
- Information security manager (ISM)
- Other related roles and structures

Section II, Chapter 4  
Detailed Guidance: Appendix C

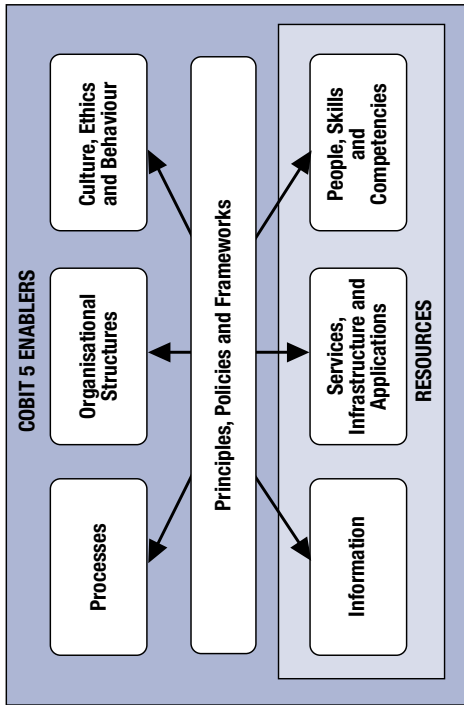
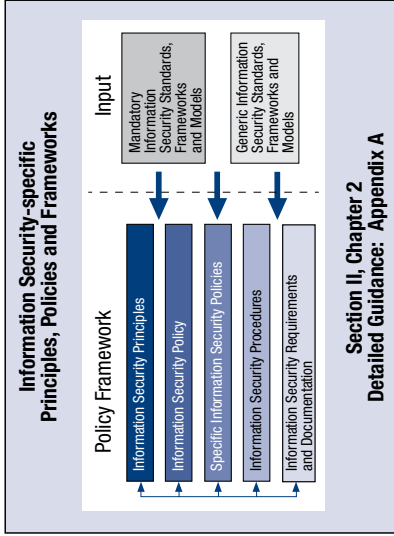
**Desired Information Security-specific Culture, Ethics and Behaviour**

- 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



Section III



**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 governance
- 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	<p>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.</p> <p>Additionally, ISACA's information security governance offerings, <i>Information Security Governance: Guidance for Information Security Managers</i> and <i>Information Security Governance: Guidance for Boards of Directors and Executive Management, 2<sup>nd</sup> Edition</i> were analysed during the development of COBIT 5 for Information Security.</p>
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](http://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](http://www.isaca.org/cobit5info-sec)

**Not a member?** Learn the value of ISACA membership. Additional information is available at [www.isaca.org/membervalue](http://www.isaca.org/membervalue).