COBIT Focus Area: Information Security

Using COBIT 2019

COBIT®
An ISACA Framework

ISACA®

About ISACA

For more than 50 years, ISACA® (*www.isaca.org*) has advanced the best talent, expertise and learning in technology. ISACA equips individuals with knowledge, credentials, education and community to progress their careers and transform their organizations, and enables enterprises to train and build quality teams. ISACA is a global professional association and learning organization that leverages the expertise of its 145,000 members who work in information security, governance, assurance, risk and privacy to drive innovation through technology. It has a presence in 188 countries, including more than 220 chapters worldwide.

Disclaimer

ISACA has designed and created *COBIT Focus Area: Information Security* (the "Work") primarily as an educational resource for enterprise governance of information and technology (EGIT), assurance, risk and 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, enterprise governance of information and technology (EGIT), assurance, risk and security professionals should apply their own professional judgment to the specific circumstances presented by the particular systems or information technology environment.

ISACA

1700 E. Golf Road, Suite 400
Schaumburg, IL 60173, USA
Phone: +1.847.660.5505
Fax: +1.847.253.1755
Contact us: https://support.isaca.org
Website: www.isaca.org

Participate in the ISACA Online Forums: https://engage.isaca.org/onlineforums

Twitter: http://twitter.com/ISACANews
LinkedIn: www.linkedin.com/company/isaca
Facebook: www.facebook.com/ISACAGlobal
Instagram: www.instagram.com/isacanews/

COBIT Focus Area: Information Security
ISBN 978-1-60420-829-0

Acknowledgments

ISACA wishes to recognize:

Development Team
Mattias Goorden, PwC, Belgium
Stefanie Grijp, PwC, Belgium
J. Winston Hayden, CISA, CRISC, CISM, CGEIT, South Africa
Dirk Steuperaert, CISA, CRISC, CGEIT, IT In Balance, Belgium
Jo Stewart-Rattray, CISA, CRISC, CISM, CGEIT, FACS CP, BRM Advisory, Australia

Expert Reviewers
Allan Boardman, CISA, CRISC, CISM, CGEIT, CISSP, CyberAdvisor.London, United Kingdom
Graciela Braga, CGEIT, Auditor and Advisor, Argentina
Leela Ravi Shankar Dhulipalla, CGEIT, CDPSE, COBIT Certified Assessor, TOGAF, PMP, NCSP Practitioner, IAITAM - CHAMP, CSAM, CITAM, First Abu Dhabi Bank, UAE
John E. Jasinski, CISA, CRISC, CISM, CGEIT, CSX, COBIT 5 Assessor, COBIT and ITIL Accredited Instructor, AWS Practitioner, CCSK, Certified Scrum Master and Product Owner, ISO 20000, IT4IT, ITIL Expert, Lean IT, MOF, ServiceNow and RSA Archer Certified System Administrator, Six Sigma Blackbelt, TOGAF, USA
Larry Marks, CISA, CRISC, CISM, CGEIT, CDPSE, CISSP, ITIL, PMP, BDO USA
Okanlawon Zachy Olorunojowon, CISA, CGEIT, PMP, BC Ministry of Health, Canada
Matthew A. Shabat, JD, CISM, CRISC, Native American Industrial Solutions LLC, USA
Caren Shiozaki, CGEIT, Thornburg Mortgage, USA
Bruno Horta Soares, CISA, CRISC, CGEIT, PMP, GOVaaS—Governance Advisors-as-a-Service, Portugal
Ilker Tutu, CISA, CRISC, CISM, CGEIT, CCSP, CIA, CISSP, ISO 27001, ITIL, PCI ISA, PayPal Europe, Luxembourg
Kevin Wegryn, PfMP, PMP, Security+, Wells Fargo, USA
Greg Witte, CISM, USA
Ning Ye, CISA, CIA, China Construction Bank, China

Board of Directors
Tracey Dedrick, Chair, Former Chief Risk Officer, Hudson City Bancorp, USA
Rolf von Roessing, Vice-Chair, CISA, CISM, CGEIT, CDPSE, CISSP, FBCI, Partner, FORFA Consulting AG, Switzerland
Gabriela Hernandez-Cardoso, Independent Board Member, Mexico
Pam Nigro, CISA, CRISC, CGEIT, CRMA, Vice President–Information Technology, Security Officer, Home Access Health, USA
Maureen O'Connell, Board Chair, Acacia Research (NASDAQ), Former Chief Financial Officer and Chief Administration Officer, Scholastic, Inc., USA
David Samuelson, Chief Executive Officer, ISACA, USA
Gerrard Schmid, President and Chief Executive Officer, Diebold Nixdorf, USA
Gregory Touhill, CISM, CISSP, President, AppGate Federal Group, USA
Asaf Weisberg, CISA, CRISC, CISM, CGEIT, Chief Executive Officer, introSight Ltd., Israel
Anna Yip, Chief Executive Officer, SmarTone Telecommunications Limited, Hong Kong
Brennan P. Baybeck, CISA, CRISC, CISM, CISSP, ISACA Board Chair, 2019-2020, Vice President and Chief Information Security Officer for Customer Services, Oracle Corporation, USA
Rob Clyde, CISM, ISACA Board Chair, 2018-2019, Independent Director, Titus, and Executive Chair, White Cloud Security, USA
Chris K. Dimitriadis, Ph.D., CISA, CRISC, CISM, ISACA Board Chair, 2015-2017, Group Chief Executive Officer, INTRALOT, Greece

Page intentionally left blank

TABLE OF CONTENTS

Page intentionally left blank

LIST OF FIGURES

Chapter 1. Introduction

Chapter 2. Structure of This Publication and Intended Audience

Chapter 3. Structure of COBIT Governance and Management Objectives

Page intentionally left blank

Chapter 1
Introduction

1.1 COBIT as an Information and Technology (I&T) Governance Framework

Over the years, best practice frameworks have been developed and promoted to assist in the process of understanding, designing and implementing enterprise governance of IT (EGIT). COBIT® 2019 builds on and integrates more than 25 years of development in this field, not only incorporating new insights from science but also operationalizing these insights as practice.

From its foundation in the IT audit community, COBIT® has developed into a broader and more comprehensive information and technology (I&T) governance and management framework and continues to establish itself as a generally accepted framework for I&T governance.

What Is COBIT and What Is It Not?

Before describing the COBIT framework, it is important to explain what COBIT is and is not.

COBIT is a framework for the governance and management of information and technology, aimed at the whole enterprise. Enterprise I&T includes all the technology and information processing the enterprise puts in place to achieve its goals, regardless of where this happens in the enterprise. In other words, enterprise I&T is not limited to the IT department of an organization but certainly includes it.

Enterprise I&T includes all the technology and information processing the enterprise puts in place to achieve its goals, regardless of where this happens in the enterprise.

The COBIT framework makes a clear distinction between governance and management. These two disciplines encompass different activities, require different organizational structures and serve different purposes.

- **Governance** ensures that:
  - Stakeholder needs, conditions and options are evaluated to determine balanced, agreed-on enterprise objectives.
  - Direction is set through prioritization and decision making.
  - Performance and compliance are monitored against agreed-on direction and objectives.

  In most enterprises, governance is the responsibility of the board of directors, under the leadership of the chairperson. Specific governance responsibilities may be delegated to special organizational structures at an appropriate level, particularly in larger, complex enterprises.
- **Management** plans, builds, runs and monitors activities, in alignment with the direction set by the governance body, to achieve enterprise objectives.

  In most enterprises, management is the responsibility of the executive management under the leadership of the chief executive officer (CEO).

COBIT defines the components to build and sustain a governance system: processes, organizational structures, policies and procedures, information flows, culture and behaviors, skills, and infrastructure.

COBIT defines the design factors that should be considered by the enterprise to build a best-fit governance system.

COBIT addresses governance issues by grouping relevant governance components into governance and management objectives that can be managed to the required capability levels.

Several misconceptions about COBIT should be dispelled:

- COBIT is not a full description of the whole IT environment of an enterprise.
- COBIT is not a framework to organize business processes.
- COBIT is not an (IT-)technical framework to manage all technology.
- COBIT does not make or prescribe any IT-related decisions. It will not decide what the best IT strategy is, what the best architecture is, or how much IT can or should cost. Rather, COBIT defines all the components that describe which decisions should be taken, and how and by whom they should be taken.

1.2 COBIT Overview

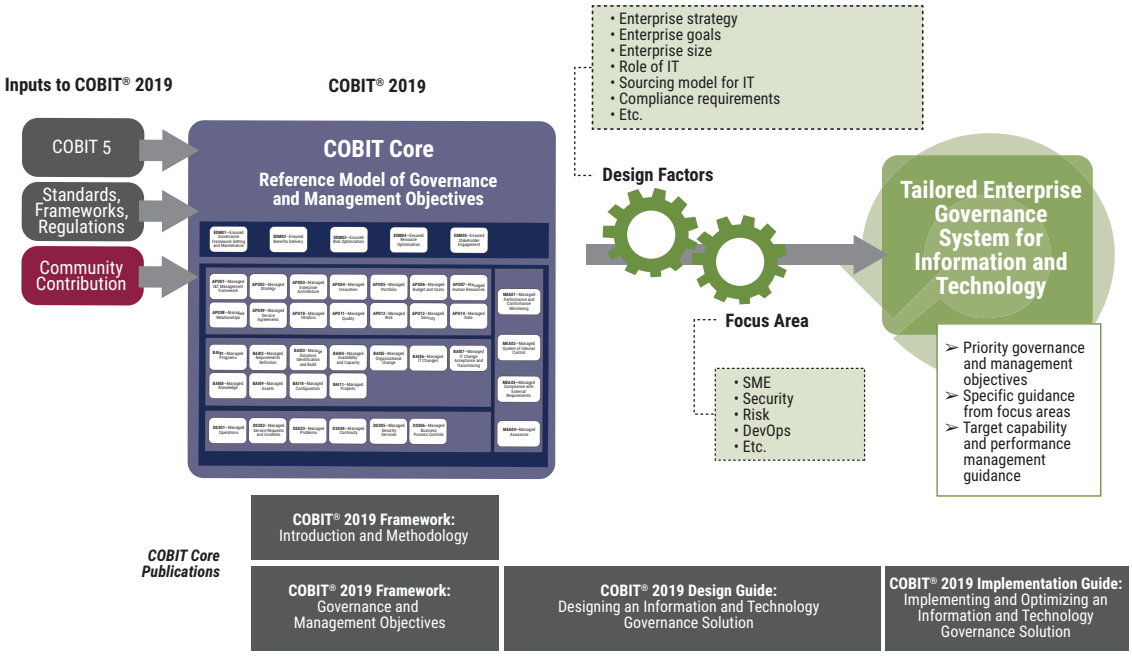
The COBIT 2019 product family is open-ended and designed for customization. The following publications are currently available:

- ***COBIT 2019 Framework: Introduction and Methodology***[1] introduces the key concepts of COBIT 2019.
- ***COBIT 2019 Framework: Governance and Management Objectives***[2] comprehensively describes the 40 core governance and management objectives, the processes contained therein, and other related components. This guide also references other standards and frameworks.
- ***COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution***[3] explores design factors that can influence governance and includes a workflow for planning a tailored governance system for the enterprise.
- ***COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution***[4] represents an evolution of the *COBIT 5 Implementation* guide and develops a road map for continuous governance improvement. It may be used in combination with the *COBIT 2019 Design Guide.*

Figure 1.1 shows the high-level overview of COBIT 2019 and illustrates how different publications within the set cover different aspects.

1 ISACA, *COBIT 2019 Framework: Introduction and Methodology*, USA, 2018, *https://www.isaca.org/bookstore/bookstore-cobit_19-print/cb19fim*
2 ISACA, *COBIT 2019 Framework: Governance and Management Objectives*, USA, 2018, *https://www.isaca.org/bookstore/bookstore-cobit_19-print/cb19fgm*
3 ISACA, *COBIT 2019 Design Guide: Designing an Information and Technology Governance Solution*, USA, 2018, *https://www.isaca.org/bookstore/bookstore-cobit_19-digital/wcb19dgd*
4 ISACA, *COBIT 2019 Implementation Guide: Implementing and Optimizing an Information and Technology Governance Solution*, USA, 2018, *https://www.isaca.org/bookstore/bookstore-cobit_19-print/cb19igio*

Figure 1.1—COBIT Overview



Source: ISACA, *COBIT 2019 Framework: Introduction and Methodology*, USA, 2018, figure 4.1, *https://www.isaca.org/bookstore/bookstore-cobit_19-print/cb19fim*

The following sections explain the key concepts and terms used in COBIT 2019.

Focus area content (see **figure 1.1)** contains more detailed guidance on specific themes. This focus area publication provides a tailored version of guidance—specific to information security—based on (and extending from) the core publication, *COBIT Framework: Governance and Management Objectives*.

1.3 Terminology and Key Concepts of the COBIT Framework

1.3.1 Governance and Management Objectives

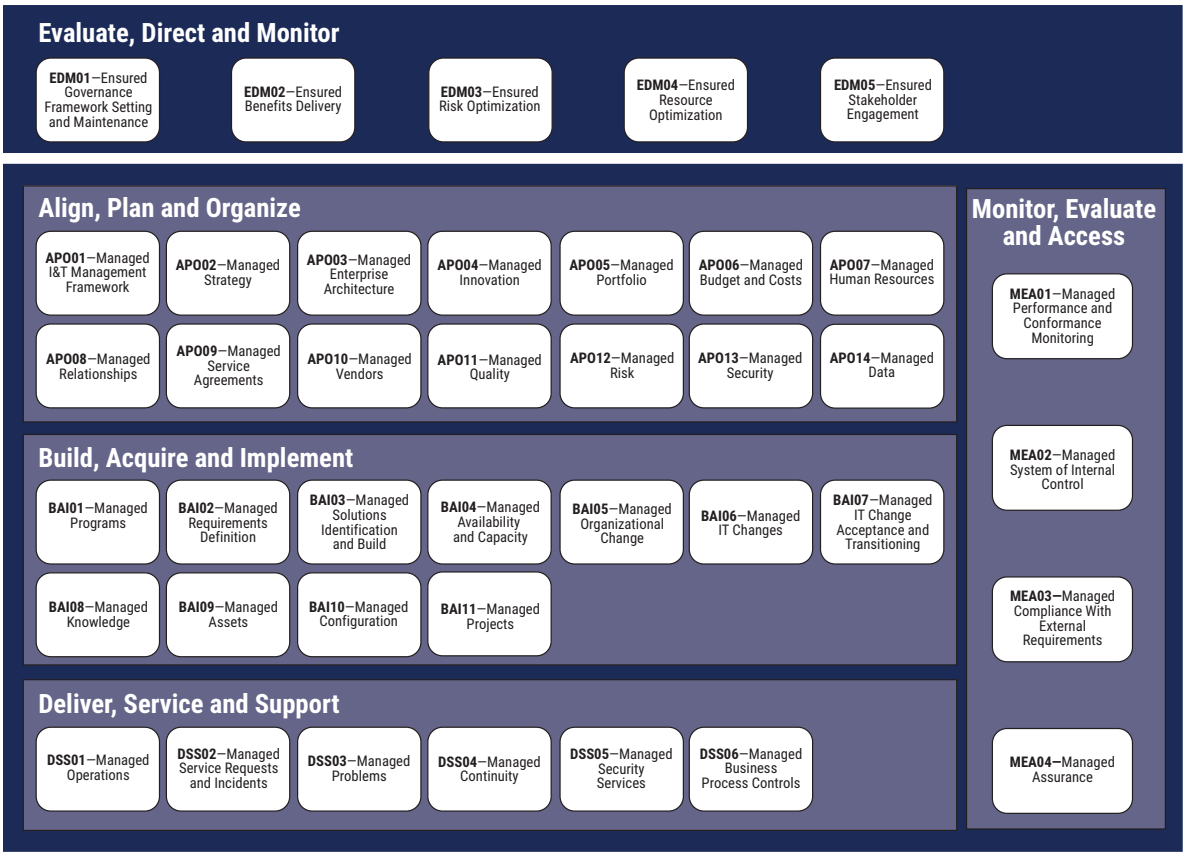
For information and technology to contribute to enterprise goals, a number of governance and management objectives should be achieved. Basic concepts relating to governance and management objectives are:

- A governance or management objective **always relates to one process** (with an identical or similar name) and a series of related components of other types to help achieve the objective.
- A governance objective relates to a governance process (depicted on the dark blue background in **figure 1.2**), while a management objective relates to management processes (depicted on the lighter blue background in **figure 1.2**). Boards and executive management are typically accountable for governance processes, while management processes are the domain of senior and middle management.

The governance and management objectives in COBIT are grouped into five domains. The domains have names with verbs that express the key purpose and areas of activity of the objectives contained in them:

- Governance objectives are grouped in the **Evaluate, Direct and Monitor** (EDM) domain. In this domain, the governing body evaluates strategic options, directs senior management on the chosen strategic options and monitors the achievement of the strategy.
- Management objectives are grouped in four domains.
  - **Align, Plan and Organize** (APO) addresses the overall organization, strategy and supporting activities for I&T.
  - **Build, Acquire and Implement** (BAI) treats the definition, acquisition and implementation of I&T solutions and their integration in business processes.
  - **Deliver, Service and Support** (DSS) addresses the operational delivery and support of I&T services, including security.
  - **Monitor, Evaluate and Assess** (MEA) addresses performance monitoring and conformance of I&T with internal performance targets, internal control objectives and external requirements.

Figure 1.2—COBIT Core Model



Source: ISACA, *COBIT 2019 Framework: Introduction and Methodology*, USA, 2018, figure 4.2

1.3.2 Components of the Governance System

To satisfy governance and management objectives, each enterprise needs to establish, tailor and sustain a governance system built from a number of components:

- Components are factors that, individually and collectively, contribute to the good operations of the enterprise's governance system over I&T.
- Components interact with each other, resulting in a holistic governance system for I&T.
- Components can be of different types. The most familiar are processes. However, components of a governance system also include organizational structures; policies and procedures; information items; culture and behavior; skills and competencies; and services, infrastructure and applications (**figure 1.3**).
  - **Processes** describe an organized set of practices and activities to achieve certain objectives and produce a set of outputs that support achievement of overall IT-related goals.
  - **Organizational structures** are the key decision-making entities in an enterprise.
  - **Principles, policies and frameworks** translate desired behavior into practical guidance for day-to-day management.
  - **Information** is pervasive throughout any organization and includes all information produced and used by the enterprise. COBIT focuses on the information required for the effective functioning of the governance system of the enterprise.
  - **Culture, ethics and behavior** of individuals and of the enterprise are often underestimated as factors in the success of governance and management activities.
  - **People, skills and competencies** are required for good decisions, execution of corrective action and successful completion of all activities.
  - **Services, infrastructure and applications** include the infrastructure, technology and applications that provide the enterprise with the governance system for I&T processing.

Figure 1.3—COBIT Components of a Governance System

Source: ISACA, *COBIT 2019 Framework: Introduction and Methodology*, USA, 2018, figure 4.3

Components of all types can be generic or can be variants of generic components:

- **Generic** components are described in the COBIT core model (**figure 1.2**) and apply in principle to any situation. However, they are generic in nature and generally need customization before being practically implemented.
- **Variants** are based on generic components but are tailored for a specific purpose or context within a focus area (e.g., for information security, DevOps, a particular regulation).

1.3.3 Focus Areas

A **focus area** describes a certain governance topic, domain or issue that can be addressed by a collection of governance and management objectives and their components. Examples of potential focus areas include small and medium enterprises, information security, risk, digital transformation, cloud computing, privacy, and DevOps.[5] Focus areas may contain a combination of generic governance components and variants.

This publication describes the topic of information security and details additional metrics and activities that should be considered when implementing or assessing COBIT in the context of information security.

The number of focus areas is virtually unlimited. That is what makes COBIT open-ended. New focus areas can be added as required or as subject matter experts and practitioners contribute to the open-ended COBIT model.

1.4 Information Security Focus Area Overview

This publication provides specific guidance related to the information security focus area (ISFA). It is based on the COBIT core guidance for governance and management objectives, and has been tailored to address information security practices which include cybersecurity practices.

The terms information security and cybersecurity are often used interchangeably; however, cybersecurity is a subset of information security. Information security deals with information, regardless of its format—it encompasses paper documents, digital and intellectual property in people's minds, and verbal or visual communications. Cybersecurity is concerned with protecting digital assets—all resources encompassed within network hardware, software and electronic information that is processed, stored within isolated systems or transported by internetworked information environments. Unlike information security, cybersecurity does not concern natural hazards, personal mistakes or physical security.

Information security deals with information, regardless of its format—it encompasses paper documents, digital and intellectual property, and verbal or visual communications.

According to the ISACA® glossary, information security:

> *[e]nsures that within the enterprise, information is protected against disclosure to unauthorized users (confidentiality), improper modification (integrity) and nonaccess when required (availability).*
>
> - *Confidentiality means preserving authorized 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 nonrepudiation and authenticity.*
> - *Availability means ensuring timely and reliable access to and use of information.*

[5] DevOps exemplifies both a component variant and a focus area. DevOps is a current theme in the marketplace and definitely requires specific guidance, making it a focus area. DevOps includes a number of generic governance and management objectives of the core COBIT model, along with a number of variants of development-, operational- and monitoring-related processes and organizational structures.

Although several other definitions of this term exist, ISACA's definition provides the very basics of information security in the concepts of confidentiality, integrity and availability (CIA). 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 uses the terms to connote completeness and accuracy of information.

Information security is a business enabler that correlates directly 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—and protect I&T assets from ever-changing threats—is constantly intensifying. Increasing regulation and dependence on technology raise the profile of information security across the enterprise, even awareness by the board of directors, of the criticality of information security for all I&T assets.

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—and protect I&T assets from ever-changing threats—is constantly intensifying.

1.4.1 Drivers

The purpose of this publication is to provide guidance for governing and managing information security. It provides stakeholders with the information they need to understand the context of information security within the enterprise.

The major drivers for the development of this publication include:

- The need to describe information security in an enterprise context, including:
  - The full end-to-end business and I&T functional responsibilities for information security
  - Key aspects that lead to effective governance and management of information security, such as organizational structures, policies and culture
  - The relationship and alignment of information security with enterprise objectives
- An ever-increasing need for the enterprise to:
  - Achieve and maintain information risk at an acceptable level; protect information from unauthorized disclosure, unauthorized or inadvertent modification, and possible intrusion; and protect technology assets from damage and destruction
  - Ensure that services and systems are continuously available to internal and external resources for whom it is appropriate to have access leading to user satisfaction with I&T engagement and services
  - Ensure cybercrime resilience within the enterprise
  - Comply with relevant laws and regulations, contractual requirements and internal policies on information and systems security and protection, and provide transparency regarding compliance
  - Achieve all of the above while containing the cost of I&T services and technology protection
- The need to connect to and, where relevant, align with other major frameworks and standards in the marketplace
- The need to link all major ISACA research, frameworks and guidance, with a primary focus on the Business Model for Information Security (BMIS)[6] and COBIT, but also other relevant focus areas, the IT Assurance Framework (ITAF),[7] etc.

[6] ISACA, *The Business Model for Information Security,* USA, 2010, *https://www.isaca.org/bookstore/it-governance-and-business-management/wbmis1*
[7] ISACA, *ITAF: A Professional Practices Framework for IS Audit/Assurance*, 3rd Edition, USA, 2014, *https://www.isaca.org/bookstore/audit-control-and-security-essentials/witaf*

COBIT Focus Area: Information Security addresses the basic 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 damages or operational deficiencies. Breaches can expose the enterprise to external impacts such as reputational, legal and regulatory risk, and jeopardize customer and employee relations—or even the survival of the enterprise itself.

A broad range of factors and scenarios illustrates the imperative for stronger, more systematic approaches to information security:

- National critical infrastructure depends on information systems, and successful intrusions can result in a significant impact to economies and human safety.
- Nonpublic financial information can be used for economic gain.
- Disclosure of confidential information can embarrass the enterprise, damage reputations or jeopardize business relations.
- Intrusions 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 expose trade secrets and increase competition for manufacturing enterprises.
- Leaks of national or military intelligence can damage political relationships.
- Personal data leaks can lead to individual financial losses, unnecessary efforts to rebuild an individual's financial reputation, and even physical harm.
- Failure to comply with laws and regulatory requirements can result in fines or penalties, and/or loss of operating licenses.
- Significant unplanned costs (both financial and operational) related to containing, investigating and remediating security breaches can impact any enterprise that has suffered a breach.

1.4.2 Benefits

COBIT Focus Area: Information Security offers a number of information security-related tenets, whose benefits include:

- Reduction of complexity and increased cost-effectiveness through improved and easier integration and alignment of information security standards, good practices and/or sector-specific guidelines
- Higher stakeholder satisfaction with information security outcomes
- Better integration of information security across the enterprise
- Better informed risk decisions and risk awareness
- Improvements in prevention, detection and recovery
- Reduction—in terms of both impact and probability—of information security incidents
- Better support for innovation and competitiveness
- Better management and optimization of costs related to information security
- Better understanding of information security by stakeholders

Figure 1.4 explores benefits associated with the key tenets of *COBIT Focus Area: Information Security*.

Figure 1.4—*COBIT Focus Area: Information Security* Tenets	
Tenet	**Description**
Contemporary view on governance	*COBIT Focus Area: Information Security* provides a contemporary view on information security governance and management through alignment with the COBIT core framework, International Organization for Standardization (ISO®)/International Electrotechnical Commission (IEC) 38500 and other IT governance initiatives. *COBIT Focus Area: Information Security* aligns with other major frameworks, standards and models in the marketplace, including ISO/IEC 27000 series, Capability Maturity Model Integration (CMMI®), the Information Security Forum® (ISF) *Standard of Good Practice for Information Security*, and others.
Clear distinction between governance and management	COBIT clarifies the roles of governance and management and provides a clear distinction between them, with a revised model reflecting this distinction and showing how they relate to each other.
End-to-end view	*COBIT Focus Area: Information Security* posits a model that integrates 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 beginning to end.
Holistic guidance	*COBIT Focus Area: Information Security* provides comprehensive and holistic guidance on information security. Holistic means that attention is paid to components (i.e., processes and information) where information security-specific guidance is warranted. Practitioners are directed to COBIT core model guidance where additional component customization is not required.

Page intentionally left blank

Chapter 2
Structure of This Publication and Intended Audience

2.1 Structure of This Publication

This publication provides a comprehensive description of the 40 governance and management objectives relevant to information security, as defined in the COBIT core model (**figure 1.2**).

The balance of this publication includes the following sections and appendices:

- Chapter 3 explains the structure that is used to detail the guidance for all 40 governance and management objectives, across all applicable components.
- Chapter 4 provides comprehensive, detailed information security-specific guidance for all 40 governance and management objectives, focusing on two key components: processes (core-model Component A) and information flows and items (core-model Component C).

2.2 Intended Audience

The target audience for this publication includes all stakeholders of information security who seek detailed guidance on COBIT governance and management objectives (**figure 2.1**). Chief information officers (CIOs), chief information security officers (CISOs), information security managers (ISMs) and other information security professionals are the most obvious target audiences. However, information security is the responsibility of all stakeholders in the enterprise, including all staff members and third parties. Therefore, this publication can benefit all stakeholders in the enterprise.

Figure 2.1—*COBIT Focus Area: Information Security* Stakeholders and Benefits

Stakeholder	Benefits of *COBIT Focus Area: Information Security*
Boards	Use this publication as a reference to ensure security risk is mitigated to risk appetite
CISO	Reference this publication for comprehensive guidance to help establish and maintain an information security management strategy and governance system
CIO	Reference this publication to address all technical and organizational measures regarding security within the organization
Other executive management	Use guidance in this publication to implement information security governance best practices
Information security managers and security practitioners	Mine this publication for detailed knowledge to help manage and maintain an information security management system (ISMS) and carry out security governance strategy
Business managers	Reference this publication to understand when and how security should be implemented in developing and building new applications/products

A certain level of experience and understanding of the enterprise and security is required to benefit from this guide, and to enable practitioners to customize COBIT—which is open and flexible in nature—into tailored, focused and contextually sensitive guidance for the enterprise.

Page intentionally left blank

Chapter 3
Structure of COBIT Governance and Management Objectives

3.1 Introduction

This chapter describes the generic structure used to detail each of the COBIT governance and management objectives. For each governance and management objective, chapter 4 of this publication provides information related to the following two governance components applicable to that governance or management objective:

- Processes (section 3.3)
- Information flows and items (section 3.5)

The structure for this information is detailed in sections 3.2, 3.3 and 3.5. For each governance and management objective, chapter 4 elaborates additional detail specific to the information security focus area for the process and information flows and items components (Components A and C, respectively).

Additional information for the other five components is detailed in this chapter. These components include:

- Organizational structures (section 3.4)
- People, skills and competencies (section 3.6)
- Principles, policies and procedures (section 3.7)
- Culture, ethics and behavior (section 3.8)
- Services, infrastructure and applications (section 3.9)

3.2 Governance and Management Objectives

COBIT 2019 includes 40 governance and management objectives, organized into five domains (**figure 1.2**).

- There is one **governance** domain:
  - Evaluate, Direct and Monitor (EDM)
- There are four **management** domains:
  - Align, Plan and Organize (APO)
  - Build, Acquire and Implement (BAI)
  - Deliver, Service and Support (DSS)
  - Monitor, Evaluate and Assess (MEA)

The high-level information detailed for each objective (**figure 3.1**) includes:

- Domain name
- Focus area (in this publication, information security)
- Governance or management objective name
- Description
- Purpose statement
- Focus area relevance statement

Focus area relevance statements describe how COBIT objectives relate to information security.

Figure 3.1—Display of Governance and Management Objectives	
Domain: <NAME> Governance/Management Objective: <NAME>	**Focus Area: Information Security**
Description	
<TEXT>	
Purpose	
<TEXT>	
Information Security Focus Area Relevance	
<TEXT>	

In *COBIT 2019 Framework: Governance and Management Objectives*, the management objectives APO13 *Managed security* and DSS05 *Managed security services* already describe how to define, operate and monitor a system for security management in general.

Because information security concerns the entire enterprise, however, it necessarily relates to every governance and management objective performed. For the other 38 objectives, therefore, specific attention is given to information security-related metrics and activities. Metrics and activities outlined in chapter 4 should be consulted (in addition to COBIT 2019 core-model guidance) when practitioners apply COBIT in an information security-related context.

3.3 Component: Process

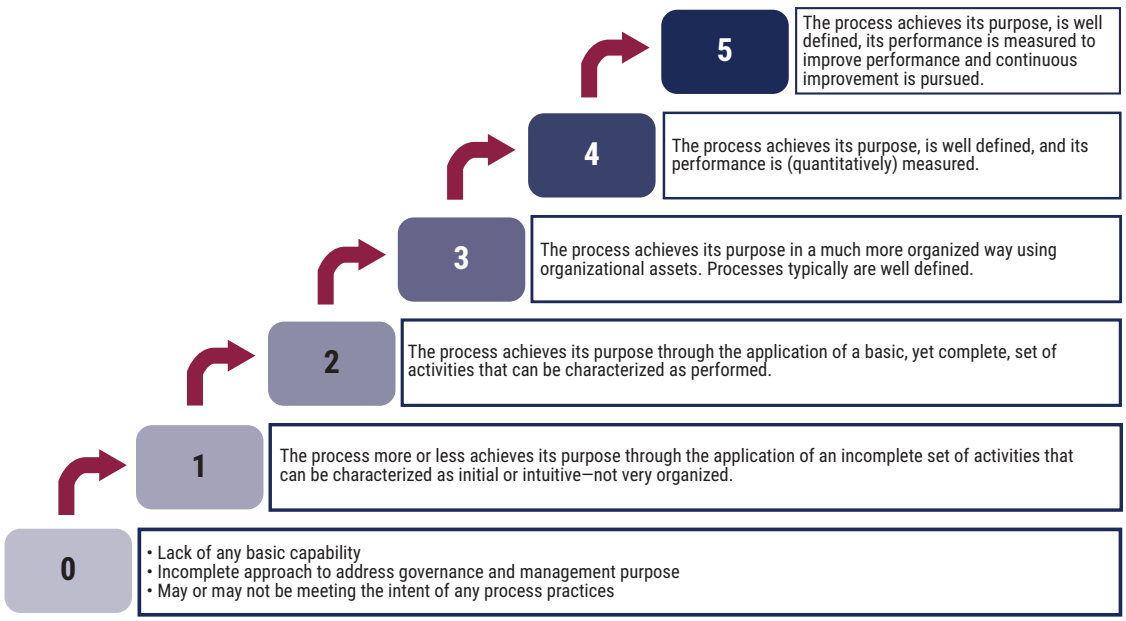
Each governance and management objective includes a process component with several governance or management process practices (**figure 3.2**). Each practice has one or more activities. A number of example metrics accompanies each process practice, to measure the achievement of the process practice and its contribution to the achievement of the overall objective. Metrics in this publication relate specifically to information security, and they should be considered in addition to the core model metrics in *COBIT 2019 Framework: Governance and Management Objectives.*

Security-specific activities are included in each practice. Several activities specific to information security supplement management objectives APO13 *Managed security* and DSS05 *Managed security services*. Users should also consult the core model, which provides basic guidance to define, operate and monitor a system for general security management.

Figure 3.2—Display of Process Component		
A. Component: Process		
Governance/Management Practice	**Example Information Security-specific Metrics**	
<REF> <NAME> <DESCRIPTION>	<METRIC>	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. <TEXT>		<NR>
2. <TEXT>		<NR>
n. <TEXT>		<NR>
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
<STANDARD NAME>	<TEXT>	

A capability level is assigned to all process activities, enabling clear definition of processes at different capability levels. A process reaches a certain capability level when all activities at that capability level are performed successfully. COBIT supports a CMMI-based process-capability scheme, ranging from 0 to 5. The capability level is a measure of how well a process is implemented and performing. **Figure 3.3** depicts the model, the increasing capability levels and the general characteristics of each.

Figure 3.3—Capability Levels for Processes



Source: ISACA, *COBIT 2019 Framework: Introduction and Methodology*, USA, 2018, figure 3.5

References to other standards and guidance are offered for relevant practices (**figure 3.2**) Related guidance refers to all standards, frameworks, compliance requirements and guidance that are relevant for the process at hand. Detailed references cite specific chapters or sections within related guidance. A complete list of sources for related guidance is included in appendix C of *COBIT 2019 Framework: Governance and Management Objectives*.

3.4 Component: Organizational Structures

3.4.1 Introduction

The organizational structures governance component is not reproduced in chapter 4 of this publication similar to its presentation in chapter 4 of the core model (*COBIT® 2019 Framework: Governance and Management Objectives*). A discussion, however, of organizational structures and their applicability to information security follows.

The following roles and organizational structures—defined in the COBIT 2019 core model—are also relevant for *COBIT Focus Area: Information Security*.

Not every organization will have (or will need) all possible roles—and not all roles are essential for the adoption of the information security focus area. Any security functions within an enterprise may include roles described in **figure 3.4**.[8]

[8] Roles and descriptions are excerpted from ISACA, *COBIT 2019 Framework: Governance and Management Objectives,* USA, 2018, Appendix B, *https://www.isaca.org/bookstore/bookstore-cobit_19-print/cb19fgm*.

Figure 3.4—COBIT Roles and Organizational Structures for Security Functions	
Role/Structure	**Description**
Board	Group of the most senior executives and/or nonexecutive directors accountable for governance and overall control of enterprise resources
Executive Committee	Group of senior executives appointed by the board to ensure that the board is involved in, and kept informed of, major decisions (The executive committee is accountable for managing the portfolios of I&T-enabled investments, I&T services and I&T assets; ensuring that value is delivered; and managing risk. The committee is normally chaired by a board member.)
Chief Executive Officer	Highest-ranking officer charged with the total management of the enterprise
Chief Operating Officer	Most senior official accountable for operation of the enterprise
Chief Risk Officer	Most senior official accountable for all aspects of risk management across the enterprise (An I&T risk officer function may be established to oversee I&T-related risk.)
Chief Information Officer	Most senior official responsible for aligning IT and business strategies and accountable for planning, resourcing and managing delivery of I&T services and solutions
Chief Information Security Officer	Most senior official accountable for all aspects of security management across the enterprise
Chief Technology Officer	Most senior official accountable for all technical aspects of I&T, including managing and monitoring decisions related to I&T services, solutions and infrastructures (This role may also be taken by the CIO.)
Chief Digital Officer	Most senior official tasked with putting into practice the digital ambition of the enterprise or business unit
I&T Governance Board	Group of stakeholders and experts accountable for guiding I&T-related matters and decisions, including managing I&T-enabled investments, delivering value and monitoring risk
Architecture Board	Group of stakeholders and experts accountable for guiding enterprise architecture-related matters and decisions and for setting architectural policies and standards
Enterprise Risk Committee	Group of executives accountable for enterprise-level collaboration and consensus required to support enterprise risk management (ERM) activities and decisions (An I&T risk council may be established to consider I&T risk in more detail and advise the enterprise risk committee.)
Portfolio Manager	Individual responsible for guiding portfolio management, ensuring selection of correct programs and projects, managing and monitoring programs and projects for optimal value, and realizing long-term strategic objectives effectively and efficiently
Steering (Programs/Projects) Committee	Group of stakeholders and experts accountable for guiding programs and projects, including managing and monitoring plans, allocating resources, delivering benefits and value, and managing program and project risk
Program Manager	Individual responsible for guiding a specific program, including articulating and following up on goals and objectives of the program and managing risk and impact on the business
Project Manager	Individual responsible for guiding a specific project, including coordinating and delegating time, budget, resources and tasks across the project team
Data Management Function	Function responsible for supporting enterprise data assets across the data life cycle and managing data strategy, infrastructure and repositories

Figure 3.4—COBIT Roles and Organizational Structures for Security Functions *(cont.)*	
Role/Structure	**Description**
Head Human Resources/ Chief People Officer	Most senior official accountable for planning and policies regarding human resources in the enterprise
Relationship Manager	Senior individual responsible for overseeing and managing the internal interface and communications between business and I&T functions
Head Architect	Senior individual accountable for the enterprise architecture process
Head Development	Senior individual accountable for I&T-related solution development processes
Head IT Operations	Senior individual accountable for IT operational environments and infrastructure
Head IT Administration	Senior individual accountable for I&T-related records and responsible for supporting I&T-related administrative matters
Service Manager	Individual who manages the development, implementation, evaluation and ongoing maintenance of new and existing products and services for a specific customer (user) or group of customers (users)
Information Security Manager	Individual who manages, designs, oversees and/or assesses an enterprise's information security
Business Continuity Manager	Individual who manages, designs, oversees and/or assesses an enterprise's business continuity capability, to ensure that the enterprise's critical functions continue to operate following disruptive events
Privacy Officer	Individual responsible for monitoring risk and business impact of privacy laws and for guiding and coordinating the implementation of policies and activities that ensure compliance with privacy directives (In some enterprises, the position may be referenced as the data protection officer.)
Legal Counsel	Function responsible for guidance on legal and regulatory matters

Using a standard RACI schema, *COBIT 2019 Framework: Governance and Management Objectives* assigns roles to one of the following two categories (or levels) of participation:

- **Responsible (R)**—Who is getting the task done? Who drives the task?

  Responsible roles take the main operational stake in fulfilling a practice and ensuring its intended outcome, often performing or executing key activities.

- **Accountable (A)**—Who accounts for the success and achievement of the task?

  Accountable roles incur overall accountability for a practice. Accountability cannot, in principle, be shared.

Practitioners may supplement the organizational structure component in *COBIT 2019 Framework: Governance and Management Objectives* by assigning the following additional levels of participation:

- **Consulted (C)**—Who provides input?

  Consulted roles contribute input for the practice.

- **Informed (I)**—Who receives information?

  Informed roles often need to understand the status or level of achievement of a practice or its associated deliverables.

COBIT provides flexible guidance regarding which role in the organization is responsible or accountable for each practice. Once the key roles are assigned to responsible and accountable level(s), practitioners may determine that additional roles should be consulted and/or informed, based on the unique requirements and/or context of the enterprise.

Enterprises should periodically review RA(CI) levels and update roles and organizational structures according to the enterprise's context, priorities and preferred terminology.

Based on guidance in *COBIT 2019 Framework: Governance and Management Objectives*, the CISO is responsible or accountable for the following practices (**figure 3.5**).[9]

Figure 3.5—RA(CI) Chart for CISO

Responsible (R) or Accountable (A)	Objective	Practice	Practice Name
R	EDM03	EDM03.03	Monitor risk management.
R	APO01	APO01.02	Communicate management objectives, direction and decisions made.
R		APO01.03	Implement management processes (to support the achievement of governance and management objectives).
R	APO12	APO12.01	Collect data.
R		APO12.06	Respond to risk.
R	APO14	APO14.01	Define and communicate the organization's data management strategy and roles and responsibilities.
R		APO14.02	Define and maintain a consistent business glossary.
R		APO14.03	Establish the processes and infrastructure for metadata management.
R		APO14.04	Define a data quality strategy.
R		APO14.05	Establish data profiling methodologies, processes and tools.
R		APO14.06	Ensure a data quality assessment approach.
R		APO14.07	Define the data cleansing approach.
R		APO14.08	Manage the life cycle of data assets.
R		APO14.09	Support data archiving and retention.
R		APO14.10	Manage data backup and restore arrangements.
R	DSS04	DSS04.01	Define the business continuity policy, objectives and scope.
R		DSS04.05	Review, maintain and improve the continuity plans.
R		DSS04.08	Conduct post-resumption review.
R	DSS06	DSS06.02	Control the processing of information.
R		DSS06.03	Manage roles, responsibilities, access privileges and levels of authority.
R		DSS06.04	Manage errors and exceptions.
R		DSS06.05	Ensure traceability and accountability for information events.
R		DSS06.06	Secure information assets.
A	APO13	APO13.01	Establish and maintain an information security management system (ISMS).
A		APO13.02	Define and manage an information security risk treatment plan.
A		APO13.03	Monitor and review the information security management system (ISMS).
A	DSS05	DSS05.01	Protect against malicious software.
A		DSS05.02	Manage network and connectivity security.
A		DSS05.03	Manage endpoint security.
A		DSS05.04	Manage user identity and logical access.
A		DSS05.05	Manage physical access to I&T assets.
A		DSS05.07	Manage vulnerabilities and monitor the infrastructure for security-related events.

[9] A RA(CI) chart by roles based on *COBIT® 2019 Framework: Governance and Management Objectives* may be found in the COBIT toolkit; see *https://www.isaca.org/resources/cobit.*

3.4.2 Key Organizational Structures and Roles for Information Security

Management objectives APO13 *Managed security* and DSS05 *Managed security services* contemplate the use and optimization of several key information security decision-making roles and organizational entities in an enterprise (note that some of these roles would be considered consulted or informed). **Figures 3.6** to **3.10** describe the mandate, operating principles, responsibilities, authority level, and delegation and escalation rights associated with roles and entities appropriate for enterprises of a certain size and complexity that handle sensitive information:

- Chief information security officer (CISO)
- Information security steering committee (ISSC)
- Information security manager (ISM)
- Information owner
- Information custodian

Many large enterprises—or those with a more robust focus on information security—may require additional groups and/or roles, including:

- Information security administrators
- Information security architects
- Information security compliance and auditing officers

Governance practitioners should carefully consider the relationship between information security and IT within enterprises. When the information security function reports directly to IT, there may be a conflict of interest. IT necessarily provides services to the enterprise, while information security manages risk related to the protection of information. This dichotomy could allow IT to override or curtail information security practices—for example, in an effort to increase IT performance or expedite IT delivery.

Therefore, IT and information security require a certain autonomy, or mutual independence, to fulfill their respective missions, and their organizational relationship should be reviewed on a regular basis. Certain security operations can be effective only by virtue of being an integral part of IT operations; however, information security does not need to be a single function within the enterprise. Information security risk, for example, may be separated from information security operations, under a different reporting line (even within IT), to ensure there is no conflict of interest.

Figure 3.6—Key Information Security Roles/Structures: Chief Information Security Officer (CISO)

Mandate	Overall responsibility of the enterprise information security program
Operating Principles	• Depending on a variety factors within the enterprise, the CISO may report to the chief executive officer (CEO), chief operating officer (COO), chief information officer (CIO), chief technology officer (CTO), chief data officer (CDO), chief risk officer (CRO) or other senior executive management. • The CISO is the liaison between executive management and the information security program. The CISO should communicate and coordinate closely with key business stakeholders to address information protection needs. • The CISO must: ▪ Understand the business strategic vision accurately ▪ Communicate effectively ▪ Build effective relationships with business leaders ▪ Translate business objectives into information security requirements

Figure 3.6—Key Information Security Roles/Structures: Chief Information Security Officer (CISO) *(cont.)*	
Span of Control	
Area	**Description**
Responsibilities	The CISO is responsible for: • Developing the IS strategy • Establishing and maintaining an information security management system (ISMS) • Monitoring and reviewing the ISMS • Defining and managing an information security risk treatment plan • Reporting to the board and the audit committee • Developing a budget for enterprise security • Chairing the ISSC and liaising with ERM committee See also **figure 3.5**.
Authority level/decision rights	The CISO is responsible for implementing and maintaining the information security strategy. Accountability (and sign-off of important decisions) resides in the function to which the CISO reports—for example, a senior executive management team member or the ISSC.
Delegation and Escalation	
Area	**Description**
Delegation rights	The CISO should delegate tasks to information security managers and business people.
Escalation rights	The CISO should escalate key information risk-related issues to his/her direct supervisor and/or the ISSC.

Figure 3.7—Key Information Security Roles/Structures: Information Security Steering Committee (ISSC)	
Mandate	Monitoring and review to ensure effective and consistent implementation of good practices in information security
Operating Principles	• The ISSC meets on a regular basis, as needed by the enterprise. More frequent meetings may be scheduled during specific initiatives, or when issues demand urgent attention. • Substitutes or proxies are allowed but should be limited. • Committee membership should be limited to a relatively small group of strategic and tactical leaders to ensure appropriate bidirectional communication and decision making. Other business leaders may be invited as needed. • Minutes of all meetings should be approved within a certain period and retained. • The CISO chairs the ISSC meetings.
Composition	
Role	**Description**
CISO	• Chairs ISSC and serves as liaison to enterprise risk management (ERM) committee • Responsible for overall enterprise information security
ISM	• Communicates design, implementation and monitoring of practices. When applicable, the ISM discusses design solutions beforehand with the information security architects to mitigate identified information risk.

Figure 3.7—Key Information Security Roles/Structures: Information Security Steering Committee (ISSC) *(cont.)*	
Composition *(cont.)*	
Role	**Description**
Business representatives	• Own business processes or applications • Responsible for communicating business initiatives that may impact information security and identifying information security practices that may impact the user community • Understands business/operational risk, costs and benefits, and specific information security requirements for their business areas
IT manager	• Reports on the status of I&T-related information security initiatives
Representatives of specialist functions	• Offers specialist/expert input when relevant, from perspectives including (for example) internal audit, HR, legal, risk or project management office (PMO). These functions may join the ISSC on occasion or as permanent members. (It may be worthwhile for representatives of internal audit to join as permanent members and advise the committee on compliance risk.)
Span of Control	
Area	**Description**
Responsibilities	The ISSC is responsible for enterprisewide information security decision making and sometimes responsible for oversight of the governance of information systems.
Authority level/decision rights	The ISSC is responsible for enterprise information security decisions in support of strategic decisions of the ERM committee.
Delegation and Escalation	
Area	**Description**
Delegation rights	The ISSC is ultimately responsible for the design and implementation strategy of the information security program and cannot delegate this responsibility to other member roles.

Figure 3.8—Key Information Security Roles/Structures: Information Security Manager (ISM)	
Area	**Description**
Mandate	Overall responsibility for management of information security efforts
Operating Principles	Reports to CISO (or, in some enterprises, to business unit leads)
Span of Control	
Area	**Description**
Responsibilities	The ISM is responsible for information security application, infrastructure, access management, threat and incident management, risk management, awareness program, metrics, and vendor assessments.
Authority level/decision rights	The ISM has overall decision making authority over information security domain practices.
Delegation and Escalation	
Area	**Description**
Delegation rights	The ISM should not delegate decisions related to information security domain practices.
Escalation rights	The ISM should escalate issues to the CISO.

Figure 3.9—Key Information Security Roles/Structures: Information Owner	
Mandate	Overall accountability for a specific information asset; usually the most senior officer in a division or business unit
Operating Principles	Reports to the CIO or CISO
Span of Control	
Area	**Description**
Responsibilities	The information owner is responsible for: • Assigning a clear and appropriate classification to information assets • Ensuring compliance with legal and regulatory requirements • Defining requirements for access to information assets
Authority level/decision rights	The information owner has overall decision-making authority over the information assets and their classification schemes.
Delegation and Escalation	
Area	**Description**
Delegation rights	The information owner will delegate information security tasks and maintenance to the information custodian.
Escalation rights	The information owner will escalate all issues to the CIO or CISO.

Figure 3.10—Key Information Security Roles/Structures: Information Custodian	
Mandate	Overall responsibility for overseeing and implementing necessary safeguards to protect information assets, according to rules classified by information owner(s), to ensure proper security, confidentiality, integrity and accessibility
Operating Principles	Reports to information owner
Span of Control	
Area	**Description**
Responsibilities	The information custodian is responsible for: • Ensuring that information assets are assigned appropriate security classifications • Assigning and removing access to information assets • Implementing appropriate physical and technical safeguards • Ensuring that information users receive appropriate training and support materials • Regularly reviewing access to information assets and their data • Staying informed on information security and data-protection issues
Authority level/decision rights	The information custodian has overall decision-making authority on accessibility for information assets.
Delegation and Escalation	
Area	**Description**
Delegation rights	The information custodian can delegate day-to-day activity associated with custody of information assets/data to data managers.
Escalation rights	The information custodian will escalate issues to information owners.

3.5 Component: Information Flows and Items

Component C: Information Flows and Items provides guidance on information flows and items related to process practices. For each practice, relevant inputs and outputs indicate the information item origin and destination—both inside and outside of COBIT—which provide input to or constitute output from the given practice (**figure 3.11**). For each governance and management objective, chapter 4 of this publication outlines detailed, security-specific examples of information that are common in an information security governance and management context.

Figure 3.11— Display of Information Security-specific Information Flows and Items Component

C. Component: Information Flows and Items				
Governance/Management Practice	Information Security-specific Inputs		Information Security-specific Outputs	
<REF><NAME>	From	Description	Description	To
	<REF>	<TEXT>	<TEXT>	<REF>

Note that the practices for management objectives APO13 *Managed security* and DSS05 *Managed security services* have no security-specific inputs and outputs from/to themselves, as they are already focused on security; however, these objectives nevertheless receive other inputs and outputs from practices in other governance and management objectives.

Several information security-related information types—specific to objectives APO13 and DSS05—warrant additional discussion:

- Information security strategy (APO13) (**figure 3.12**)
- Information security budget (APO13) (**figure 3.13**)
- Information security plan/program (APO13) (**figure 3.14**)
- Information security requirements (APO13) (**figure 3.15**)
- Information security review report (APO13) (**figure 3.16**)
- Information security management report (DSS05) (**figure 3.17**)
- Information security service catalog (DSS05) (**figure 3.18**)

Figure 3.12—Information Security Strategy

Description	Information security strategy provides the enterprise with adequate direction on the matter of information security; this strategy includes the entire enterprise—for example, senior management, audit, business management, IT development and IT operations. Typically, an enterprise defines a strategy for the medium term to support achievement of the desired future state, but allowing for short-term (e.g., annual) updates. The information security strategy should be made available to all relevant stakeholders.
Goals and quality criteria	Information security strategy should strive to be state of the art and in line with generally recognized principles. Architecture and design should align with the organization's enterprise architecture and specific situation; it should be comprehensive and complete, and contain all required information at the appropriate level of detail to be actionable. The information security strategy should be accessible only to those who need access (i.e., the stakeholders).
Metrics	Information security strategy goals can be measured by metrics including: • Percent of information security activities that follow a recognized framework or are benchmarked against peers • Number of mismatches between information security strategy and architecture and enterprise architecture • Percent of stakeholders without access to information security strategy • Number of information security violations

Figure 3.12—Information Security Strategy *(cont.)*	
Structure/high-level content	The CISO/ISM is responsible for developing the information security strategy for the enterprise. The development of the information security strategy is described as follows: *The business strategy provides the basis for a road map to achieving the business objectives. In addition, it should provide one of the primary inputs into... the information security strategy. This flow serves to promote alignment of information security with business goals. The balance of inputs comes from determining the desired state of [information] security compared to the existing, or current, state. Business processes must also be considered, as well as key organizational risk, including regulatory requirements, risk analysis and the associated impact analysis to determine protection levels and priorities...* *The objective of the [information] security strategy is the desired state defined by business and [information] security attributes. The strategy provides the basis for an action plan comprised of one or more [information] security programs that, as implemented, achieve the [information] security objectives. The action plan(s) must be formulated based on available resources and constraints, including consideration of relevant legal and regulatory requirements.* *The strategy and action plans must contain provisions for monitoring as well as defined metrics to determine the level of success. This provides feedback to the CISO and steering committee to allow for midcourse correction and ensure that information security initiatives are on track to meet defined objectives.*[10] In this development process, the CISO/ISM should consider the following factors, given that various constraints may influence the information security strategy: • Legal and regulatory requirements • Culture • Organizational structure • Costs • Resources • Capabilities • Time • Risk acceptance and tolerance The information security strategy should address the following topics, among others: • Alignment of information security activities with overall enterprise objectives • Information risk management, including the information risk management system that will be implemented throughout the enterprise. Such a system requires: ▪ Enterprise view of strategic objectives and risk ▪ Definition of enterprisewide risk appetite ▪ Enterprisewide policy on risk response options and selection ▪ Risk monitoring • Overall principles and approach to governance and management, including: ▪ Principles and policies ▪ Organizational structures ▪ Processes and practices ▪ Skills, culture elements and behaviors

[10] ISACA, *CISM Review Manual, 15th Edition*, USA, 2016, section 1.7, pages 44-45, *https://www.isaca.org/bookstore/cism-exam-resources/cm15ed*

Figure 3.12—Information Security Strategy *(cont.)*	
Structure/high-level content *(cont.)*	• These considerations are critical to set direction and monitor information security appropriately, so it aligns with enterprise objectives and risk appetite. Governance defines, among other elements, accountability, responsibility and decision making. • The following areas should also be contemplated, developed and aligned with the information security strategy: ▪ **Information security architecture**—Including major logical grouping(s) of capabilities to manage information security (e.g., information, applications, technology and their relationships to business processes) ▪ **Compliance**—Including all applicable rules and regulations throughout the enterprise, and the system of policies, procedures and other measures that the enterprise implements not only to comply with regulations but also to monitor compliance on a continuous basis ▪ **Information security operations**—Including information security-related operational processes and procedures (e.g., information security administration, monitoring and incident response) ▪ **Information security road map**—Outlining the secure future state, including people, processes, technologies and other resources

Figure 3.13—Information Security Budget	
Description	Budgeting for information security depends on where accountability and responsibility for information security reside within the enterprise. This publication assumes that the information security function is empowered to develop its own information security budget. This is the most effective method for ensuring that adequate information security resources are provided. Typically, enterprises have a yearly budget cycle. Budgets for information security-related costs and investments should follow this cycle.
Goals and quality criteria	The information security budget should be adequate (ensuring appropriate resources), accurate, and contain correct and realistic amounts for all budget items. The budget should be comprehensive and complete, and should align with enterprise security requirements and overall risk appetite. The information security budget should be available on a timely basis and accessible only to those who need access (i.e., stakeholders).
Metrics	Examples of metrics for the budget include: • Number of additional budget requests made after the annual budgeting cycle (to review and assess budget evolution) • Number of discrepancies between information security budget and overall security needs (e.g., a budget vs. actual needs review) • Difference between budget and actual costs • Percent of stakeholders without access to the information security budget The CISO has responsibility for developing a budget for the information security function, as part of the budget cycle of the organizational entity to which the information security function reports, applying the enterprisewide budget process, and including an overview of information security-related investment and expenditures across the enterprise. The information security budget should be framed in such a manner as to ensure that it provides funding for the information security program and enable appropriate information security support to the business. The information security program includes all investments required to execute the information security strategy and architecture. In this context, it is important to have a proper budget allocation process in place.

Figure 3.13—Information Security Budget *(cont.)*	
Structure/high-level content	The information security-related budget can include the following items: • Budget for operating the information security function (staff cost, infrastructure, technology, projects) • Budget for the information security program, which can include: ■ One-off costs and investments to set up the information security function and processes to execute information security-related projects ■ Recurring costs for operational information security measures (information security administration, monitoring, reporting, compliance) ■ Security awareness program costs ■ Continuous improvement of security skills (security expert training, certification, travel, conferences) ■ Corporate security certifications and external security audit costs ■ Outsourcing costs ■ Preparation for incident response costs Information security budgets also are subject to regular follow-up (actual vs. budget, variances) according to the enterprise's policies and processes.

Figure 3.14—Information Security Plan/Program	
Description	The information security plan/program are based on an information security strategy, which includes a sound risk analysis/management plan and addresses all information risk that exceeds the risk appetite. It also covers all risk response types (avoid, mitigate, transfer, accept), particularly addressing risk mitigation and risk transfer (e.g., insurance). The information security plan/program is created and regularly revisited and updated, as needed, by the ISSC, synchronized with the budget cycle.
Goals and quality criteria	The information security plan/program should be accurate, comprehensive and complete, and contain correct and realistic actions based on the information security strategy. It should align with enterprise architecture and context, and should be in line with overall risk appetite. The information security plan/program should be available on a timely basis and accessible only to those who need access (i.e., stakeholders).
Metrics	These goals can be measured by metrics including: • Number of actions that could not be implemented or executed • Number of mismatches between the information security plan/program and enterprise architecture • Percent of stakeholders without access to the plan/program • Number of violations against the plan
Structure/high-level content	The CISO/ISM has the responsibility of developing the information security plan/program. The information security plan/program define all investments required to execute the information security strategy and architecture. The information security plan/program are defined in terms of all governance components: • Processes that need to be defined, implemented or strengthened • Organizational structures that need to be set up or strengthened • Information flows related to information security management that need to be implemented • Policies and procedures that need to be defined and put in practice • Information security culture that needs to be adjusted or maintained • Skills and behaviors that need to be built up or changed • Capabilities that need to be acquired (e.g., technology for information security, information security-specific applications and services)

Figure 3.15—Information Security Requirements	
Description	Information security requirements are part of the overall requirements for any type of governance component. They typically apply to new applications and infrastructure, but they can also apply to other equipment. Information security requirements are defined at several trigger points: • At the beginning of new business projects, as part of the overall business and functional requirements (information security is a business requirement; information security requirements are reviewed throughout the life cycle of an initiative) • During contract development/agreements with third parties • When investigating company acquisitions/mergers (e.g., putting requirements in place for managing brand-name threats)
Goals and quality criteria	Information security requirements should be accurate and realistic, and should align with business and regulatory needs. Requirements should be made available on a timely basis and be accessible only by stakeholders (i.e., those who need access).
Metrics	Examples of metrics include: • Number of projects with information security requirements reviewed by the information security function • Number of requirements that are not met • Number of requirements that are delivered in organizational projects or that are missing from delivered projects • Number of signed acceptances by end users, indicating their receipt and acknowledgment of the latest security requirements
Structure/high-level content	Information security requirements are the responsibility of the end user—for example, the business process owner (for applications) or IT management (for IT infrastructure). Information security requirements are defined relative to the business impact, goals and criteria in terms of: • **Confidentiality**—Preserving authorized restrictions on access and disclosure, including means for protecting privacy and proprietary information. Typical questions include: ▪ Who has access to information, on the basis of what job needs? ▪ Who has access to data sets owned by different organizational structures and who does not? • **Integrity**—Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity. This applies to specifications for information (application controls for information/transactions), policies (integrity of policies), etc. • **Availability**—Ensuring timely and reliable access to and use of information

Figure 3.16—Information Security Review Report	
Description	Information security management reporting requires many types of reports, including: • Information security audit findings • Information security maturity report • Information security-related risk management reports, such as: ▪ Threat analysis reports or documentation ▪ Vulnerability (information security) assessment reports ▪ Business impact analysis (BIA) Threat analysis should be both periodic and event driven (i.e., updated periodically *and* when specific events occur). Examples of events that might necessitate an update of the threat analysis include new projects or a change in business initiatives.
Goals and quality criteria	Information security management reporting should be accurate and complete, with spending targeted to areas of identified risk, and a focus on reducing expenditures required to recover from exploits or incidents (including minimizing revenue losses). Threat analyses should identify all relevant, significant threats to the business and develop an appropriate action and risk response. Dashboards for key stakeholders should be updated on a timely basis and should be accessible only to those who need access (i.e., stakeholders).
Metrics	Information security management reporting can be measured by metrics including: • Number of threat analyses presented per year • Number of threats identified • Percent of threats addressed with information security practices • Percent of updates performed as scheduled • Percent of stakeholders without access • Number of information security violations
Structure/high-level content	To stay current on threats, the CISO and IT and business managers should follow the latest information security-related news and research, sourced from information-sharing forums, industry forums and information-sharing and analysis centers (ISACs). They should also periodically connect with threat-intelligence vendors. Internal and external loss data provide information to enable the creation of scenarios that can be used to further analyze threats. Organizations should conduct a high-level threat analysis to identify strategic information risk. For example, if a bank does not comply with information security requirements driven by a local financial supervisory authority, it may lose its license to operate. The enterprise risk management (ERM) function should define and implement threat analysis as part of the risk management process, to aid business stakeholders in identifying, assessing, mitigating and predicting threats (to information security and other areas) in a preventive way. Effective analysis requires appropriate experts from the respective enterprise areas. Threat analysis should be created by the business managers, IT managers and the CISO/chief security officer (CSO). Participants need the appropriate functional skills and knowledge to perform threat analyses. (It should be remembered that people are a key source of violations, and may contribute to the materialization of threats.) Threat analysis can be supported, to some extent, by technology that gathers information. For example, technology may assist with log correlation and analysis using security information and event management (SIEM) systems, data mining or business intelligence (for pattern recognition), and data loss tools to identify data leakage or detect fraud. The outcome of threat analysis is a confidential document that serves as input for the risk profile, information security design and information security management program. It should be restricted to the relevant business, IT and information security managers, and should be stored and updated by the CSO/CISO.

Figure 3.17—Information Security Management Report	
Description	Information security management reports (or dashboards) should contain all reports, events and additional information as stated in the information security requirements. The reports should be stored centrally and made available to all stakeholders in the form of a dashboard. Extracts or summaries can be produced, depending on the need or level of interest of a specific stakeholder. Report components should be renewed on a regular basis. Frequency of update depends on the data type and criticality. For example, information security incidents may require immediate online updates, whereas other components—such as information security action plan status—may update monthly.
Goals and quality criteria	Information security management reports should contain all events and additional information as stated in the information security requirements. Required information should reflect the appropriate level of detail to be actionable. Reports for key stakeholders should be updated on a timely basis and should be accessible only to those who need access (i.e., stakeholders).
Metrics	Examples of metrics for these goals include: • Number of problems with report accuracy and completeness • Number of mismatches between information security report contents and information security requirements • Time needed to analyze reports and obtain required information • Percent of updates performed as scheduled • Percent of stakeholders without access to information security reports • Number of information security violations against information security reports
Structure/high-level content	When building and operating an information security management report, practitioners should remember that people are the greatest asset of any enterprise and integral to the successful implementation of the SIEM architecture; however, they need appropriate functional skills and knowledge. Enterprises should define and implement repeatable SIEM processes that will assist business stakeholders in accomplishing day-to-day business requirements. • Information security management reports should reference: ▪ Information regarding operational information and security-threats, threat levels and vulnerabilities ▪ Effectiveness and efficiency of information security activities ▪ Areas where improvement is required ▪ Information and systems subject to an unacceptable level of risk ▪ Actions required to help minimize information risk (e.g., reviewing the enterprise risk appetite, understanding the information security threat environment, and encouraging business and system owners to remedy unacceptable risk) ▪ Details of progress made since previous monitoring reports ▪ Financial information regarding the cost of information security controls and the financial impact of information security incidents

Figure 3.18—Information Security Service Catalog	
Description	The information security service catalog should provide an overview of the technology resource and service portfolio that security can deliver to the business to proactively manage information security. It is of the utmost importance to mitigate risk to the organization's critical assets and overall business.
Goals and quality criteria	The information security service catalog should include a complete and diverse set of services that provide high value and help organizations secure and maintain the confidentiality, integrity and availability of their critical assets and processes. Some of the benefits that should be achieved through a complete service catalog are: • Improved risk management • Ability to solve specific security problems • Enhanced operational efficiencies and security
Metrics	Information security service catalog metrics include: • Number of identified threats that could not be solved by a service in the catalog • Number of services in the catalog • Percentage of issues addressed by the catalog
Structure/high-level content	The service catalog is intended to help the IT service provider efficiently and effectively manage and meet end-user expectations. Therefore, the security service catalog needs to be produced and maintained to provide an accurate and complete set of information on services, including: • Security assessment • Risk and compliance service • Incident response • File integrity monitoring • Information security training and awareness • Vulnerability scanning service • Security monitoring and alerting • Security device management

3.6 Component: People, Skills and Competencies

In *COBIT 2019 Framework: Governance and Management Objectives*, the people, skills and competencies governance component identifies human resources and skills required to achieve the governance or management objective.

COBIT 2019 based this guidance on the *Skills Framework for the Information Age* (SFIA®), version 6.[11] All skills are described in detail in the SFIA framework. (Because there is no change from the COBIT core model, references to SFIA are not detailed in *COBIT Focus Area: Information Security*.)

To operate an information security function effectively in an enterprise, individuals with appropriate knowledge and experience (e.g., skills and competencies) must exercise that function.

In management objectives APO13 *Managed security* and DSS05 *Managed security services,* some typical security-related skills and competencies are listed. While these skills can also translate to a specific position in larger enterprises (e.g., information security architecture skills may define an information security architect position), this is not always the case in smaller enterprises. The skills/competencies are:

- Information security governance (APO13) (**figure 3.19**)
- Information assessment and testing and compliance (APO13) (**figure 3.20**)

[11] SFIA Foundation, *Skills Framework for the Information Age,* version 6, United Kingdom, 2015, *https://www.sfia-online.org/en/framework/sfia-6*

- Information security strategy development (APO13) (**figure 3.21**)
- Information security architecture development (APO13) (**figure 3.22**)
- Information risk management (APO13) (**figure 3.23**)
- Information security operations (DSS05) (**figure 3.24**)

Skills and competencies follow a life cycle. An information security function must identify its current skill base —and then align the skill base to the required skill set. This alignment is influenced by the information security strategy and goals (among other factors). Skills need to be developed (e.g., through classroom and hands-on training) or acquired (e.g., through recruitment) and deployed in the various roles within the structure. Skills may need to be realigned if, for example, an activity is automated or outsourced. The enterprise should assess its skill base periodically (e.g., annually) to understand the evolution of the skill base over time; this assessment, in turn, will inform the planning process for the next period, and may also factor into the employee reward and recognition process for human resources.

Figure 3.19—Information Security Governance

Description
This skill establishes and maintains an information security governance framework and supporting processes to ensure that the information security strategy is aligned with organizational goals and objectives, information risk is managed appropriately, and program resources are managed responsibly.

Experience, Education and Qualification	
Requirement	**Description**
Experience	Several years of experience in information security and IT/business management (recommended), including experience in: • Creating, implementing and measuring information security policies • Ensuring information security compliance with external regulations • Aligning information security strategy with corporate governance • Creating information security policies that align with business needs; devising methods to measure policy effectiveness • Communicating with executive leadership
Education/qualification	CISM, CGEIT

Knowledge, Technical Skills and Behavioral Skills	
Requirement	**Description**
Knowledge	Ability to: • Define metrics that apply to information security governance • Create a performance measurement model based on the information security governance metrics, to ensure that organizational objectives are achieved • Develop a business case justifying investments in information security Knowledge of: • Legal and regulatory requirements affecting information security • Roles and responsibilities required for information security throughout the enterprise • Methods to implement information security governance policies • Fundamental concepts of governance and how they relate to information security • Internationally recognized standards, frameworks and good practices related to information security governance and strategy development
Technical skills	Good understanding of information security practices that apply to the specific business
Behavioral skills	• Proven leader with excellent communication skills • Process orientation

Figure 3.20—Information Assessment and Testing and Compliance	
Description	
This skill manages the information security program in alignment with the information security strategy, including: • Planning, establishing and managing the capability to detect, investigate, respond to and recover from information security incidents to minimize business impact • Performing user provisioning tasks for enterprise systems and application environments • Assisting with definition of roles and access models for various application and platform environments • Monitoring and maintaining technology platforms and access management solutions that support the access management capabilities • Managing network and connectivity information security • Managing endpoint information security • Protecting against malware • Handling security incident and event management	
Experience, Education and Qualification	
Requirement	**Description**
Experience	IT or information security experience (recommended), including: • Strong background in information security • Working knowledge of all information security functions in an enterprise and understanding of how they align with business objectives • Experience in implementing information security management program directives to protect corporate assets while minimizing corporate risk, liabilities and losses
Education/qualification	• CRISC, CISM, CISSP • Vendor- and technology-specific certifications
Knowledge, Technical Skills and Behavioral Skills	
Requirement	**Description**
Knowledge	Knowledge of: • Managing computer information security programs, policies, procedures and standards as they pertain to business activities • Log monitoring, log aggregation and log analysis
Technical skills	• Strong subject matter expertise in computer operation • In-depth knowledge of Windows®/UNIX® operating systems, authentication methods, firewalls, routers, web services, etc.
Behavioral skills	• Proficiency in managing projects and staff • Analytical mindset, detail orientation • Strong communication and facilitation skills • Strong time management skills

Figure 3.21—Information Security Strategy Development	
Description	
This skill defines and implements the information security vision, mission and goals, in alignment with corporate strategy and culture.	
Experience, Education and Qualification	
Requirement	**Description**
Experience	At least five years of experience in information security and IT/business management (recommended), including: ● Experience in information security strategy and governance ● Experience in creating and implementing strategies and information security principles, practices and activities ● A broad understanding of all information security functions and how they relate to the business
Education/qualification	CISM, CGEIT
Knowledge, Technical Skills and Behavioral Skills	
Requirement	**Description**
Knowledge	Ability to: ● Understand the enterprise culture and values ● Define an information security strategy that aligns with enterprise strategy ● Develop information security policies and devise metrics to measure the policies Knowledge of: ● Information security trends, services and disciplines ● Legal and regulatory requirements affecting information security ● Internationally recognized standards, frameworks and good practices related to information security strategy development
Technical skills	Broad understanding of identity access management, threat and vulnerability management, information security architecture, and data protection
Behavioral skills	● Proven leader with excellent communication skills and ability to interface with all levels of the enterprise ● Business orientation ● High-level strategic thinking ● Holistic understanding of global enterprise context

Figure 3.22—Information Security Architecture Development	
Description	
This skill oversees the design and implementation of the information security architecture.	
Experience, Education and Qualification	
Requirement	**Description**
Experience	Several years of experience in information security (recommended), including: • Experience working with hardware and software systems, operating systems (OSs), databases, applications and networks • Technical understanding of how various systems interconnect with each other
Education/qualification	• Good understanding of networking protocol, databases, applications and OSs, and their relevance to business processes • CRISC, CISM, CISSP, The Open Group Architecture Framework (TOGAF®), Sherwood Applied Business Security Architecture (SABSA®)
Knowledge, Technical Skills and Behavioral Skills	
Requirement	**Description**
Knowledge	Knowledge of: • Relationship of enterprise technologies and business and information security policies • Information security architectures (e.g., SABSA, TOGAF) and methods to apply them • Application design review and threat modeling • Methods to design information security practices • Managing computer information security programs, policies, procedures and standards as they pertain to business activities • Information security industry standards/good practices, including ISO/IEC 27000 series, Information Security Forum® (ISF), US National Institute of Standards and Technology (NIST), Payment Card Industry Data Security Standard (PCI DSS) • Information security-related laws and regulations • Emerging information security technologies and development methodologies
Technical skills	• Deep and broad knowledge of I&T and emerging trends • Technical design capabilities • Strong subject matter expertise in computer operations
Behavioral skills	• Abstract thinking and analysis • Problem-solving expertise

Figure 3.23—Information Risk Management	
Description	
This skill ensures that information risk is managed to comply with enterprise risk management (ERM) directives.	
Experience, Education and Qualification	
Requirement	**Description**
Experience	Several years of experience in information security and IT/business management (recommended), including: • Assessing risk related to information security practices • Mitigating risk based on enterprise business needs • Managing risk, profiling risk and assessing threats related to information security
Education/qualification	CRISC, CISM
Knowledge, Technical Skills and Behavioral Skills	
Requirement	**Description**
Knowledge	Knowledge of: • Methods to establish an information asset classification model consistent with business objectives • Risk assessment and analysis methodologies • Business processes and essential functions • Information security industry standards (e.g., NIST, PCI) • Information security-related laws and regulations (e.g., national and regional privacy legislation) • Risk frameworks and models, risk quantification, risk recording and risk reporting
Technical skills	• Understanding of information security practices, activities and associated risk • Risk analysis and mitigating controls
Behavioral skills	• Abstract thinking and analysis • Problem-solving expertise • Process orientation

Figure 3.24—Information Security Operations	
Description	
This skill defines and implements the information security vision, mission and goals, in alignment with corporate strategy and culture.	
Experience, Education and Qualification	
Requirement	**Description**
Experience	At least five years of experience in information security and IT/business management (recommended), including: • Experience in information security strategy and governance • Experience in creating and implementing strategies and information security principles, practices and activities • Understanding of all information security functions and their relations to the business
Education/qualification	CISM
Knowledge, Technical Skills and Behavioral Skills	
Requirement	**Description**
Knowledge	Ability to: • Understand enterprise culture and values • Define information security strategy that aligns with enterprise strategy • Develop information security policies and devise metrics to measure the policies Knowledge of: • Information security trends, services and disciplines • Legal and regulatory requirements affecting information security • Internationally recognized standards, frameworks and good practices related to information security strategy development
Technical skills	Broad understanding of identity access management, threat and vulnerability management, information security architecture, and data protection
Behavioral skills	• Proven leader with excellent communication skills and ability to interface with all levels of the enterprise • Business orientation • High-level strategic thinking • Holistic understanding of global enterprise context

3.7 Component: Principles, Policies and Procedures

Principles, policies and procedures document and communicate the enterprise rules that support governance objectives and enterprise values. To supplement the guidance on principles, policies and procedures in *COBIT 2019 Framework: Governance and Management Objectives*, this section elaborates detailed information security-specific principles and policies.

3.7.1 Principles

Information security principles should be limited in number and expressed in simple language.

More than a decade ago, three leading global information security organizations—ISACA, ISF and (ISC)²®—joined forces to develop 12 independent, nonproprietary principles to help information security professionals add value to their organizations by successfully supporting the business and promoting good information security practices. These principles are still valid today, and they are structured in support of three key tasks (**figure 3.25**):

- Support the business.
- Defend the business.
- Promote responsible information security behavior.

These principles are generic, apply to all enterprises, and can be used as a basis for developing information security principles unique to any organization.

Figure 3.25—Information Security Principles

Principle	Objective	Description
1. Support the business.		
Focus on the business.	Ensure that information security is integrated into essential business activities.	Individuals within the information security community should forge relationships with business leaders and show how information security can complement key business and risk management processes. They should adopt an advisory approach to information security by supporting business objectives through resource allocation, programs and projects. High-level, enterprise-focused advice should be provided to protect information and help manage information risk, both now and in the future.
Deliver quality and value to stakeholders.	Ensure that information security delivers value and meets business requirements.	Internal and external stakeholders should be engaged through regular communication so their changing requirements for information security can continue to be met. Promoting the value of information security (both financial and nonfinancial) helps to gain support for decision making, which can, in turn, foster success of the vision for information security.
Comply with relevant legal and regulatory requirements.	Ensure that statutory obligations are met, stakeholder expectations are managed, and civil or criminal penalties are avoided.	Compliance obligations should be identified, translated into requirements specific to information security and communicated to all relevant individuals. Penalties associated with noncompliance should be clearly understood. Controls should be monitored, analyzed and brought up to date to meet new or updated legal or regulatory requirements.
Provide timely and accurate reporting on information security performance.	Support business requirements and manage information risk.	Requirements for reporting information security performance should be clearly defined, supported by the most relevant and accurate information security metrics (such as compliance, incidents, control status and costs), and aligned to business objectives. Information should be captured in a periodic, consistent and rigorous manner so the information remains accurate and results can be presented to meet the objectives of relevant stakeholders.
Evaluate current and future information threats.	Analyze and assess emerging information security threats so that informed, timely actions can be taken to mitigate risk.	Major trends and specific information security threats should be categorized in a comprehensive, standard framework covering a wide range of topics such as political, legal, economic, sociocultural and technical issues. Individuals should share and build on their knowledge of upcoming threats to address their causes proactively, rather than just respond to symptoms.

Figure 3.25—Information Security Principles *(cont.)*		
Principle	**Objective**	**Description**
Promote continuous improvement in information security.	Reduce costs, improve efficiency and effectiveness, and promote a culture of continuous improvement in information security.	Constantly changing organizational business models—coupled with evolving threats—require information security techniques to be adapted and their level of effectiveness improved on an ongoing basis. Knowledge of the latest information security techniques should be maintained by learning from incidents and liaising with independent research organizations.
2. Defend the business.		
Protect classified information.	Prevent disclosure of classified (e.g., confidential or sensitive) information to unauthorized individuals.	Information should be identified and then classified according to its level of confidentiality (e.g., secret, restricted, internal and public). Classified information should be protected accordingly throughout all stages of the information life cycle—from creation to destruction—using appropriate controls such as encryption and access restrictions.
Concentrate on critical business applications.	Prioritize scarce information security resources by protecting the business applications on which an information security incident would have the greatest business impact.	Understanding the business impact of a loss of integrity or availability of important information handled by business applications (e.g., processed, stored or transmitted) will help to establish levels of criticality. Information security resource requirements can then be determined, and a priority placed on protecting the applications that are most critical to the success of the organization.
Develop systems securely.	Build quality, cost-effective systems (e.g., those that are consistently robust, accurate and reliable) on which businesspeople can rely.	Information security should be integral to the scope, design, build and testing phases of the system development life cycle (SDLC). Good information security practices (e.g., rigorous testing for information security weaknesses; peer review; and ability to cope with error, exception and emergency conditions) should play a key role at all stages of the development process.
3. Promote responsible information security behavior.		
Act in a professional and ethical manner.	Ensure that information security-related activities are performed in a reliable, responsible and effective manner.	Information security relies heavily on the ability of professionals within the industry to perform their roles responsibly and with a clear understanding of how their integrity has a direct impact on the information they are charged with protecting. Information security professionals must be committed to a high standard of quality in their work, while demonstrating consistent and ethical behavior and respect for business needs, other individuals and confidential (often personal) information.
Foster an information security-positive culture.	Provide a positive information security influence on the behavior of end users, reduce the likelihood of occurrence of information security incidents, and limit their potential business impact.	Emphasis should be placed on making information security a key part of business as usual, raising information security awareness among users and ensuring that they have the skills required to protect critical or classified information and systems. Individuals should be made aware of the risk to information in their care and empowered to take the necessary steps to protect it.

3.7.2 Policies

A comprehensive security policy should include statements that clearly document information security processes and procedures and drive compliance. Comprehensive policy would cover items including:

- Application security
- Architecture
- Cloud security
- Controls
- Encryption
- Endpoint security
- Engineering
- Information asset management
- Information classification
- Information security management (ISM)
- Mobile security
- Network and Internet security
- Patch management
- Program management
- Risk management
- Secure development
- Security assurance
- Security awareness and training
- Security configuration
- Security monitoring
- Security operations center (SOC)
- Security reporting
- Security testing
- Strategy
- Systems security
- Third-party risk
- Vulnerability management

Management objectives APO13 *Managed security* and DSS05 *Managed security services* reference example policies driven by different information security functions, including access control, personnel information, physical and environmental information, and security incidents. For each of the following policies, a description is provided, illustrating the scope and goals of the policy and paths for distribution to the proper audience (**figure 3.26**):

- Access control policy
- Information security and privacy policy
- Personnel information security policy
- Physical and environmental information security policy
- Security incident response policy

The information security policy should be actively communicated to the entire enterprise and distributed to all employees, contractors, temporary employees and third-party vendors. Stakeholders need to know the information principles, high-level requirements, and roles and responsibilities for information security. The responsibility for updating and revalidating the information security policy lies with the information security function (CISO/ISM), but approval of the overarching security policy must come from the board of directors.

Figure 3.26—Additional Detail on Objective APO13 Information Security Policies

Policy	Description
Access control policy	The access control policy provides proper access to internal and external stakeholders to accomplish business goals. This policy can be measured by metrics including: • Number of access violations that exceed the amount allowed • Amount of work disruption due to insufficient access rights • Number of segregation-of-duties (SoD) incidents or audit findings The access control policy should ensure that emergency access is appropriately permitted and revoked in a timely manner. Metrics related to this goal include: • Number of emergency access requests • Number of active emergency accounts exceeding approved time limits The access control policy should cover the following topics, among others: • Physical and logical access provisioning life cycle • Least privilege/need to know • SoD • Emergency access This policy is meant for all business units, vendors and third parties. Updates and revalidation should involve HR, data and system owners, and information security. A new or updated policy should be distributed to all corresponding business units, vendors and third parties.
Information security and privacy policy	Information security policies vary widely among enterprises. Some enterprises consider a one-page overview to be sufficient. In this case, the policy could be considered a directive statement, and it should clearly describe links to other specific policies. In other enterprises, the information security and privacy policy is fully developed, containing nearly all the detailed guidance needed to put the principles into practice. It is important to understand what the information stakeholders expect in terms of coverage and to adapt to this expectation. Regardless of size or degree of detail, the information security and privacy policy needs a clearly defined scope, including: • Definition of information security for the enterprise • Responsibilities associated with information security • Vision for information security, accompanied by appropriate goals and metrics, and an explanation of how the vision is supported by the information security culture and awareness • Explanation of alignment among the information security and privacy policy and other high-level policies • Elaboration of specific information security topics, such as data management; information risk assessment; and compliance with legal, regulatory and contractual obligations • Information security life cycle budget and cost management, information security strategic plans and portfolio management

Figure 3.26—Additional Detail on Objective APO13 Information Security Policies *(cont.)*	
Policy	**Description**
Information security and privacy policy *(cont.)*	This list is not exhaustive; more topics may be in scope, depending on the business context. It is important to innovate constantly and reuse good practices. Reuse and ongoing validation can be achieved via communication, reporting, and the required governance of technology and architecture. Enterprise context and interactions among stakeholders should be taken into account. The policy should be actively communicated to the entire enterprise, and distributed to all employees, contractors, temporary employees and third-party vendors. Stakeholders need to know the information principles, high-level requirements, and roles and responsibilities for information security. The responsibility for updating and revalidating the information security policy lies with the information security function (CISO/ISM).
Personnel information security policy	The personnel information security policy objective includes the following goals, among others: • Execute regular background checks of all employees and people at key positions. To measure this goal, count the number of completed background checks for key personnel. Review the number of overdue background check renewals, based on a predetermined frequency. • Acquire information about key personnel in information security positions. To measure this goal, count the number of personnel in key positions that have not rotated according to a predefined frequency. • Develop a succession plan for all key information security positions. One possible measure of this goal is to list all critical information security positions that lack backup personnel. • Determine whether information security personnel have the necessary current and pertinent skills and related certifications. A shortage in the number of critical information security positions with proper or qualified staffing could reflect the status of the goal. This policy applies to all business units, vendors and third parties. Updates and revalidation should involve HR, the privacy officer, the legal department, information security and facility security. A new or updated policy needs to be distributed to employees, contract personnel, vendors (as indicated under contract) and temporary employees.
Physical and environmental information security policy	The objective of this policy is to provide direction regarding: • Security of physical locations • Environmental controls that provide capabilities to support operations Security of physical locations can be measured by the number of identified, exploitable vulnerabilities and/or incidents attributed to physical location threats (criminal, transportation and industrial hazards, natural threats). Environmental controls can be verified by measuring the number of identified exploitable vulnerabilities and/or incidents attributed to environmental control systems. Indirectly, the policy contributes to optimizing insurance costs. Related metrics include the trending of insurance costs related to losses on account of physical, criminal and environmental threats. Scope of the policy can include: • Facility selection ▪ Criteria for selection ▪ Construction attributes • Environmental control standards • Physical access control standards (employee, vendor, visitor) • Information security monitoring and physical intrusion detection

Figure 3.26—Additional Detail on Objective APO13 Information Security Policies *(cont.)*	
Policy	**Description**
Physical and environmental information security policy *(cont.)*	This policy is intended for employees, all business units, vendors holding organizational assets and all visitors. Updates and revalidation should involve facilities, legal, information security, and data and system owners. A new or updated policy should be distributed to employees, contract personnel, vendors (as indicated under contract) and temporary employees.
Security incident response policy	The security incident response policy documents response goals and protocols, including target time frames for recovering business activities. The policy should cover: • Definition of an information security incident • Statements regarding incident handling • Requirements for incident response teams, organizational roles and responsibilities • Requirements for creating a tested incident response plan, which will provide documented procedures and guidelines for: ■ Criticality of incidents ■ Reporting and escalation process ■ Recovery, including: - Recovery time objectives (RTOs) for return to the trusted state - Investigation and preservation of process • Testing and training ■ Postincident meetings to document root cause analysis and enhancements of information security practices to prevent future similar events • Incident documentation and closing This policy is intended for all business units and key employees. Updates and revalidation should involve the information security function. A new or updated policy should be distributed to key employees.

3.8 Component: Culture, Ethics and Behavior

The governance component on culture, ethics and behavior provides guidance to optimize desired cultural elements within the organization that support the achievement of governance and management objectives.

Figure 3.27 identifies nine desirable information security behaviors that will positively influence culture toward information security and foster its implementation in the enterprise's day-to-day life:

- Everyone is accountable for the protection of information within the enterprise.
- Information security is practiced in daily operations.
- People respect the importance of information security policies and principles.
- People are provided with sufficient and detailed information security guidance and are encouraged to participate in and challenge the current information security situation.
- Stakeholders are aware of how to identify and respond to threats to the enterprise.

- Management proactively supports and anticipates new information security innovations and communicates them throughout the enterprise. The enterprise is ready to account for and address new information security challenges.
- Senior and middle management engages in continuous cross-functional collaboration to foster efficient and effective information security programs.
- Executive management recognizes the business value of information security.
- Management provides clear communication on information security (enabling awareness and training).

Each of the identified behaviors occurs in an enterprise at two levels: the **organizational level**, where behaviors are determined by the values (ethics, culture or attitude) by which the enterprise wants to live, and the **individual level**, where behaviors are defined by the personal values (ethics, culture or attitude) of the individual.

Behaviors can be influenced further by leadership at different levels of the enterprise. Three levels of leadership can be distinguished: information security management (CISO/ISM) at the information security level, business management at the business-unit level, and executive management at the top level. These layers of leadership influence behavior through the use of communication, enforcement and rules, incentives and rewards, and awareness. Three critical aspects of leadership are elaborated in **figure 3.28**.

Figure 3.27—Beneficial Behaviors

Beneficial Behavior	Description
Behavior 1: Everyone is accountable for the protection of information within the enterprise.	This accountability is reflected at two levels in the enterprise. At the organizational level, issues requiring accountability (discipline) are acted upon, and the roles of stakeholders are confirmed for enforcement. The individual level requires each individual to understand the responsibilities regarding information security.
Behavior 2: Information security is practiced in daily operations.	Information security is part of the enterprise's daily functioning. At the organizational level, the behavior indicates that information security is accepted as a business imperative in organizational goal setting. At the individual level, it means that the individual cares about the well-being of the enterprise and applies a prudent approach and information security techniques to his/her daily operations.
Behavior 3: People respect the importance of information security policies and principles.	The importance of information security policies and principles is acknowledged by the people in the enterprise. At the organizational level, policies and principles are endorsed by senior management, and approval, review and communication of policies occur on a regular basis. At the individual level, people have read and understood the policies, and they feel empowered to follow enterprise guidance.
Behavior 4: People are provided with sufficient and detailed information security guidance and are encouraged to participate in and challenge the current information security situation.	People are provided with sufficient information security guidance, and are encouraged to challenge the current information security situation at two levels. The organizational culture indicates a two-way communication process for guidance and feedback and provides stakeholders an opportunity to comment on changes; the individual culture demonstrates stakeholder participation via questioning and commentary, upon request.
Behavior 5: Stakeholders are aware of how to identify and respond to threats to the enterprise.	Appropriate processes for identifying and reacting to threats are implemented at the organizational level by installing a reporting process and an incident response process to minimize losses. At the individual level, people must be educated on what an information security incident is, and how to report and react to it.

Figure 3.27—Beneficial Behaviors *(cont.)*	
Beneficial Behavior	**Description**
Behavior 6: Management proactively supports and anticipates new information security innovations and communicates them throughout the enterprise. The enterprise is ready to account for and address new information security challenges.	Information security innovations and challenges are tackled at the organizational level through an information security research and development team. The individual culture contributes when stakeholders bring forward new ideas.
Behavior 7: Senior and middle management engages in continuous cross-functional collaboration to foster efficient and effective information security programs.	Cross-functional collaboration is fostered by organizationwide acceptance of a holistic information security strategy and improves integration of information security with the business. The individual contributes by reaching out to other business functions and identifying potential synergies.
Behavior 8: Executive management recognizes the business value of information security.	The business value of information security is recognized at the organizational level when information security is viewed as a means to improve business value (including revenue, expense optimization, reputation and competitive advantage). Transparency in response to incidents is key, and an understanding of consumer expectations is essential. At the individual level, behavior is marked by creative ideas to improve value through information security.
Behavior 9: Management provides clear communication on information security (enabling awareness and training).	Providing the content, delivery and analysis of information security-related training, education, news and events—clearly targeted for, and relevant to, given enterprise groups—will enable employees to include information security in their day-to-day work.

Figure 3.28—Leadership Aspects	
Leadership Aspect	**Description**
Aspect 1: Influencing behavior through communication, enforcement, and rules and norms	Leadership uses communication, enforcement, and rules and norms to influence behaviors in an enterprise. Communication is always essential to influence any kind of behavior. Enforcement of an information security culture depends on the degree of importance of information security within the broader enterprise culture. Rules can be used to force internal action where information security is legally mandated. Information security management (CISO/ISM) ensures that information security is embedded in enterprise policies and procedures and regular guidance and updates are performed. The CISO/ISM ensures annual recertification of policies and principles. Together with executive management, the CISO/ISM completes a formal sign-off of these policies. Business unit managers follow up on corrective actions and executive management conducts an annual review of information security performance. The CISO/ISM works together with business unit management to ensure stakeholder acknowledgment. The business unit managers also set an example by leading.[12] The CISO/ISM implements an incident management process, supported by a reporting mechanism, which includes trigger points for stakeholders (clients, vendors, etc.). Market trends are tracked by the CISO/ISM as well, for both information security and the business. While executive management ensures that information security is represented in the correct structures (e.g., committees, task forces, implementation teams), the CISO/ISM communicates the information security processes to the entire enterprise.
Aspect 2: Influencing behavior through incentives and rewards	Management influences behavior through measures designed to provide positive reinforcement for desired conduct and negative reinforcement for conduct it wishes to discourage. An absence of rewards inhibits adoption of an information security culture. Business management needs to know that secure behavior will be rewarded; this in turn means that executive management must make its intentions clear by encouraging the implementation of security safeguards and promoting attitudes that constitute a culture of security. Monetary rewards to individuals are not necessarily required; instead, incentives may include organizational advancement in the form of budget control, influence, management attention, etc. The following incentives and rewards may be implemented by various management levels to influence behavior: • Information security management (CISO/ISM) may organize sessions regarding information security in personal life (e.g., covering children and social media, wireless network setup) to embed information security in daily operations, give positive recognition for the information security achievement, and distribute bonuses for innovation within the information security function. The CISO/ISM is not the only level of management to give bonuses; executive management may also give rewards for alerting of threats or for any profitable idea. • Business management focuses on information security as a component of performance evaluation and ensures that it is embedded in all job descriptions, while executive management tailors incentives and rewards to the responsibility of the stakeholders. Business management is responsible for an annual review of the incentives and rewards program and ensures that information security policies are a requirement of employment (terms and conditions).

[12] Management behavior is probably one of the biggest influencers. Does management make decisions that support or contradict what it says? When management dismisses or disregards security policies, processes or requirements, it sets the tone at the top, and the rest of the organization adopts the same attitude.

Figure 3.28—Leadership Aspects *(cont.)*	
Leadership Aspect	**Description**
Aspect 3: Influencing behavior through raising awareness	Awareness programs have their place, but they are insufficient by themselves. People must be educated about security and their roles in it. Different management levels can raise awareness through a variety of means. Information security management may organize awareness training on information security topics, supported by regular update sessions, and ensure that policies are readily available (e.g., through Internet publication). The CISO/ISM is also responsible for sharing knowledge regarding changes in the threat landscape, regularly communicating new ideas and outcomes, keeping track of market trends, and performing competitive analyses. Business managers regularly follow these awareness training events and are responsible for notifications or requests for comments on proposed changes. Executive management ensures that information security incidents are communicated to staff.

To influence culture, the enterprise needs champions who advance changes throughout the organization. Champions include those who are eager to speak up and set examples for others. Champions may be the senior executives of an enterprise, but the role is not limited to that group. Staff members can be champions as well, as long as they actively provide the background for change and enforcement of a culture. ISACA's publication, *Creating a Culture of Security*,[13] outlines a number of common roles that can serve as information security champions:

- Risk managers/chief risk officer (CRO)
- Information security professionals
- C-level executives: CEO, COO, CFO, CIO
- Head of HR

Leadership—the decision makers in the information security context—can be equally important. Champions are needed to influence leadership to make decisions that reflect information security requirements.

3.9 Component: Services, Infrastructure and Applications

The services, infrastructure and applications governance component provides detailed guidance on third-party services, types of infrastructure and categories of applications that support achievement of governance and management objectives. (Guidance in this context remains generic—to avoid naming specific vendors or products.)

In the COBIT core model, the following services, infrastructure and applications are recommended in management objectives APO13 *Managed security* and DSS05 *Managed security services:*

- Configuration management tools
- Directory services
- Email filtering systems
- Identity and access management systems
- Security and privacy awareness services
- Security information and event management (SIEM) tools
- Security operations center (SOC) services
- Third-party security assessment services
- URL filtering systems

[13] ISACA, *Creating a Culture of Security*, USA, 2011, *https://www.isaca.org/bookstore/it-governance-and-business-management/wccs*

In addition to this list, the following additional services, infrastructure and applications should be considered for information security[14]:

- Alerting systems
- Anti-malware
- Anti-phishing
- Anti-spyware
- Biometrics
- Browser protection
- Cloud access security broker (CASB) systems
- Code scanners
- Compilers
- Deep packet inspection tools
- Device management provision tools
- DLP tools
- Endpoint detection and response systems
- File-integrity monitoring
- Fire protection system
- Firewall
- First responder interfaces
- Honeypots
- Incident response tools
- Information security testing tools
- Insider threat software
- Internet proxy system
- Intrusion prevention system (IPS)/Intrusion detection system (IDS)
- Local and remote encryption tools
- Locks
- Log analyzers
- Malware analysis tools
- Memory inspection tools
- Network access control systems
- Network analyzers
- Packet analyzers
- Passive and active network analyzers
- Penetration testing tools
- Privileged access management systems
- Ransomware detectors
- Real-time database activity monitoring solutions
- Regression analysis tools
- Release candidate push solutions

[14] Consult the ISACA Glossary for defintiions, *https://www.isaca.org/resources/glossary*

- Remote access controllers
- Reverse engineering tools
- Sandboxing
- Signature verification solutions
- Smart cards
- Sniffers
- Software distribution solutions
- Test scripts
- Threat Intelligence systems
- Unit test tools
- Vaults
- Virtual private networks (VPNs)
- Vulnerability scanners
- Webapp security tools
- Web application firewalls

Chapter 4

COBIT Governance and Management Objectives—Detailed Information Security-specific Guidance

4.1 Evaluate, Direct and Monitor (EDM)

Page intentionally left blank

Domain: Evaluate, Direct and Monitor Governance Objective: EDM01 — Ensured Governance Framework Setting and Maintenance	Focus Area: Information Security
Description	
Analyze and articulate the requirements for the governance of enterprise I&T. Put in place and maintain governance components with clarity of authority and responsibilities to achieve the enterprise's mission, goals and objectives.	
Purpose	
Provide a consistent approach integrated and aligned with the enterprise governance approach. I&T-related decisions are made in line with the enterprise's strategies and objectives and desired value is realized. To that end, ensure that I&T-related processes are overseen effectively and transparently; compliance with legal, contractual and regulatory requirements is confirmed; and the governance requirements for board members are met.	
Information Security Focus Area Relevance	
Information security is an integral part of the enterprise I&T governance framework and system that needs to be defined, evaluated and monitored.	

A. Component: Process	
Governance Practice	**Example Information Security-specific Metrics**
EDM01.01 Evaluate the governance system. Continually identify and engage with the enterprise's stakeholders, document an understanding of the requirements, and evaluate the current and future design of governance of enterprise I&T.	a. Number of business inquiries that could not be addressed by existing policies b. Percent of business units involved in policy updates c. Time between significant business changes and policy updates d. Frequency of policy updates e. Number of audit findings related to security policies f. Number of security incidents that are not related to a policy violation g. Stakeholder satisfaction with information security

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Analyze and identify the internal and external environmental factors (legal, regulatory and contractual obligations) and trends in the business environment that may influence the information security governance design.	2
2. Evaluate the extent to which information security meets business and compliance/regulatory needs.	
3. Articulate principles that will guide the design of information security and promote a security-positive environment.	
4. Understand the enterprise's decision-making culture and determine the optimal decision-making model for information security.	
5. Understand the enterprise's training program to promote a governance structure and environment.	3
6. Evaluate the extent to which information security is aligned to legal and regulatory trends.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	GE.AG Apply Governance System; GE.MG Monitor Governance System
ISO/IEC 38500:2015(E)	5.2 Principle 1: Responsibility (Evaluate)
ITIL V3, 2011	Service Strategy, 2.3 Governance and management systems
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Tasks 2, 3, 4, 5)

A. Component: Process *(cont.)*	
Governance Practice	**Example Information Security-specific Metrics**
EDM01.02 Direct the governance system. Inform leaders on I&T governance principles and obtain their support, buy-in and commitment. Guide the structures, processes and practices for the governance of I&T in line with the agreed governance principles, decision-making models and authority levels. Define the information required for informed decision making.	a. Percent of information security processes and practices with clear traceability to governance principles b. Number of information security breaches related to noncompliance with ethical and professional behavior guidelines

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Obtain senior management commitment to information security and information risk management.	2
2. Mandate an enterprisewide information security function.	
3. Establish an Information Security Steering Committee (ISSC), governed by a charter.	
4. Implement hierarchical information and decision-escalation procedures.	3
5. Integrate information security strategy with business strategy.	
6. Foster an information security-positive culture and environment.	
7. Ensure periodic reporting of key information security initiatives and issues to the board of directors.	4
8. Ensure the roles and responsibilities of the board of directors are documented and understood.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	GE.DG Direct Governance System
ISF, The Standard of Good Practice for Information Security 2016	SG1.1 Security Governance Framework
ISO/IEC 38500:2015(E)	5.2 Principle 1: Responsibility (Direct)
ISO/IEC 38502:2017(E)	Governance of IT - Framework and model (all chapters)
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas - Principle 12
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.14 Planning (PL-2, PL-10)

Governance Practice	Example Information Security-specific Metrics
EDM01.03 Monitor the governance system. Monitor the effectiveness and performance of the enterprise's governance of I&T. Assess whether the governance system and implemented mechanisms (including structures, principles and processes) are operating effectively and provide appropriate oversight of I&T to enable value creation.	a. Number of information security breaches related to noncompliance with information security-related legislation and regulation b. Number of active mandatory corrective-action initiatives

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Monitor regular and routine mechanisms for ensuring that the use of information security measurement systems complies with information security-related legislation and regulation.	4
2. Analyze the impact and overall implications of the changing threat landscape on the enterprise.	
3. Determine if the enterprise has a threat intelligence process.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISO/IEC 38500:2015(E)	5.2 Principle 1: Responsibility (Monitor)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.14 Planning (PL-11)

C. Component: Information Flows and Items				
Governance Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
EDM01.01 Evaluate the governance system.	Outside COBIT	Internal and external environmental factors (legal, regulatory and contractual obligations) and trends	Information security guiding principles	ISFA EDM01.02 ISFA APO01.01 ISFA APO01.02 ISFA APO01.04 ISFA APO02.01 ISFA APO02.05 ISFA APO12.03
EDM01.02 Direct the governance system.	ISFA APO02.05	Information security strategy	Information security-positive culture and environment	Internal
	ISFA EDM01.01	Information security guiding principles		
EDM01.03 Monitor the governance system.	Outside COBIT	Information security-related legislation and regulation	Governance compliance assessment	Internal

Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 2, 3, 4, 5): Inputs and Outputs

Page intentionally left blank

Domain: Evaluate, Direct and Monitor Governance Objective: EDM02 — Ensured Benefits Delivery	Focus Area: Information Security
Description	
Optimize the value to the business from investments in business processes, I&T services and I&T assets.	
Purpose	
Secure optimal value from I&T-enabled initiatives, services and assets; cost-efficient delivery of solutions and services; and a reliable and accurate picture of costs and likely benefits so that business needs are supported effectively and efficiently.	
Information Security Focus Area Relevance	
The business benefits, costs and risk of information security investments are balanced to achieve optimal value.	

A. Component: Process	
Governance Practice	**Example Information Security-specific Metrics**
EDM02.01 Establish the target investment mix. Review and ensure clarity of the enterprise and I&T strategies and current services. Define an appropriate investment mix based on cost, alignment with strategy, type of benefit for the programs in the portfolio, degree of risk, and financial measures such as cost and expected return on investment (ROI) over the full economic life cycle. Adjust the enterprise and I&T strategies where necessary.	a. Percent of I&T investments traceable to information security incidents
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Identify and record the requirements of stakeholders (such as shareholders, regulators, auditors and customers) for protecting their interests and delivering value through information security activity. Set direction accordingly.	2
2. Define an investment mix that achieves the right balance among a number of dimensions, including information security activities.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
King IV Report on Corporate Governance for South Africa, 2016	Part 5.5: Stakeholder relationships—Principle 17
The Open Group IT4IT Reference Architecture, Version 2.0	3.2 IT Value Chain and IT4IT Reference Architecture
Governance Practice	**Example Information Security-specific Metrics**
EDM02.02 Evaluate value optimization. Continually evaluate the portfolio of I&T-enabled investments, services and assets to determine the likelihood of achieving enterprise objectives and delivering value. Identify and evaluate any changes in direction to management that will optimize value creation.	a. Level of stakeholder satisfaction achieved based on ROI b. Percent of security risk reduction achieved per dollar
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Establish a method of demonstrating the value of information security (including defining and collecting relevant data) to ensure the efficient use of existing information security-related assets.	3
2. Ensure the use of financial and nonfinancial measures to describe the added value of information security initiatives.	
3. Use business-focused methods of reporting on the added value of information security initiatives.	4
4. Establish methods to measure the cost of security incidents.	
5. Establish processes to evaluate information security expenses against publicly known security incidents and potential regulatory fines in the industry.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
COSO Enterprise Risk Management, June 2017	7. Strategy and Objective-Setting—Principle 8
ISF, The Standard of Good Practice for Information Security 2016	SG2.2 Stakeholder Value Delivery
ISO/IEC 38500:2015(E)	5.3 Principle 2: Strategy (Evaluate)
King IV Report on Corporate Governance for South Africa, 2016	Part 5.2: Strategy, performance and reporting—Principle 4
The Open Group IT4IT Reference Architecture, Version 2.0	5. Strategy to Portfolio (S2P) Value Stream

A. Component: Process *(cont.)*	
Governance Practice	**Example Information Security-specific Metrics**
EDM02.03 Direct value optimization. Direct value management principles and practices to enable optimal value realization from I&T-enabled investments throughout their full economic life cycle.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Direct any required changes to the portfolio of investments and services to realign with new security-related risk and implications.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 38500:2015(E)	5.3 Principle 2: Strategy (Direct)
Governance Practice	**Example Information Security-specific Metrics**
EDM02.04 Monitor value optimization. Monitor key goals and metrics to determine whether the enterprise receives expected value and benefit from I&T-enabled investments and services. Identify significant issues and consider corrective actions.	a. Number of threats mitigated due to information security investments
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Track outcomes of information security initiatives and compare to expectations to ensure value delivery against business goals. Take appropriate management action as required.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 38500:2015(E)	5.3 Principle 2: Strategy (Monitor)

C. Component: Information Flows and Items				
Governance Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
EDM02.01 Establish the target investment mix.	Outside COBIT	Evaluation of strategic alignment	Updated portfolio	Internal
EDM02.02 Evaluate value optimization.	Outside COBIT	Investment types and criteria	Updated investment types and criteria	Internal
EDM02.03 Direct value optimization.	There are no information security-specific inputs for this practice.		Feedback on value delivery of information security initiatives	Internal
EDM02.04 Monitor value optimization.	There are no information security-specific inputs or outputs for this practice.			
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this practice				

Domain: Evaluate, Direct and Monitor Governance Objective: EDM03 — Ensured Risk Optimization	Focus Area: Information Security
Description	
Ensure that the enterprise's risk appetite and tolerance are understood, articulated and communicated, and that risk to enterprise value related to the use of I&T is identified and managed.	
Purpose	
Ensure that I&T-related enterprise risk does not exceed the enterprise's risk appetite and risk tolerance, the impact of I&T risk to enterprise value is identified and managed, and the potential for compliance failures is minimized.	
Information Security Focus Area Relevance	
Information security risk is an integral part of enterprise risk and is optimized within the enterprise risk appetite and tolerance.	

A. Component: Process		
Governance Practice	**Example Information Security-specific Metrics**	
EDM03.01 Evaluate risk management. Continually examine and evaluate the effect of risk on the current and future use of I&T in the enterprise. Consider whether the enterprise's risk appetite is appropriate and ensure that risk to enterprise value related to the use of I&T is identified and managed.	a. Percent of information security risk that is related to business risk	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.		N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
COSO Enterprise Risk Management, June 2017	Strategy and Objective-Setting—Principles 6 and 7; 9. Review and Revision—Principle 16	
Governance Practice	**Example Information Security-specific Metrics**	
EDM03.02 Direct risk management. Direct the establishment of risk management practices to provide reasonable assurance that I&T risk management practices are appropriate, and that actual I&T risk does not exceed the board's risk appetite.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.		N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
CMMI Cybermaturity Platform, 2018	RS.AS Apply Risk Management Strategy; BC.RO Determine Strategic Risk Objectives	
ISF, The Standard of Good Practice for Information Security 2016	IR1.1 Information Risk Assessment—Management Approach	
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas—Principle 11	
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.5 Assessment (Task 2)	

A. Component: Process *(cont.)*	
Governance Practice	**Example Information Security-specific Metrics**
EDM03.03 Monitor risk management. Monitor the key goals and metrics of the risk management processes. Determine how deviations or problems will be identified, tracked and reported for remediation.	a. Percent of business risk that has been effectively mitigated with information security controls

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	9. Review and Revision—Principle 17
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 7); 3.5 Assessment (Task 1); 3.6 Authorization (Task 1)
The Open Group IT4IT Reference Architecture, Version 2.0	6. Requirement to Deploy (R2D) Value Stream; 7. Request to Fulfill (R2F) Value Stream

C. Component: Information Flows and Items				
Governance Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
EDM03.01 Evaluate risk management.	Outside COBIT	Enterprise key risk indicators (KRIs)	Alignment of enterprise key risk indicators (KRIs) with information security KRIs	ISFA EDM03.02
	Outside COBIT	Enterprise risk appetite guidance	Information security risk acceptable level	ISFA EDM03.02 ISFA EDM03.03
EDM03.02 Direct risk management.	ISFA EDM03.01	Alignment of enterprise KRIs with information security KRIs	Updated risk management policies	Internal
	ISFA EDM03.01	Information security risk acceptable level		
EDM03.03 Monitor risk management.	ISFA APO01.01	Information security and related policies	Remedial actions to address risk management deviations	Internal
	ISFA EDM03.01	Information security risk acceptable level		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 7): Inputs and Outputs; 3.5 Assessment (Tasks 1, 2): Inputs 2, and Outputs; 3.6 Authorization (Task 1): Inputs and Outputs

Domain: Evaluate, Direct and Monitor Governance Objective: EDM04 — Ensured Resource Optimization	Focus Area: Information Security
Description	
Ensure that adequate and sufficient business and I&T-related resources (people, process and technology) are available to support enterprise objectives effectively and, at optimal cost.	
Purpose	
Ensure that the resource needs of the enterprise are met in the optimal manner, I&T costs are optimized, and there is an increased likelihood of benefit realization and readiness for future change.	
Information Security Focus Area Relevance	
Information security resourcing requirements are achieved in an optimal manner relative to their costs, benefits and associated risk.	

A. Component: Process	
Governance Practice	**Example Information Security-specific Metrics**
EDM04.01 Evaluate resource management. Continually examine and evaluate the current and future need for business and I&T resources (financial and human), options for resourcing (including sourcing strategies), and allocation and management principles to meet the needs of the enterprise in the optimal manner.	a. Percent of reuse of information security solutions b. Percent of staff that are employees c. Percent of staff that are contract employees
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Evaluate the effectiveness of information security resources in terms of provision, training, awareness and competencies.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	GR.DR Direct Resource Management Needs
ISO/IEC 38500:2015(E)	5.4 Principle 3: Acquisition (Evaluate)
Governance Practice	**Example Information Security-specific Metrics**
EDM04.02 Direct resource management. Ensure the adoption of resource management principles to enable optimal use of business and I&T resources throughout their full economic life cycle.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that information security resource management is aligned to business needs.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	GR.ER Evaluate Resource Management Needs
COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principle 5
ISO/IEC 38500:2015(E)	5.4 Principle 3: Acquisition (Direct)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.14 Planning (PL-4)
Governance Practice	**Example Information Security-specific Metrics**
EDM04.03 Monitor resource management. Monitor the key goals and metrics of the resource management processes. Determine how deviations or problems will be identified, tracked and reported for remediation.	a. Amount of deviation from information security budget b. Benchmarking of information security spending in relation to previous years and/or industry best practices
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Monitor the effectiveness, efficiency and capacity of information security resources against business needs.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	GR.MR Monitor Resource Management Needs
ISO/IEC 38500:2015(E)	5.4 Principle 3: Acquisition (Evaluate)

C. Component: Information Flows and Items				
Governance Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
EDM04.01 Evaluate resource management.	Outside COBIT	Approved resources plan	Updated information security resources	Internal
EDM04.02 Direct resource management.	Outside COBIT	Assigned responsibilities for resource management	Updated information security resources	Internal
EDM04.03 Monitor resource management.	There are no information security-specific inputs for this practice.		Remedial actions to address resource management deviations	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this practice				

Domain: Evaluate, Direct and Monitor Governance Objective: EDM05 — Ensured Stakeholder Engagement	Focus Area: Information Security
Description	
Ensure that stakeholders are identified and engaged in the I&T governance system and that enterprise I&T performance and conformance measurement and reporting are transparent, with stakeholders approving the goals and metrics and necessary remedial actions.	
Purpose	
Ensure that stakeholders are supportive of the I&T strategy and road map, communication to stakeholders is effective and timely, and the basis for reporting is established to increase performance. Identify areas for improvement, and confirm that I&T-related objectives and strategies are in line with the enterprise's strategy.	
Information Security Focus Area Relevance	
Stakeholders are engaged to provide information security direction based on periodic communication and reporting.	

A. Component: Process	
Governance Practice	**Example Information Security-specific Metrics**
EDM05.01 Evaluate stakeholder engagement and reporting requirements. Continually examine and evaluate current and future requirements for stakeholder engagement and reporting (including reporting mandated by regulatory requirements), and communication to other stakeholders. Establish principles for engaging and communicating with stakeholders.	a. Stakeholder satisfaction with the information security reporting process (timely, complete, relevant, reliable, accurate, etc.) and frequency, based on surveys
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Determine the audience, including internal and external individuals or groups, for communication and reporting on information security-related activities.	2
2. Identify requirements for reporting on information security to stakeholders (e.g., what information is required, when it is required, how it is presented).	
3. Identify the means and channels to communicate information security issues.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	SR.DR Direct Stakeholder Communication and Reporting
Governance Practice	**Example Information Security-specific Metrics**
EDM05.02 Direct stakeholder engagement, communication and reporting. Ensure the establishment of effective stakeholder involvement, communication and reporting, including mechanisms for ensuring the quality and completeness of information, overseeing mandatory reporting, and creating a communication strategy for stakeholders.	a. Effectiveness of information security status reports communicated to senior management b. Percent of reports with invalid reporting data
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Perform internal and external assessments to gauge the effectiveness of the information security governance program.	3
2. Produce for stakeholders regular information security status reports that include information security activities, performance, achievements, risk profile, business benefits, emerging technologies, outstanding risk and capability gaps.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	SR.AR Apply Stakeholder Reporting Requirements
King IV Report on Corporate Governance for South Africa, 2016	Part 5.5: Stakeholder relationships—Principle 16
King IV Report on Corporate Governance for South Africa, 2016	Part 5.2: Strategy, performance and reporting—Principle 5
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity V1.1, April 2018	3.3 Communicating Cybersecurity Requirements with Stakeholders

A. Component: Process *(cont.)*	
Governance Practice	**Example Information Security-specific Metrics**
EDM05.03 Monitor stakeholder engagement. Monitor stakeholder engagement levels and the effectiveness of stakeholder communication. Assess mechanisms for ensuring accuracy, reliability and effectiveness, and ascertain whether the requirements of different stakeholders in terms of reporting and communication are met.	a. Percent of information security reports that are delivered on time b. Percent of information security reports containing inaccuracies
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Establish information security monitoring and reporting (e.g., using key performance indicators [KPIs] for information security and information risk management that are based on metrics and measurements in the MEA domain).	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	SR.MC Monitor Stakeholder Communication

C. Component: Information Flows and Items				
Governance Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
EDM05.01 Evaluate stakeholder engagement and reporting requirements.	Outside COBIT	Evaluation of enterprise reporting requirements	Information security reporting requirements and communication channels	Internal
EDM05.02 Direct stakeholder engagement, communication and reporting.	There are no information security-specific inputs for this practice.		Information security status reports	Internal
EDM05.03 Monitor stakeholder engagement.	There are no information security-specific inputs for this practice.		Information security monitoring and reporting	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this practice				

4.2 Align, Plan and Organize (APO)

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO01 — Managed I&T Management Framework	Focus Area: Information Security
Description	
Design the management system for enterprise I&T based on enterprise goals and other design factors. Based on this design, implement all required components of the management system.	
Purpose	
Implement a consistent management approach for enterprise governance requirements to be met, covering governance components such as management processes; organizational structures; roles and responsibilities; reliable and repeatable activities; information items; policies and procedures; skills and competencies; culture and behavior; and services, infrastructure and applications.	
Information Security Focus Area Relevance	
Information security is an integral component of the I&T management framework.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
APO01.01 Design the management system for enterprise I&T. Design a management system tailored to the needs of the enterprise. Management needs of the enterprise are defined through the use of the goals cascade and by application of design factors. Ensure the governance components are integrated and aligned with the enterprise's governance and management philosophy and operating style.	a. Percent of information strategy portfolio activities that are aligned to business strategy b. Level of stakeholder satisfaction with the alignment of the overall management system to the information security management system
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Align with applicable local, national and international information security standards and codes of practice, and evaluate available information security good practices.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
COSO Enterprise Risk Management, June 2017	7. Strategy and Objective-Setting—Principle 9
ISO/IEC 27001:2013/Cor.2:2015(E)	International standard for establishing, implementing and maintaining a management system (all chapters)
ITIL V3, 2011	Service Strategy, 2.3 Governance and management systems
Management Practice	**Example Information Security-specific Metrics**
APO01.02 Communicate management objectives, direction and decisions made. Communicate awareness and promote understanding of alignment and I&T objectives to stakeholders throughout the enterprise. Communicate at regular intervals on important I&T-related decisions and their impact for the organization.	a. Frequency of communication on management objectives and direction for information security b. Percent of people who have successfully completed the information security awareness program c. Percent of people who have completed required annual information security training d. Percent of people demonstrating improvement in measured information security behaviors
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Define the expectations with regard to information security, including specific organizational ethics and culture.	2
2. Develop an information security awareness program.	3
3. Establish metrics to measure behaviors regarding information security.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this practice	
Management Practice	**Example Information Security-specific Metrics**
APO01.03 Implement management processes (to support the achievement of governance and management objectives). Define target process capability levels and implementation priority based on the management system design.	a. Current-state process capability level b. Target-state process capability level, one year out c. Current-state maturity level d. Target-state maturity level, one year out
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO01.04 Define and implement the organizational structures. Put in place the required internal and extended organizational structures (e.g., committees) per the management system design, enabling effective and efficient decision making. Ensure that required technology and information knowledge is included in the composition of management structures.	a. Degree to which executives agree that the information security-related organization is aligned with enterprise business goals
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Align the information security-related organization with enterprise architecture organizational models.	3
2. Establish an information security steering committee (ISSC) (or equivalent).	
3. Define the information security function, including internal and external roles, capabilities, and decision rights required.	
4. Define the information security function, including reporting responsibilities required.	
5. Define the first-line operational role and the second-line control functions in the enterprise to better segregate oversight roles.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this practice	
Management Practice	**Example Information Security-specific Metrics**
APO01.05 Establish roles and responsibilities. Define and communicate roles and responsibilities for enterprise I&T, including authority levels, responsibilities and accountability.	a. Number of IS roles with responsibilities defined in the IS management RACI chart
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Establish, agree on and communicate the roles of security leadership (e.g., CISO and ISM or equivalents).	2
2. Determine the degree to which other organizational roles have information security obligations, and add these obligations to the relevant job descriptions.	
3. Identify training required based on roles.	3
4. Establish, agree on and communicate the roles and responsibilities of the board of directors.	4
5. Determine the reporting relationship of the CISO in the enterprise.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this practice	
Management Practice	**Example Information Security-specific Metrics**
APO01.06 Optimize the placement of the IT function. Position the IT capabilities in the overall organizational structure to reflect the strategic importance and operational dependency of IT within the enterprise. The reporting line of the CIO and representation of IT within senior management should be commensurate with the importance of I&T within the enterprise.	a. Stakeholder satisfaction with placement of the information security functions
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Define the information security function and all relevant activities and attributes.	2
2. Define the placement of the information security function in the enterprise and obtain agreement from all relevant parties.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 27002:2013/Cor.2:2015(E)	8.2 Information classification

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO01.07 Define information (data) and system ownership. Define and maintain responsibilities for ownership of information (data) and information systems. Ensure that owners classify information and systems and protect them in line with their classification.	a. Percent of information systems with defined owners
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Assign information security data custodians to all data assets within the information security management processes.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this practice	
Management Practice	**Example Information Security-specific Metrics**
APO01.08 Define target skills and competencies. Define the required skills and competencies to achieve relevant management objectives.	a. Percent of staff who have attended training to mitigate an information security knowledge or skills requirement gap b. Number of information security staff with targeted skills certifications
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this practice	
Management Practice	**Example Information Security-specific Metrics**
APO01.09 Define and communicate policies and procedures. Put in place procedures to maintain compliance with and performance measurement of policies and other components of the control framework. Enforce the consequences of noncompliance or inadequate performance. Track trends and performance and consider these in the future design and improvement of the control framework.	a. Number of regular internal or third-party assessments completed to determine compliance with information security policies and procedures b. Number of information security policies c. Number of information security controls d. Number of information security deficiencies identified by external auditors e. Business impact due to heightened information security awareness
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Develop information security and related policies, taking into account business and legal or regulatory requirements and contractual security obligations, high-level organizational policies, and the enterprise's internal environment.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this practice	
Management Practice	**Example Information Security-specific Metrics**
APO01.10 Define and implement infrastructure, services and applications to support the governance and management system. Define and implement infrastructure, services and applications to support the governance and management system (e.g., architecture repositories, risk management system, project management tools, cost-tracking tools and incident monitoring tools).	a. Percent of critical systems, infrastructure tools and applications adequately secured b. Number of critical systems, infrastructure tools and applications that have undergone a risk assessment c. Number of critical systems, infrastructure tools and applications without risk treatment d. Number of critical systems requiring risk acceptance by the business e. Frequency of architecture review of infrastructure, services and applications supporting information security
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Identify, review and implement adequately secured and configured systems, tools and applications in line with information security requirements and architecture.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO01.11 Manage continual improvement of the I&T management system. Continually improve processes and other management system components to ensure that they can deliver against governance and management objectives. Consider COBIT implementation guidance, emerging standards, compliance requirements, automation opportunities and the feedback of stakeholders.	a. Frequency of information security assessment for continual improvement of the I&T management system b. Number of information security weaknesses identified in reports, but not mitigated c. Number of active improvement projects related to information security

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Identify information security-critical processes, tools and capabilities based on conformance to specification, related risk and potential costs. Assess capability and identify improvement targets.	4
2. Analyze gaps in capability and control. Identify options for improving or redesigning the process in line with information security requirements.	
3. Review reports (such as audit reports or risk assessments) detailing information security control and process weaknesses.	
4. Consider ways to improve the efficiency and effectiveness of the information security function, such as training information security staff; documenting processes, technology and applications; and standardizing and automating processes.	5

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ITIL V3, 2011	Continual Service Improvement, 4.1 The 7-Step Improvement Process

C. Component: Information Flows and Items

Management Practice	Information Security-specific Inputs		Information Security-specific Outputs	
	From	Description	Description	To
APO01.01 Design the management system for enterprise I&T.	ISFA EDM01.01	Information security guiding principles	Information security and related policies	ISFA EDM03.03 ISFA APO07.01 ISFA APO07.06 ISFA APO12.01 ISFA BAI01.01 ISFA BAI02.01 ISFA BAI03.08 ISFA BAI05.01 ISFA BAI06.01 ISFA BAI11.07 ISFA DSS01.02 ISFA DSS02.01 ISFA MEA01.01 ISFA MEA02.01
	Outside COBIT	Information security-related rules and regulations		
	Outside COBIT	Information security standards and guidelines		
APO01.02 Communicate management objectives, direction and decisions made.	ISFA APO02.06	Communication on information security objectives	Information security training and awareness program	ISFA APO02.06
	ISFA DSS05.01	Malicious software prevention policy		
	ISFA DSS05.02	Connectivity security policy		
	ISFA DSS05.03	Security policies for endpoint devices		
	ISFA EDM01.01	Information security guiding principles		
APO01.03 Implement management processes (to support the achievement of governance and management objectives).	There are no information security-specific inputs or outputs for this practice.			

C. Component: Information Flows and Items *(cont.)*				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO01.04 Define and implement the organizational structures.	ISFA EDM01.01	Information security guiding principles	ISSC mandate and structure	Internal
	Outside COBIT	IT strategy		
	Outside COBIT	Information security standards and guidelines		
APO01.05 Establish roles and responsibilities.	ISFA APO13.01	Information security management system (ISMS) scope statement	Chief information security officer (CISO) and information security manager (ISM) job definitions	Internal
	Outside COBIT	Applicable regulations	Definition of IT-related roles and responsibilities	ISFA DSS05.04
	Outside COBIT	Human resources (HR) and legal policies		
	Outside COBIT	Information security standards and guidelines		
APO01.06 Optimize the placement of the IT function.	There are no information security-specific inputs for this practice.		Information security function definition and placement in the enterprise	ISFA APO01.07
APO01.07 Define information (data) and system ownership.	ISFA APO01.06	Information security function definition and placement in the enterprise	Information security roles and responsibilities	ISFA APO11.01
			Data classification guidelines	ISFA DSS05.02
APO01.08 Define target skills and competencies.	There are no information security-specific inputs for this practice.		Information security compliance assessment	ISFA APO02.02 ISFA APO12.01
APO01.09 Define and communicate policies and procedures.	ISFA APO02.05	Information security strategy	There are no information security-specific outputs for this practice.	
	ISFA APO02.06	Information security plan/program		
	Outside COBIT	Organizational objectives		
	Outside COBIT	Information security related rules and regulations		
	Outside COBIT	Information security standards and guidelines		
APO01.10 Define and implement infrastructure, services and applications to support the governance and management system.	There are no information security-specific inputs or outputs for this practice.			

C. Component: Information Flows and Items *(cont.)*				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
APO01.11 Manage continual improvement of the I&T management system.	**From**	**Description**	**Description**	**To**
	ISFA MEA01.04	Information security reports and corrective action plans updated	Documentation of processes, technology and applications, and standardization	Internal
			Training of the information security staff	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this practice				

Domain: Align, Plan and Organize Management Objective: APO02 — Managed Strategy	Focus Area: Information Security
Description	
Provide a holistic view of the current business and I&T environment, the future direction, and the initiatives required to migrate to the desired future environment. Ensure that the desired level of digitization is integral to the future direction and the I&T strategy. Assess the organization's current digital maturity and develop a road map to close the gaps. With the business, rethink internal operations as well as customer-facing activities. Ensure focus on the transformation journey across the organization. Leverage enterprise architecture building blocks, governance components and the organization's ecosystem, including externally provided services and related capabilities, to enable reliable but agile and efficient response to strategic objectives.	
Purpose	
Support the digital transformation strategy of the organization and deliver the desired value through a road map of incremental changes. Use a holistic I&T approach, ensuring that each initiative is clearly connected to an overarching strategy. Enable change in all different aspects of the organization, from channels and processes to data, culture, skills, operating model and incentives.	
Information Security Focus Area Relevance	
The information security strategy is defined, aligned, integrated with and supportive of the overall enterprise and I&T strategies.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
APO02.01 Understand enterprise context and direction. Understand the enterprise context (industry drivers, relevant regulations, basis for competition), its current way of working and its ambition level in terms of digitization.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Understand how information security should support overall enterprise objectives and protect stakeholder interests by taking into account the need to manage information risk while meeting legal and regulatory compliance requirements.	2
2. Understand the current enterprise architecture and identify potential information security gaps.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
COSO Enterprise Risk Management, June 2017	7. Strategy and Objective-Setting—Principle 6
Management Practice	**Example Information Security-specific Metrics**
APO02.02 Assess current capabilities, performance and digital maturity of the enterprise. Assess the performance of current I&T services and develop an understanding of current business and I&T capabilities (both internal and external). Assess current digital maturity of the enterprise and its appetite for change.	a. Percent of systems not in conformance with security baseline b. Percent of information security baseline controls for which a policy is approved c. Enterprise stakeholder satisfaction survey feedback on the effectiveness of the information security strategy
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Develop an information security capability baseline.	2
2. Create relevant and clear information security criteria to identify risk and prioritize gaps.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
COSO Enterprise Risk Management, June 2017	7. Strategy and Objective-Setting—Principle 6; 9. Review and Revision—Principle 15
Management Practice	**Example Information Security-specific Metrics**
APO02.03 Define target digital capabilities. Based on the understanding of enterprise context and direction, define the target I&T products and services and required capabilities. Consider reference standards, best practices and validated emerging technologies.	a. Number of information security policies needed b. Number of information security initiatives needed c. Percent of projects in the enterprise and IT project portfolios that involved information security
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that information security requirements are included in the definition of target IT capabilities.	2
2. Define the target state for information security.	
3. Define and agree on the impact of information security requirements on enterprise architecture, acknowledging the relevant stakeholders.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO02.04 Conduct a gap analysis. Identify gaps between current and target environments and describe the high-level changes in the enterprise architecture.	a. Percent of information and technology systems that meet information security benchmarks
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Assess and analyze the current information security posture against industry best practices, standards, regulations and other compliance requirements.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
APO02.05 Define the strategic plan and road map. Develop a holistic digital strategy, in cooperation with relevant stakeholders, and detail a road map that defines the incremental steps required to achieve the goals and objectives. Ensure focus on the transformation journey through the appointment of a person who helps spearhead the digital transformation and drives alignment between business and I&T.	a. Number of items not currently covered in information security policies that should be addressed b. Percent and number of information security initiatives for which a value metric (e.g., ROI) has been calculated c. Percent of information security initiatives completed vs. planned
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Define the information security strategy and align it with IT and business strategies and the enterprise's overall objectives.	3
2. Ensure that the current I&T strategic plan and road map take into account information security requirements.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SG2.1 Information Security Strategy
ITIL V3, 2011	Service Strategy, 4.1 Strategy management for IT services
Management Practice	**Example Information Security-specific Metrics**
APO02.06 Communicate the I&T strategy and direction. Create awareness and understanding of the business and I&T objectives and direction, as captured in the I&T strategy, through communication to appropriate stakeholders and users throughout the enterprise.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Promote the information security function.	2
2. Develop the information security plan/program, outlining the practical consequences of information security for the enterprise.	3
3. Communicate the information security strategy and information security plan/program to the enterprise and all relevant stakeholders.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO02.01 Understand enterprise context and direction.	ISFA EDM01.01	Information security guiding principles	High-level sources and priorities for changes	ISFA APO02.02
	ISFA APO13.03	Information security review report		

C. Component: Information Flows and Items *(cont.)*				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO02.02 Assess current capabilities, performance and digital maturity of the enterprise.	ISFA APO01.09	Information security compliance assessment	Information security capabilities	ISFA APO02.03 ISFA APO04.04 ISFA APO08.05 ISFA APO09.05 ISFA APO11.01 ISFA BAI01.01 ISFA BAI02.01 ISFA BAI04.01 ISFA BAI11.01
	ISFA APO02.01	High-level sources and priorities for changes		
	ISFA DSS05.01	Information security management reports		
APO02.03 Define target digital capabilities.	ISFA APO02.02	Information security capabilities	Information security requirements in target IT capabilities	ISFA APO02.04
	ISFA BAI02.01	Information security requirements		
	ISFA DSS05.01	Information security management reports		
	Outside COBIT	Information security standards and regulations		
APO02.04 Conduct a gap analysis.	ISFA APO02.03	Information security requirements in target IT capabilities	Information security capability benchmark	ISFA APO03.01
			Gaps to be closed and changes required to realize target capability	ISFA APO13.02
APO02.05 Define the strategic plan and road map.	ISFA EDM01.01	Information security guiding principles	Information security strategic road map	ISFA BAI05.04
	ISFA APO13.02	Information security business cases	Information security strategy	ISFA EDM01.02 ISFA APO01.08 ISFA APO03.01 ISFA APO13.01
APO02.06 Communicate the I&T strategy and direction.	ISFA APO01.02	Information security training and awareness program	Communication on information security objectives	ISFA APO01.02
			Information security plan/program	ISFA APO01.08 ISFA APO04.04 ISFA APO04.05 ISFA APO07.01 ISFA APO07.05 ISFA APO07.06 ISFA APO09.05 ISFA APO11.01 ISFA APO13.01 ISFA BAI01.01 ISFA BAI01.04 ISFA BAI01.08 ISFA BAI02.01 ISFA BAI05.03 ISFA BAI05.04 ISFA BAI11.01 ISFA BAI11.07
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
ITIL V3, 2011		Service strategy, 3.9 Service strategy inputs and outputs		

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO03 — Managed Enterprise Architecture	Focus Area: Information Security
Description	
Establish a common architecture consisting of business process, information, data, application and technology architecture layers. Create key models and practices that describe the baseline and target architectures, in line with the enterprise and I&T strategy. Define requirements for taxonomy, standards, guidelines, procedures, templates and tools, and provide a linkage for these components. Improve alignment, increase agility, improve quality of information and generate potential cost savings through initiatives such as re-use of building block components.	
Purpose	
Represent the different building blocks that make up the enterprise and its interrelationships as well as the principles guiding their design and evolution over time, to enable a standard, responsive and efficient delivery of operational and strategic objectives.	
Information Security Focus Area Relevance	
The information security architecture is defined, aligned and integrated with the enterprise architecture and principles.	

A. Component: Process		
Management Practice	**Example Information Security-specific Metrics**	
APO03.01 Develop the enterprise architecture vision. The architecture vision provides a first-cut, high-level description of the baseline and target architectures, covering the business, information, data, application and technology domains. The architecture vision provides the sponsor with a key tool to sell the benefits of the proposed capabilities to stakeholders within the enterprise. The architecture vision describes how the new capabilities (in line with I&T strategy and objectives) will meet enterprise goals and strategic objectives and address stakeholder concerns when implemented.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. Define information security objectives and requirements for the enterprise architecture.		2
2. Consider industry best practices in building the information security architecture vision.		3
3. Ensure inclusion of information security requirements when analyzing gaps and selecting solutions for the enterprise.		
4. Define the information security goals and metrics.		4
5. Incorporate defense-in-depth strategies in the enterprise security architecture.		
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-7)	
The Open Group Standard TOGAF version 9.2, 2018	6. Phase A: Architecture Vision	
Management Practice	**Example Information Security-specific Metrics**	
APO03.02 Define reference architecture. The reference architecture describes the current and target architectures for the business, information, data, application and technology domains.	a. Number of deviations between information security architecture and enterprise architecture	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. Maintain the architecture repository containing information security-related standards, reusable components, modeling artifacts, relationships, dependencies and views to enable uniformity of architectural organization and maintenance.		3
2. Ensure inclusion of information security artifacts, policies and standards in the architecture repository.		
3. Ensure that information security is integrated across all architectural domains (e.g., business, information, data, applications, technology).		

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Platform and Architecture—Architectural Approach; Platform and Architecture—Data Integration
ITIL V3, 2011	Service Strategy, 5.4 IT service strategy and enterprise architecture
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 9)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-8)
The Open Group Standard TOGAF version 9.2, 2018	7. Phase B: Business Architecture; 8. Phase C: Information Systems Architectures; 9. Phase C: Information Systems Architectures Data Architecture; 10. Phase C: Information Systems Architectures Application Architecture; 11. Phase D: Technology Architecture
Management Practice	**Example Information Security-specific Metrics**
APO03.03 Select opportunities and solutions. Rationalize the gaps between baseline and target architectures, accounting for both business and technical perspectives, and logically group them into project work packages. Integrate the project with any related I&T-enabled investment programs to ensure that the architectural initiatives are aligned with and enable these initiatives as part of overall enterprise change. Make this a collaborative effort with key enterprise stakeholders from business and IT to assess the enterprise's transformation readiness, and identify opportunities, solutions and all implementation constraints.	a. Number of identified security gaps
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure inclusion of information security requirements when analyzing gaps and selecting solutions for the enterprise.	3
2. Provide a detailed inventory of information and physical assets with proper classification, ownership, location, maintenance type, value and criticality.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Platform and Architecture—Architectural Approach; Platform and Architecture—Data Integration
The Open Group Standard TOGAF version 9.2, 2018	12. Phase E: Opportunities and Solutions
Management Practice	**Example Information Security-specific Metrics**
APO03.04 Define architecture implementation. Create a viable implementation and migration plan in alignment with the program and project portfolios. Ensure the plan is closely coordinated to deliver value and that the required resources are available to complete the necessary work.	a. Number of deviations between information security architecture and enterprise architecture b. Date of last review and/or updates to information security controls applied to enterprise's architecture
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Align information security with I&T architecture.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Platform and Architecture—Architectural Approach; Platform and Architecture—Data Integration
The Open Group Standard TOGAF version 9.2, 2018	13. Phase F: Migration Planning

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO03.05 Provide enterprise architecture services. Provide enterprise architecture services within the enterprise that include guidance to and monitoring of implementation projects, formalizing ways of working through architecture contracts, and measuring and communicating architecture's value and compliance monitoring.	a. Percent of projects that use the information security architecture framework and methodology b. Number of information security reviews that do not meet information security requirements c. Number of incidents that the configuration management system (CMS) utilized to properly identify impact and users affected

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Develop and/or adopt information security standards and design patterns for the enterprise architecture.	3
2. Ensure that any technology acquisitions and business-change activities include information security reviews to confirm that information security requirements are met.	4
3. Use the configuration management system (CMS) to assess the impact of an event.	5
4. Leverage the CMS as a proactive approach to prevent events due to misconfigurations.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Platform and Architecture—Architectural Standards
ITIL V3, 2011	Service Design, 3.9 Service Oriented Architecture
The Open Group Standard TOGAF version 9.2, 2018	14. Phase G: Implementation Governance; 15. Phase H: Architecture Change Management

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO03.01 Develop the enterprise architecture vision.	ISFA APO02.04	Information security capability benchmark	Information security architecture vision	Internal
	ISFA APO02.05	Information security strategy	Information security value proposition, goals and metrics	Internal
APO03.02 Define reference architecture.	Outside COBIT	Enterprise architecture	Information security target architecture definition	ISFA APO03.03
			Baseline domain descriptions and architecture definition	ISFA APO13.02
			Information architecture model	ISFA DSS05.03 ISFA DSS05.04 ISFA DSS05.06
APO03.03 Select opportunities and solutions.	ISFA APO03.02	Information security target architecture definition	Information security architecture implementation and migration strategy	ISFA APO03.04
APO03.04 Define architecture implementation.	ISFA APO03.03	Information security architecture implementation and migration strategy	Detailed information security architecture and service implementation plan	Internal
APO03.05 Provide enterprise architecture services.	There are no information security-specific inputs for this practice.		Information security architecture service implementation guidance	ISFA DSS01.01

C. Component: Information Flows and Items *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 9): Inputs and Outputs
The Open Group Standard TOGAF version 9.2, 2018	6. Phase A: Architecture Vision: Inputs and Outputs; 7. Phase B: Business Architecture: Inputs and Outputs; 9. Phase C: Information Systems Architectures Data Architecture: Inputs and Outputs; 10. Information Systems Architectures Application Architecture: Inputs and Outputs; 11. Phase D: Technology Architecture: Inputs and Outputs; 12. Phase E: Opportunities and Solutions: Inputs and Outputs; 13. Phase F: Migration Planning: Inputs and Outputs; 14. Phase G: Implementation Governance: Inputs and Outputs; 15. Phase H: Architecture Change Management: Inputs and Outputs

Domain: Align, Plan and Organize Management Objective: APO04 — Managed Innovation	Focus Area: Information Security
Description	
Maintain an awareness of I&T and related service trends and monitor emerging technology trends. Proactively identify innovation opportunities and plan how to benefit from innovation in relation to business needs and the defined I&T strategy. Analyze what opportunities for business innovation or improvement can be created by emerging technologies, services or I&T-enabled business innovation; through existing established technologies; and by business and IT process innovation. Influence strategic planning and enterprise architecture decisions.	
Purpose	
Achieve competitive advantage, business innovation, improved customer experience, and improved operational effectiveness and efficiency by exploiting I&T developments and emerging technologies.	
Information Security Focus Area Relevance	
Innovative and emerging information security technologies, developments and practices are continuously researched, assessed and adopted.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
APO04.01 Create an environment conducive to innovation. Create an environment that is conducive to innovation, considering methods such as culture, reward, collaboration, technology forums, and mechanisms to promote and capture employee ideas.	a. Percent of budget assigned to information security research and development
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Maintain information security principles and policies in support of innovation while managing information risk.	2
2. Establish connections to research and other security advisory services.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
APO04.02 Maintain an understanding of the enterprise environment. Work with relevant stakeholders to understand their challenges. Maintain an adequate understanding of enterprise strategy, competitive environment and other constraints, so that opportunities enabled by new technologies can be identified.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Maintain an understanding of information security drivers, operations and challenges to identify opportunities and limitations of technological innovation.	2
2. Determine the effects and impact of innovations on technology, the environment and information security.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
APO04.03 Monitor and scan the technology environment. Set up a technology watch process to perform systematic monitoring and scanning of the enterprise's external environment to identify emerging technologies that have the potential to create value (e.g., by realizing the enterprise strategy, optimizing costs, avoiding obsolescence, and better enabling enterprise and I&T processes). Monitor the marketplace, competitive landscape, industry sectors, and legal and regulatory trends to be able to analyze emerging technologies or innovation ideas in the enterprise context.	a. Frequency of scans of the external environment to identify emerging trends in information security
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Perform research and scan the external environment to identify emerging trends in information security.	3
2. Encourage stakeholder feedback on information security innovation.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO04.04 Assess the potential of emerging technologies and innovative ideas. Analyze identified emerging technologies and/or other I&T innovative suggestions to understand their business potential. Work with stakeholders to validate assumptions on the potential of new technologies and innovation.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Evaluate information security implications of identified innovations.	3
2. Assess proof-of-concept activities for innovation initiatives to ensure coverage of information security requirements. Evaluate compliance to these requirements.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
APO04.05 Recommend appropriate further initiatives. Evaluate and monitor the results of proof-of-concept initiatives and, if favorable, generate recommendations for further initiatives. Gain stakeholder support.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Provide information security advice based on the proof-of-concept results of I&T innovation initiatives.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
APO04.06 Monitor the implementation and use of innovation. Monitor the implementation and use of emerging technologies and innovations during adoption, integration and for the full economic life cycle to ensure that the promised benefits are realized and to identify lessons learned.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Measure security benefits and risk during proof-of-concept and other innovation activities.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO04.01 Create an environment conducive to innovation.	ISFA DSS05.01	Information security service catalog	Information security innovation plan	ISFA APO04.06
APO04.02 Maintain an understanding of the enterprise environment.	Outside COBIT	External research	Information security impact assessments of new initiatives	Internal
APO04.03 Monitor and scan the technology environment.	Outside COBIT	External research	Identified emerging trends in information security	ISFA APO08.02
APO04.04 Assess the potential of emerging technologies and innovative ideas.	ISFA APO02.02	Information security capabilities	Information security requirements compliance assessment	ISFA APO04.05
	ISFA APO02.06	Information security plan/program		
	ISFA BAI02.01	Information security requirements		
APO04.05 Recommend appropriate further initiatives.	ISFA APO02.06	Information security plan/program	Information security advice on test results from proof of concept	Internal
	ISFA APO04.04	Information security requirements compliance assessment		
APO04.06 Monitor the implementation and use of innovation.	ISFA APO04.01	Information security innovation plan	Adjusted innovation plans	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this practice				

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO05 — Managed Portfolio	Focus Area: Information Security
Execute the strategic direction set for investments in line with the enterprise architecture vision and I&T road map. Consider the different categories of investments and the resources and funding constraints. Evaluate, prioritize and balance programs and services, managing demand within resource and funding constraints, based on their alignment with strategic objectives, enterprise worth and risk. Move selected programs into the active products or services portfolio for execution. Monitor the performance of the overall portfolio of products and services and programs, proposing adjustments as necessary in response to program, product or service performance or changing enterprise priorities.	
Purpose	
Optimize the performance of the overall portfolio of programs in response to individual program, product and service performance and changing enterprise priorities and demand.	
Information Security Focus Area Relevance	
Information security is integrated with the enterprise portfolio of investments, programs, products and services.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
APO05.01 Determine the availability and sources of funds. Determine potential sources of funds, different funding options and the implications of the funding source on the investment return expectations.	a. Percent of funds dedicated to the development of the information security portfolio b. Number of unfunded security requirements
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Develop the information security target investment mix, taking into account enterprise risk, financial and nonfinancial benefits, and potential return on the initiatives.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
APO05.02 Evaluate and select programs to fund. Based on requirements for the overall investment portfolio mix and the I&T strategic plan and road map, evaluate and prioritize program business cases and decide on investment proposals. Allocate funds and initiate programs.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 1.2.3 Relationship of project, program, portfolio and operations management
Management Practice	**Example Information Security-specific Metrics**
APO05.03 Monitor, optimize and report on investment portfolio performance. On a regular basis, monitor and optimize the performance of the investment portfolio and individual programs throughout the entire investment life cycle. Ensure continuous follow-up on the alignment of the portfolio with I&T strategy.	a. Percent of information security portfolio activities that are aligned to business strategy
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO05.04 Maintain portfolios. Maintain portfolios of investment programs and projects, I&T products and services, and I&T assets.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Strategy, 4.2 Service portfolio management
Management Practice	**Example Information Security-specific Metrics**
APO05.05 Manage benefits achievement. Monitor the benefits of providing and maintaining appropriate I&T products, services and capabilities, based on the agreed and current business case.	a. Number of changes in the information security risk profile
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Communicate the benefits achieved in the areas of confidentiality, integrity and availability of information.	4
2. Assess changes in the information security risk profile to illustrate realized benefits.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO05.01 Determine the availability and sources of funds.	Outside COBIT	Risk assessment	Information security target investment mix	Internal
			Funding options	ISFA APO05.02
APO05.02 Evaluate and select programs to fund.	ISFA APO05.01	Funding options	Information security program	Internal
APO05.03 Monitor, optimize and report on investment portfolio performance.	There are no information security-specific inputs or outputs for this practice.			
APO05.04 Maintain portfolios.	There are no information security-specific inputs or outputs for this practice.			
APO05.05 Manage benefits achievement.	Outside COBIT	Program budget	Updated information security risk profile	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this practice				

Domain: Align, Plan and Organize Management Objective: APO06 — Managed Budget and Costs	Focus Area: Information Security
Description	
Manage the I&T-related financial activities in both the business and IT functions, covering budget, cost and benefit management and prioritization of spending through the use of formal budgeting practices and a fair and equitable system of allocating costs to the enterprise. Consult stakeholders to identify and control the total costs and benefits within the context of the I&T strategic and tactical plans. Initiate corrective action where needed.	
Purpose	
Foster a partnership between IT and enterprise stakeholders to enable the effective and efficient use of I&T-related resources and provide transparency and accountability of the cost and business value of solutions and services. Enable the enterprise to make informed decisions regarding the use of I&T solutions and services.	
Information Security Focus Area Relevance	
Information security budgets are prepared, prioritized and maintained, and costs are managed.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
APO06.01 Manage finance and accounting. Establish and maintain a method to manage and account for all I&T-related costs, investments and depreciation as an integral part of enterprise financial systems and accounts. Report using the enterprise's financial measurement systems.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Strategy, 4.3 Financial management for IT services
Management Practice	**Example Information Security-specific Metrics**
APO06.02 Prioritize resource allocation. Implement a decision-making process to prioritize the allocation of resources and establish rules for discretionary investments by individual business units. Include the potential use of external service providers and consider the buy, develop and rent options.	a. Percent of alignment between IT resources and high-priority information security and control initiatives b. Ratio of information security costs, per I&T system, between preventive controls and incident response/recovery measures
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that criteria for prioritization in accordance with the information security risk profile are taken into account when allocating resources.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
APO06.03 Create and maintain budgets. Prepare a budget reflecting investment priorities based on the portfolio of I&T-enabled programs and I&T services.	a. Number of additional budget requests due to information security events
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 20000-1:2011(E)	6.4 Budgeting and accounting for services
PMBOK Guide Sixth Edition, 2017	Part 1: 7. Project cost management

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO06.04 Model and allocate costs. Establish and use an I&T costing model based, for example, on the service definition. This approach ensures that allocation of costs for services is identifiable, measurable and predictable, and encourages the responsible use of resources, including those provided by service providers. Regularly review and benchmark the cost/chargeback model to maintain its relevance and appropriateness for evolving business and IT activities.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
APO06.05 Manage costs. Implement a cost management process that compares actual costs against budget. Costs should be monitored and reported. Deviations from budget should be identified in a timely manner and their impact on enterprise processes and services assessed.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Management Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO06.01 Manage finance and accounting.	There are no information security-specific inputs or outputs for this practice.			
APO06.02 Prioritize resource allocation.	There are no information security-specific inputs for this practice.		Initiative prioritization	ISFA APO06.03
APO06.03 Create and maintain budgets.	ISFA APO06.02	Initiative prioritization	Information security budget	Internal ISFA APO13.01 ISFA APO14.01
APO06.04 Model and allocate costs.	There are no information security-specific inputs or outputs for this practice.			
APO06.05 Manage costs.	There are no information security-specific inputs or outputs for this practice.			
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
PMBOK Guide Sixth Edition, 2017	Part 1: 7. Project cost management: Inputs and Outputs			

Domain: Align, Plan and Organize Management Objective: APO07 — Managed Human Resources	Focus Area: Information Security
Description	
Provide a structured approach to ensure optimal recruitment/acquisition, planning, evaluation and development of human resources (both internal and external).	
Purpose	
Optimize human resources capabilities to meet enterprise objectives.	
Information Security Focus Area Relevance	
Qualified information security human resources are competent, skilled, managed and optimized.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
APO07.01 Acquire and maintain adequate and appropriate staffing. Evaluate staffing requirements on a regular basis, or upon major changes to the enterprise, operational or IT environments, to ensure that the enterprise has sufficient human resources to support enterprise goals and objectives. Staffing includes both internal and external resources.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that information security requirements are incorporated into the HR staffing and/or recruitment process for employees, contractors and vendors.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
COSO Enterprise Risk Management, June 2017	6. Governance and Culture—Principle 5
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Acquire
Management Practice	**Example Information Security-specific Metrics**
APO07.02 Identify key IT personnel. Identify key IT personnel. Use knowledge capture (documentation), knowledge sharing, succession planning and staff backup to minimize reliance on a single individual performing a critical job function.	a. Number of key security personnel without a succession plan
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure segregation of duties (SoD) in critical positions.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	RI.RR Identification of Roles and Responsibilities
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Acquire
Management Practice	**Example Information Security-specific Metrics**
APO07.03 Maintain the skills and competencies of personnel. Define and manage the skills and competencies required of personnel. Regularly verify that personnel have the competencies to fulfill their roles on the basis of their education, training and/or experience. Verify that these competencies are being maintained, using qualification and certification programs where appropriate. Provide employees with ongoing learning and opportunities to maintain their knowledge, skills and competencies at a level required to achieve enterprise goals.	a. Qualification of staff in terms of certifications, education and years of experience
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Obtain formal agreement from staff on information security policies and requirements.	2
2. Provide professional development training and programs on information security.	
3. Use credentialing to augment a quality information security professional skill set.	3
4. Establish appropriate enterprisewide education, training and awareness programs for information security.	

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	PM2.3 Security Education/Training
ISO/IEC 27001:2013/Cor.2:2015(E)	7.2 Competence
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity V1.1, April 2018	PR.AT Awareness and Training
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.2 Awareness and training (AT-3, AT-4)
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Deploy
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 17: Security Skills Assessment and Appropriate Training to Fill Gaps
Management Practice	**Example Information Security-specific Metrics**
APO07.04 Assess and recognize/reward employee job performance. Conduct timely, regular performance evaluations against individual objectives derived from enterprise goals, established standards, specific job responsibilities, and the skills and competency framework. Implement a remuneration/recognition process that rewards successful attainment of performance goals.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Incorporate information security criteria in the personnel evaluation process.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Develop
Management Practice	**Example Information Security-specific Metrics**
APO07.05 Plan and track the usage of IT and business human resources. Understand and track the current and future demand for business and IT human resources with responsibilities for enterprise I&T. Identify shortfalls and provide input into sourcing plans, enterprise and IT recruitment processes, and business and IT recruitment processes.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Assess; Reward
Management Practice	**Example Information Security-specific Metrics**
APO07.06 Manage contract staff. Ensure that consultants and contract personnel who support the enterprise with I&T skills know and comply with the organization's policies and meet agreed contractual requirements.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Obtain formal agreement from contract staff on information security policies and requirements.	2
2. Establish formal policies and procedures for contract staff.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
Skills Framework for the Information Age V6, 2015	SFIA and skills management—Deploy

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO07.01 Acquire and maintain adequate and appropriate staffing.	ISFA APO01.01	Information security and related policies	Information security requirements for the staffing process	Internal
	ISFA APO02.06	Information security plan/program		
	Outside COBIT	Local regulations		
APO07.02 Identify key IT personnel.	Outside COBIT	List of internal and external regulations affecting vacation and other personnel rights and obligations	Emergency contact lists	Internal
	Outside COBIT	Business impact analysis (BIA) of business processes	Succession plans	Internal
	Outside COBIT	List of internal and external regulations affecting segregation of duties, HR or security personnel policies		
	Outside COBIT	List of business functions and roles and their accountabilities and responsibilities relative to business processes		
APO07.03 Maintain the skills and competencies of personnel.	Outside COBIT	Personnel lists	Information security awareness training	Internal
	Outside COBIT	List of contractors	Information security training plan	ISFA APO07.04
	Outside COBIT	Personnel skills		
APO07.04 Assess and recognize/reward employee job performance.	ISFA APO07.03	Information security training plan	Personnel information security evaluations	Internal
	ISFA MEA01.02	Agreed-on information security metrics and targets		
	Outside COBIT	HR policy		
APO07.05 Plan and track the usage of IT and business human resources.	ISFA APO02.06	Information security plan/program	Resource performance-tracking plan and indicators	Internal
	Outside COBIT	Process resource requirements	Resource allocation plan	Internal
	Outside COBIT	Personnel lists		
	Outside COBIT	Personnel skills		
APO07.06 Manage contract staff.	ISFA APO01.01	Information security and related policies	Nondisclosure agreements and other policies signed by other parties	Internal
	ISFA APO02.06	Information security plan/program		
	ISFA BAI02.01	Information security requirements		

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 9. Project resource management: Inputs and Outputs

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO08 — Managed Relationships	Focus Area: Information Security
Description	
Manage relationships with business stakeholders in a formalized and transparent way that ensures mutual trust and a combined focus on achieving the strategic goals within the constraints of budgets and risk tolerance. Base relationships on open and transparent communication, a common language, and the willingness to take ownership and accountability for key decisions on both sides. Business and IT must work together to create successful enterprise outcomes in support of the enterprise objectives.	
Purpose	
Enable the right knowledge, skills and behaviors to create improved outcomes, increased confidence, mutual trust and effective use of resources that stimulate a productive relationship with business stakeholders.	
Information Security Focus Area Relevance	
Information security has integral and productive relationships with business stakeholders.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
APO08.01 Understand business expectations. Understand current business issues, objectives and expectations for I&T. Ensure that requirements are understood, managed and communicated, and their status agreed and approved.	a. Percent of business initiatives in which information security is represented
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Understand the business and how information security enables/affects it.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
APO08.02 Align I&T strategy with business expectations and identify opportunities for IT to enhance the business. Align I&T strategies with current business objectives and expectations to enable IT to be a value-add partner for the business and a governance component for enhanced enterprise performance.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Understand information security trends and new technologies and how they can be applied innovatively to enhance business process performance.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Strategy, 4.4 Demand management
Management Practice	**Example Information Security-specific Metrics**
APO08.03 Manage the business relationship. Manage the relationship between the IT service organization and its business partners. Ensure that relationship roles and responsibilities are defined and assigned, and communication is facilitated.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Establish an approach for influencing key contacts regarding information security.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 20000-1:2011(E)	7.1 Business relationship management
ITIL V3, 2011	Service Strategy, 4.5 Business relationship management

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO08.04 Coordinate and communicate. Work with all relevant stakeholders and coordinate the end-to-end delivery of I&T services and solutions provided to the business.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Establish appropriate communication channels between the information security function and the business.	3
2. Establish appropriate reporting and metrics regarding information security.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
APO08.05 Provide input to the continual improvement of services. Continually improve and evolve I&T-enabled services and service delivery to the enterprise to align with changing enterprise objectives and technology requirements.	a. Inclusion rate of information security initiatives in investment proposals
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Incorporate information security requirements in the continual improvement process.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO08.01 Understand business expectations.	Outside COBIT	Business goals and objectives	Understanding of enterprise business processes	ISFA APO08.02 ISFA APO08.03
APO08.02 Align I&T strategy with business expectations and identify opportunities for IT to enhance the business.	ISFA APO04.03	Identified emerging trends in information security	Information security innovations	ISFA APO08.03
	ISFA APO08.01	Understanding of enterprise business processes		
APO08.03 Manage the business relationship.	ISFA APO08.01	Understanding of enterprise business processes	Strategy to obtain stakeholder commitment	Internal
	ISFA APO08.02	Information security innovations		
	ISFA DSS02.02	Classified and prioritized information security incidents and service requests		
APO08.04 Coordinate and communicate.	Outside COBIT	Enterprise communication plan	Information security communication strategy	Internal
APO08.05 Provide input to the continual improvement of services.	ISFA APO02.02 ISFA BAI02.01	Information security capabilities Information security requirements	Integration of information security in continual improvement process	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this practice				

Domain: Align, Plan and Organize Management Objective: APO09 — Managed Service Agreements	Focus Area: Information Security
Description	
Align I&T-enabled products and services and service levels with enterprise needs and expectations, including identification, specification, design, publishing, agreement, and monitoring of I&T products and services, service levels and performance indicators.	
Purpose	
Ensure that I&T products, services and service levels meet current and future enterprise needs.	
Information Security Focus Area Relevance	
Information security service levels are defined, monitored and managed, and meet the information security needs of the enterprise.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
APO09.01 Identify I&T services. Analyze business requirements and the degree to which I&T-enabled services and service levels support business processes. Discuss and agree with the business on potential services and service levels. Compare potential service levels against the current service portfolio; identify new or changed services or service level options.	a. Percent of service level agreements (SLAs) that include information security goals
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Determine the information security requirements of the identified I&T services.	2
2. Develop a portfolio of information security services.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Strategy, 4.4 Demand management
Management Practice	**Example Information Security-specific Metrics**
APO09.02 Catalog I&T-enabled services. Define and maintain one or more service catalogs for relevant target groups. Publish and maintain live I&T-enabled services in the service catalogs.	a. Frequency of updates to the information security services catalog
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Disseminate an information security service catalog.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Design, 4.2 Service Catalogue Management
Management Practice	**Example Information Security-specific Metrics**
APO09.03 Define and prepare service agreements. Define and prepare service agreements based on options in the service catalogs. Include internal operational agreements.	a. Percent of service level agreements (SLAs) that include information security requirements
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Include information security requirements in all SLAs.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SY2.1 Service Level Agreements
ISO/IEC 20000-1:2011(E)	4.5 Establish and improve the SMS; 6.1 Service level management
ITIL V3, 2011	Service Design, 4.3 Service Level Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-9)

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO09.04 Monitor and report service levels. Monitor service levels, report on achievements and identify trends. Provide the appropriate management information to aid performance management.	a. Number of information security incidents reported b. Information security service request response and completion times c. Completion percentage of planned information security risk mitigation activities d. Effectiveness, availability and coverage percentage of critical information security tools and processes
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Monitor information security effectiveness within service level monitoring.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	09.02 Control Third Party Service Delivery
ISO/IEC 20000-1:2011(E)	6.2 Service reporting
Management Practice	**Example Information Security-specific Metrics**
APO09.05 Review service agreements and contracts. Conduct periodic reviews of the service agreements and revise when needed.	a. Effectiveness of information security, based on customer surveys
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Periodically review information security requirements in SLAs based on updated business needs or trends.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO09.01 Identify I&T services.	ISFA DSS05.01	Information security service catalog	Information security requirements of the identified I&T services	ISFA APO09.02
APO09.02 Catalog I&T-enabled services.	ISFA APO09.01	Information security requirements of the identified I&T services	Information security service catalog	Internal
APO09.03 Define and prepare service agreements.	ISFA BAI03.11	Information security services	Service level agreements (SLAs)	ISFA APO09.04 ISFA DSS05.02 ISFA DSS05.03
			Operating level agreements (OLAs)	ISFA DSS05.03
APO09.04 Monitor and report service levels.	ISFA APO09.03	Service level agreements (SLAs)	Information security service level performance reports	ISFA APO09.05
	ISFA BAI03.11	Information security services		
APO09.05 Review service agreements and contracts.	ISFA APO02.02	Information security capabilities	Updated SLAs	Internal
	ISFA APO02.06	Information security plan/program		
	ISFA APO09.04	Information security service level performance reports		
	ISFA BAI02.01	Information security requirements		
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
PMBOK Guide Sixth Edition, 2017	Part 1: 12. Project procurement management: Inputs and Outputs			

Domain: Align, Plan and Organize Management Objective: APO10 — Managed Vendors	Focus Area: Information Security
Description	
Manage I&T-related products and services provided by all types of vendors to meet enterprise requirements. This includes the search for and selection of vendors, management of relationships, management of contracts, and reviewing and monitoring of vendor performance and vendor ecosystem (including upstream supply chain) for effectiveness and compliance.	
Purpose	
Optimize available I&T capabilities to support the I&T strategy and road map, minimize the risk associated with nonperforming or noncompliant vendors, and ensure competitive pricing.	
Information Security Focus Area Relevance	
Information security risk relating to the enterprise's vendors is identified and appropriately managed.	

A. Component: Process		
Management Practice	**Example Information Security-specific Metrics**	
APO10.01 Identify and evaluate vendor relationships and contracts. Continuously search for and identify vendors and categorize them into type, significance and criticality. Establish criteria to evaluate vendors and contracts. Review the overall portfolio of existing and alternative vendors and contracts.	a. Number of independent security reviews of suppliers b. Percent of suppliers granted an exception to information security requirements	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. Conduct information risk assessments and define the information risk profile.		3
2. Define the supplier relationship and requirements based on the information risk profile.		
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
No related guidance for this management practice		
Management Practice	**Example Information Security-specific Metrics**	
APO10.02 Select vendors. Select suppliers according to a fair and formal practice to ensure a viable best fit based on specified requirements. Requirements should be optimized with input from potential suppliers.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.		N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
No related guidance for this management practice		
Management Practice	**Example Information Security-specific Metrics**	
APO10.03 Manage vendor relationships and contracts. Formalize and manage the supplier relationship for each supplier. Manage, maintain and monitor contracts and service delivery. Ensure that new or changed contracts conform to enterprise standards and legal and regulatory requirements. Deal with contractual disputes.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.		N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
ISO/IEC 20000-1:2011(E)	7.2 Supplier management	
ITIL V3, 2011	Service Design, 4.8 Supplier Management	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO10.04 Manage vendor risk. Identify and manage risk relating to vendors' ability to continually provide secure, efficient and effective service delivery. This also includes the subcontractors or upstream vendors that are relevant in the service delivery of the direct vendor.	a. Number of information security breaches caused by suppliers b. Number of information security events leading to information security incidents c. Frequency of information security incidents with suppliers d. Percent of supplier contracts that include information security requirements
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Periodically reassess supplier risk profiles based on information security needs and requirements.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	RM.MP Manage External Participation
ISF, The Standard of Good Practice for Information Security 2016	SC1.1 External Supplier Management Process
ISO/IEC 27002:2013/Cor.2:2015(E)	15. Supplier relationships
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	ID.SC Supply Chain Risk Management
Management Practice	**Example Information Security-specific Metrics**
APO10.05 Monitor vendor performance and compliance. Periodically review overall vendor performance, compliance to contract requirements and value for money. Address identified issues.	a. Frequency of external compliance assessments completed b. Percent of suppliers meeting agreed information security requirements
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Review vendor information security performance.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO10.01 Identify and evaluate vendor relationships and contracts.	Outside COBIT	Vendor risk analysis	Supplier catalog	ISFA APO10.04 ISFA APO10.05 ISFA BAI03.04
APO10.02 Select vendors.	There are no information security-specific inputs or outputs for this practice.			
APO10.03 Manage vendor relationships and contracts.	There are no information security-specific inputs or outputs for this practice.			
APO10.04 Manage vendor risk.	ISFA APO10.01	Supplier catalog	Updated Vendor Risk Rating	ISFA APO10.05
APO10.05 Monitor vendor performance and compliance.	ISFA APO10.01	Supplier catalog	Supplier compliance monitoring review results	Internal
	ISFA APO10.04	Updated vendor risk rating		
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this practice				

Domain: Align, Plan and Organize Management Objective: APO11 — Managed Quality	Focus Area: Information Security
Description	
Define and communicate quality requirements in all processes, procedures and related enterprise outcomes. Enable controls, ongoing monitoring, and the use of proven practices and standards in continuous improvement and efficiency efforts.	
Purpose	
Ensure consistent delivery of technology solutions and services to meet the quality requirements of the enterprise and satisfy stakeholder needs.	
Information Security Focus Area Relevance	
Information security solutions, services and procedures meet the quality requirements of the enterprise and stakeholders.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
APO11.01 Establish a quality management system (QMS). Establish and maintain a quality management system (QMS) that provides a standard, formal and continuous approach to quality management of information. The QMS should enable technology and business processes to align with business requirements and enterprise quality management.	a. Percent of stakeholders satisfied with quality of information security services, based on surveys
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Integrate information security best practices into the QMS.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 8.1 Plan quality management
Management Practice	**Example Information Security-specific Metrics**
APO11.02 Focus quality management on customers. Focus quality management on customers by determining their requirements and ensuring integration in quality management practices.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Support information security objectives pertaining to customer quality management.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
APO11.03 Manage quality standards, practices and procedures and integrate quality management into key processes and solutions. Identify and maintain standards, procedures and practices for key processes to guide the enterprise in meeting the intent of the agreed quality management standards (QMS). This activity should align with I&T control framework requirements. Consider certification for key processes, organizational units, products or services.	a. Number of services with formal information security plans b. Number of production incidents related to security defects
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Align the information security practices with the QMS.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 8.2 Manage quality

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO11.04 Perform quality monitoring, control and reviews. Monitor the quality of processes and services on an ongoing basis, in line with quality management standards. Define, plan and implement measurements to monitor customer satisfaction with quality as well as the value provided by the quality management system (QMS). The information gathered should be used by the process owner to improve quality.	a. Percent of information security requirements being met b. Number of issues identified while monitoring information security quality metrics
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Define and monitor information security quality metrics and take corrective action where applicable.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 8.3 Control quality
Management Practice	**Example Information Security-specific Metrics**
APO11.05 Maintain continuous improvement. Maintain and regularly communicate an overall quality plan that promotes continuous improvement. The plan should define the need for, and benefits of, continuous improvement. Collect and analyze data about the quality management system (QMS) and improve its effectiveness. Correct nonconformities to prevent recurrence.	a. Timeliness of resolution of information security issues b. Number of corrective practices or actions implemented to remediate security quality issues
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that quality data inform all metrics used to identify, document and communicate the root cause(s) of all information security issues.	4
2. Apply corrective practices to remediate quality issues.	5
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	DE.DP Detection Processes

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO11.01 Establish a quality management system (QMS).	ISFA APO01.07	Information security roles and responsibilities	Relevant information security best practices and standards	ISFA APO11.03
	ISFA APO02.02	Information security capabilities		
	ISFA APO02.06	Information security plan/program		
APO11.02 Focus quality management on customers.	ISFA APO11.03	Information security quality standards	Information security quality SLAs agreed on and contractual clauses where appropriate	ISFA APO11.04
APO11.03 Manage quality standards, practices and procedures and integrate quality management into key processes and solutions.	ISFA APO11.01	Relevant information security best practices and standards	Information security quality standards	ISFA APO11.02 ISFA BAI03.06
APO11.04 Perform quality monitoring, control and reviews.	ISFA APO11.02	Information security quality SLAs agreed on and contractual clauses where appropriate	Information security quality metrics implemented in line with best practices	ISFA APO11.05
APO11.05 Maintain continuous improvement.	ISFA APO11.04	Information security quality metrics implemented in line with best practices	Link to information security incident reporting process	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
PMBOK Guide Sixth Edition, 2017		Part 1: 8. Project quality management: Inputs and Outputs		

Page intentionally left blank

Domain: Align, Plan and Organize Management Objective: APO12 — Managed Risk	Focus Area: Information Security
Description	
Continually identify, assess and reduce I&T-related risk within tolerance levels set by enterprise executive management.	
Purpose	
Integrate the management of I&T-related enterprise risk with overall enterprise risk management (ERM) and balance the costs and benefits of managing I&T-related enterprise risk.	
Information Security Focus Area Relevance	
Information security risk mitigation is an integral part of the enterprise and I&T risk management program.	

A. Component: Process		
Management Practice	**Example Information Security-specific Metrics**	
APO12.01 Collect data. Identify and collect relevant data to enable effective I&T-related risk identification, analysis and reporting.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. Identify and collect relevant data to enable effective information security-related risk identification, analysis and reporting.		3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
CMMI Data Management Maturity Model, 2014	Supporting Processes - Risk Management	
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 10	
ISO/IEC 27005:2011(E)	8.2 Risk identification; 12. Information security risk monitoring and review	
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 7)	
Management Practice	**Example Information Security-specific Metrics**	
APO12.02 Analyze risk. Develop a substantiated view on actual I&T risk, in support of risk decisions.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.		N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
CMMI Data Management Maturity Model, 2014	Supporting Processes—Risk Management	
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 11	
ISF, The Standard of Good Practice for Information Security 2016	IR2.1 Risk Assessment Scope; IR2.2 Business Impact Assessment	
ISO/IEC 27001:2013/Cor.2:2015(E)	8.2 Information security risk assessment	
ISO/IEC 27005:2011(E)	8.3 Risk analysis	
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	ID.RA Risk Assessment	
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.6 Authorization (Task 3)	
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-3)	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO12.03 Maintain a risk profile. Maintain an inventory of known risk and risk attributes, including expected frequency, potential impact and responses. Document related resources, capabilities and current control activities related to risk items.	a. Existence, timeliness and completeness of information security risk profiles b. Number of incidents with appropriately designated risk ratings
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Incorporate information security in the enterprise risk profile.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	RS.DT Define Organizational Risk Tolerance
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 12
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-7)
Management Practice	**Example Information Security-specific Metrics**
APO12.04 Articulate risk. Communicate information on the current state of I&T-related exposures and opportunities in a timely manner to all required stakeholders for appropriate response.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	RS.CR Determine Critical Infrastructure Requirements
COSO Enterprise Risk Management, June 2017	10. Information, Communication, and Reporting—Principle 19
ISO/IEC 27005:2011(E)	11. Information security risk communication and consultation
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	ID.RM Risk Management Strategy
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-32)
Management Practice	**Example Information Security-specific Metrics**
APO12.05 Define a risk management action portfolio. Manage opportunities to reduce risk to an acceptable level as a portfolio.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes—Risk Management
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 14
HITRUST CSF version 9, September 2017	03.01 Risk Management Program

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO12.06 Respond to risk. Respond in a timely manner to materialized risk events with effective measures to limit the magnitude of loss.	a. Percent of I&T risk mitigated
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Apply selected information security mitigation practices.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
COSO Enterprise Risk Management, June 2017	8. Performance—Principle 13
ISF, The Standard of Good Practice for Information Security 2016	IR2.9 Risk Treatment
ISO/IEC 27001:2013/Cor.2:2015(E)	6.1 Action to address risk and opportunities
ISO/IEC 27005:2011(E)	9. Information security risk treatment
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.6 Authorization (Task 4)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-9, PM-31)

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO12.01 Collect data.	ISFA APO01.01	Information security and related policies	Data on information security risk	ISFA APO12.02 ISFA APO12.03 ISFA APO14.01
	ISFA APO01.09	Information security compliance assessment		
	ISFA DSS02.02	Classified and prioritized information security incidents and service requests		
APO12.02 Analyze risk.	ISFA APO12.01	Data on information security risk	Information security risk analysis results	ISFA APO12.03
	ISFA DSS05.01	Evaluation of potential threats	Information security risk scenarios	ISFA APO12.03
APO12.03 Maintain a risk profile.	ISFA APO12.01	Data on information security risk	Information security risk profile	ISFA APO12.04 ISFA APO12.05 ISFA BAI01.11 ISFA BAI02.03 ISFA BAI11.07
	ISFA APO12.02	Information security risk analysis results		
	ISFA APO12.02	Information security risk scenarios		
	ISFA DSS05.01	Evaluation of potential threats		
	ISFA EDM01.01	Information security guiding principles		
APO12.04 Articulate risk.	ISFA APO12.03	Information security risk profiles	Information security risk response strategies	Internal

C. Component: Information Flows and Items *(cont.)*				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO12.05 Define a risk management action portfolio.	ISFA APO12.03	Information security risk profile	Project proposals for reducing information security risk	ISFA APO12.06
			Project proposals for reducing information security risk	ISFA APO13.02
APO12.06 Respond to risk.	ISFA APO12.05	Project proposals for reducing information security risk	Information security risk mitigation practices	Internal

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
COSO Enterprise Risk Management, June 2017	10. Information, Communication, and Reporting—Principle 20
ISF, The Standard of Good Practice for Information Security 2016	IR1.3 Information Risk Assessment—Supporting Material
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 7): Inputs and Outputs; 3.6 Authorization (Task 3, 4): Inputs and Outputs
PMBOK Guide Sixth Edition, 2017	Part 1: 11. Project risk management: Inputs and Outputs

Domain: Align, Plan and Organize Management Objective: APO13 — Managed Security	Focus Area: Information Security
Description	
Define, operate and monitor an information security management system.	
Purpose	
Keep the impact and occurrence of information security incidents within the enterprise's risk appetite levels.	
Information Security Focus Area Relevance	
Impact and frequency of information security incidents do not exceed enterprise risk appetite.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
APO13.01 Establish and maintain an information security management system (ISMS). Establish and maintain an information security management system (ISMS) that provides a standard, formal and continuous approach to information security management, enabling secure technology and business processes that are aligned with business requirements.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	0.01 Information Security Management program
ISO/IEC 20000-1:2011(E)	6.6 Information security management
ITIL V3, 2011	Service Design, 4.7 Information Security Management
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.3 Selection (Task 1); 3.4 Implementation (Task 1)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.17 Risk assessment (RA-2)
Management Practice	**Example Information Security-specific Metrics**
APO13.02 Define and manage an information security and privacy risk treatment plan. Maintain an information security plan that describes how information security risk is to be managed and aligned with enterprise strategy and enterprise architecture. Ensure that recommendations for implementing security improvements are based on approved business cases, implemented as an integral part of services and solutions development, and operated as an integral part of business operation.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO13.03 Monitor and review the information security management system (ISMS). Maintain and regularly communicate the need for, and benefits of, continuous improvement in information security. Collect and analyze data about the information security management system (ISMS), and improve its effectiveness. Correct nonconformities to prevent recurrence.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.3 Selection (Task 3)

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO13.01 Establish and maintain an information security management system (ISMS).	ISFA APO02.05	Information security strategy	There are no information security-specific outputs for this practice. The COBIT 2019 core-model outputs are applicable.	
	ISFA APO02.06	Information security plan/program		
	ISFA APO06.03	Information security budget		
APO13.02 Define and manage an information security risk treatment plan.	ISFA BAI02.01	Information security requirements	There are no information security-specific outputs for this practice. The COBIT 2019 core-model outputs are applicable.	
	ISFA MEA04.08	Audit information security report and recommendations		
APO13.03 Monitor and review the information security management system (ISMS).	There are no information security-specific inputs for this practice. The COBIT 2019 core-model inputs are applicable.		Information security review report	ISFA APO02.01

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.3 Selection (Tasks 1, 3): Inputs and Outputs; 3.4 Implementation (Task 1): Inputs and Outputs

Domain: Align, Plan and Organize Management Objective: APO14 — Managed Data	Focus Area: Information Security
Description	
Achieve and sustain effective management of the enterprise data assets across the data life cycle, from creation through delivery, maintenance and archiving.	
Purpose	
Ensure effective utilization of the critical data assets to achieve enterprise goals and objectives.	
Information Security Focus Area Relevance	
Enterprise data assets are secured and managed in accordance with information security requirements and the associated value and risk to the business.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
APO14.01 Define and communicate the organization's data management strategy and roles and responsibilities. Define how to manage and improve the organization's data assets, in line with enterprise strategy and objectives. Communicate the data management strategy to all stakeholders. Assign roles and responsibilities to ensure that corporate data are managed as critical assets and the data management strategy is implemented and maintained in an effective and sustainable manner.	a. Percent of employees successfully completing information security training b. Percent of data lost c. Percent of sensitive or confidential data improperly handled d. Number of improper downloads based on security policy e. Number of formal communications related to data management (DM) strategy and roles

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Establish appropriate ownership and responsibility for managing information and data privacy to ensure compliance with legal and regulatory requirements and prevent misuse of critical information.	2
2. Provide awareness training on information security relative to the sharing of information.	
3. Ensure that the proper measures for data loss prevention are in place.	3
4. Analyze and plan for data-related risk.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Data Management Strategy - Data Management Strategy; Data Governance—Governance Management
ITIL V3, 2011	Service Design, 5.2 Management of Data and Information
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 13: Data Protection

Management Practice	Example Information Security-specific Metrics
APO14.02 Define and maintain a consistent business glossary. Create, approve, update and promote consistent business terms and definitions to foster shared data usage across the organization.	a. Percent of users with inappropriate data access

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Manage users, privileges and responsibilities to control and secure the integrity of the business glossary.	3
2. Determine stakeholder awareness of and satisfaction with business glossary and terms.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Data Governance - Business Glossary
ISF, The Standard of Good Practice for Information Security 2016	IM1.1 Information Classification and Handling

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO14.03 Establish the processes and infrastructure for metadata management. Establish the processes and infrastructure for specifying and extending metadata about the organization's data assets, fostering and supporting data sharing, ensuring compliant use of data, improving responsiveness to business changes and reducing data-related risk.	a. Number of unauthorized access attempts
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Secure metadata at rest or in transit using proper encryption techniques, database isolation and access control lists.	3
2. Ensure that information security-related metadata (e.g., classification) are complete and accurate.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Governance—Metadata Management
ISO/IEC 27002:2013/Cor.2:2015(E)	8.2 Information classification
Management Practice	**Example Information Security-specific Metrics**
APO14.04 Define a data quality strategy. Define an integrated, organizationwide strategy to achieve and maintain the level of data quality (such as complexity, integrity, accuracy, completeness, validity, traceability and timeliness) required to support the business goals and objectives.	a. Percent of unencrypted data leaving the network b. Number of mobile devices, portable drives and systems holding sensitive information but lacking encryption software
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Encrypt sensitive information against loss, theft and corruption from internal and external actors.	3
2. Enable approved encryption software to endpoint devices.	
3. Establish an information classification scheme based on the confidentiality, integrity and availability of the information to ensure appropriate level(s) of data protection.	
4. Determine stakeholder satisfaction with data management and data quality strategies.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	DP.DR Safeguard Data at Rest; DP.DT Safeguard Data in Transit; DP.IP Integrity and Data Leak Prevention
CMMI Data Management Maturity Model, 2014	Data Quality - Data Quality Strategy
Management Practice	**Example Information Security-specific Metrics**
APO14.05 Establish data profiling methodologies, processes and tools. Implement standardized data profiling methodologies, processes, practices, tools and templates that can be applied across multiple data repositories and data stores.	a. Percent of data scanned b. Percent of data confirmed to comply with security policies
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Design and implement processes to evaluate identified data against security requirements.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Quality—Data Profiling
National Institute of Standards and Technology Special Publication 800-53, Revision 5, August 2017	3.20 System and information integrity (SI-1)

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
APO14.06 Ensure a data quality assessment approach. Provide a systematic approach to measure and evaluate data quality according to processes and techniques, and against data quality rules.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that data needed for security processes (e.g., asset inventory, data classification, configuration management system [CMS]) are of sufficient quality.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Quality—Data Quality Assessment
Management Practice	**Example Information Security-specific Metrics**
APO14.07 Define the data cleansing approach. Define the mechanisms, rules, processes, and methods to validate and correct data according to predefined business rules.	a. Number of defined data-cleansing approaches for predefined business rules
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Incorporate information security-related regulations, standards, best practices and techniques into data-cleansing policy.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Quality—Data Cleansing
Management Practice	**Example Information Security-specific Metrics**
APO14.08 Manage the life cycle of data assets. Ensure that the organization understands, maps, inventories and controls its data flows through business processes over the data life cycle, from creation or acquisition to retirement.	a. Percent of data that are secure during their life cycle b. Percent of data not in conformance with data management strategy and applicable laws and regulations
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Incorporate information security considerations into the enterprise information life cycle.	2
2. Ensure systematic and structured security of information and data, both in digital and physical form, in accordance with legal and regulatory requirements to preserve confidentiality, integrity and availability.	3
3. Communicate securely to maintain confidentiality, integrity and authenticity of data during their life cycle, whenever feasible.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Data Operations—Data Lifecycle Management
Management Practice	**Example Information Security-specific Metrics**
APO14.09 Support data archiving and retention. Ensure that data maintenance satisfies organizational and regulatory requirements for availability of historical data. Ensure that legal and regulatory requirements for data archiving and retention are met.	a. Stakeholder satisfaction with data archiving and retention
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Secure historical data to comply with legal and regulatory requirements.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Platform and Architecture—Historical Data, Retention and Archiving
Management Practice	**Example Information Security-specific Metrics**
APO14.10 Manage data backup and restore arrangements. Manage availability of critical data to ensure operational continuity.	a. Percent of data backups that follow security guidelines
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 10: Data Recovery Capability

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
APO14.01 Define and communicate the organization's data management strategy and roles and responsibilities.	ISFA APO06.03	Information security budget	Data loss prevention measures	Internal
	ISFA APO12.01	Data on information security risk	Data-related risk analysis	ISFA APO14.04
	ISFA DSS05.02	Evaluation of potential threats		
APO14.02 Define and maintain a consistent business glossary.	ISFA DSS05.02	Approved user access rights	There are no information security-specific outputs for this practice.	
APO14.03 Establish the processes and infrastructure for metadata management.	There are no information security-specific inputs for this practice.		Metadata security guidelines	Internal
APO14.04 Define a data quality strategy.	ISFA APO01.07	Data classification guidelines	There are no information security-specific outputs for this practice.	
	ISFA APO14.01	Data-related risk analysis		
	ISFA BAI08.01	Classification of information sources		
APO14.05 Establish data profiling methodologies, processes and tools.	There are no information security-specific inputs or outputs for this practice.			
APO14.06 Ensure a data quality assessment approach.	There are no information security-specific inputs or outputs for this practice.			
APO14.07 Define the data cleansing approach.	There are no information security-specific inputs or outputs for this practice.			
APO14.08 Manage the life cycle of data assets.	ISFA DSS05.02	Results of penetration tests	There are no information security-specific outputs for this practice.	
APO14.09 Support data archiving and retention.	There are no information security-specific inputs or outputs for this practice.			
APO14.10 Manage data backup and restore arrangements.	There are no information security-specific inputs or outputs for this practice.			
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this practice				

4.3 Build, Acquire and Implement (BAI)

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI01 — Managed Programs	Focus Area: Information Security
Description	
Manage all programs from the investment portfolio in alignment with enterprise strategy and in a coordinated way, based on a standard program management approach. Initiate, plan, control, and execute programs, and monitor expected value from the program.	
Purpose	
Realize desired business value and reduce the risk of unexpected delays, costs and value erosion. To do so, improve communications to and involvement of business and end users, ensure the value and quality of program deliverables and follow up of projects within the programs, and maximize program contribution to the investment portfolio.	
Information Security Focus Area Relevance	
Information security requirements must be considered and incorporated into all I&T and enterprise programs, from inception to implementation.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
BAI01.01 Maintain a standard approach for program management. Maintain a standard approach for program management that enables governance and management review, decision-making and delivery-management activities. These activities should focus consistently on business value and goals (i.e., requirements, risk, costs, schedule and quality targets).	a. Percent of programs that have an information security risk assessment and an information security plan to address the risk b. Percent of I&T programs in which information security and privacy subject matter experts are consulted and involved from inception c. Amount of actual cost divided by total budgeted projects
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Establish a process to ensure that all program-related information gathered or produced as part of the program is secured.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
BAI01.02 Initiate a program. Initiate a program to confirm expected benefits and obtain authorization to proceed. This includes agreeing on program sponsorship, confirming the program mandate through approval of the conceptual business case, appointing program board or committee members, producing the program brief, reviewing and updating the business case, developing a benefits realization plan, and obtaining approval from sponsors to proceed.	a. Percent of I&T security-related initiatives/projects aligned to a business owner b. Percent of information security-related initiatives with assigned accountability c. Number of programs undertaken without information security implications documented in the business case d. Number of process exceptions to the business case e. Percent of information security-related initiatives outsourced to vendors f. Percent of programs that comply with the organizational strategy of the enterprise
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Plan information security activities within the overall program.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
BAI01.03 Manage stakeholder engagement. Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information for all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.	a. Number of complaints from stakeholders after implementation of new information security programs/controls b. Number and percent of information security-focused programs with stakeholders from business c. Level of stakeholder engagement tracked during the life cycle of the project d. Percent of stakeholders providing feedback on whether the project meets their expectations
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 10. Project communications management

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI01.04 Develop and maintain the program plan. Formulate a program to lay the initial groundwork. Position it for successful execution by formalizing the scope of the work and identifying deliverables that will satisfy goals and deliver value. Maintain and update the program plan and business case throughout the full economic life cycle of the program, ensuring alignment with strategic objectives and reflecting the current status and insights gained to date.	a. Frequency of information security program status reviews provided to senior management
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Develop an information security plan/program that identifies the information security environment and controls to be implemented by the program team to protect organizational assets.	3
2. Engage the necessary resource(s), including human resources, infrastructure and funding, to effectively identify and implement information security requirements.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
BAI01.05 Launch and execute the program. Launch and execute the program to acquire and direct the resources needed to accomplish the goals and benefits of the program as defined in the program plan. In accordance with stage-gate or release review criteria, prepare for stage-gate, iteration or release reviews to report progress and make the case for funding up to the following stage-gate or release review.	a. Percent of stakeholder sign-offs for information security stage-gate reviews and remediation plans
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
BAI01.06 Monitor, control and report on the program outcomes. Monitor and control performance against plan throughout the full economic life cycle of the investment, covering solution delivery at the program level and value/outcome at the enterprise level. Report performance to the program steering committee and the sponsors.	a. Percent of information security program planned actions and milestones that are delivered in status reviews
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
BAI01.07 Manage program quality. Prepare and execute a quality management plan, processes and practices that align with quality management standards (QMS). Describe the approach to program quality and implementation. The plan should be formally reviewed and agreed on by all parties concerned and incorporated into the integrated program plan.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI01.08 Manage program risk. Eliminate or minimize specific risk associated with programs through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events with the potential to cause unwanted change. Define and record any risk faced by program management.	a. Percent information security objectives integrated into IT and business program management b. Percent of unmanaged information security risk c. Number of outstanding information security items in the risk log d. Number of outstanding information security items in the risk log that have exceeded their planned completion milestones e. Percent of unapproved risk exceptions/risk acceptances for the program f. Percent of risk issues without target dates for remediation

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Integrate information security into enterprise program management.	3
2. Establish an information security risk log and remediation actions for all identified risk. Periodically review and update the risk log.	
3. Define criteria for required information security engagement (e.g., processing of sensitive data or third-party access to data).	
4. Establish a process to enable the information security function to monitor ongoing programs and initiate self-engagement.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

Management Practice	Example Information Security-specific Metrics
BAI01.09 Close a program. Remove the program from the active investment portfolio when there is agreement that the desired value has been achieved or when it is clear it will not be achieved within the value criteria set for the program.	a. Percent of program data not in conformance with data destruction or retention policies or procedures

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Ensure that IS-related program information is appropriately destroyed or archived.	2
2. Ensure that program-related equipment and technology, if no longer needed, are disposed of securely (e.g., prototypes, hard drives, etc.).	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	RS.IM Improvements

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
BAI01.01 Maintain a standard approach for program management.	ISFA APO01.01	Information security and related policies	Information security requirements in the feasibility study	ISFA BAI01.02 ISFA BAI02.02 ISFA BAI03.01
	ISFA APO02.02	Information security capabilities		
	ISFA APO02.06	Information security plan/program		
	ISFA APO12.03	Information security risk profile		
	ISFA BAI02.01	Information security requirements		
BAI01.02 Initiate a program.	ISFA BAI01.01	Information security requirements in the feasibility study	Program concept business case including mandatory information security activities	ISFA BAI01.04 ISFA BAI01.08
BAI01.03 Manage stakeholder engagement.	There are no information security-specific inputs or outputs for this practice.			
BAI01.04 Develop and maintain the program plan.	ISFA APO02.06	Information security plan/program	Program concept plan including mandatory information security activities	ISFA BAI01.08
	ISFA BAI01.02	Program concept business case including mandatory information security activities		
BAI01.05 Launch and execute the program.	There are no information security-specific inputs or outputs for this practice.			
BAI01.06 Monitor, control and report on the program outcomes.	There are no information security-specific inputs or outputs for this practice.			
BAI01.07 Manage program quality.	There are no information security-specific inputs or outputs for this practice.			
BAI01.08 Manage program risk.	ISFA APO02.06	Information security plan/program	There are no information security-specific outputs for this practice.	
	ISFA BAI01.02	Program concept business case including mandatory information security activities	There are no information security-specific outputs for this practice.	
	ISFA BAI01.04	Program concept plan including mandatory information security activities	There are no information security-specific outputs for this practice.	
BAI01.09 Close a program.	There are no information security-specific inputs or outputs for this practice.			

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
PMBOK Guide Sixth Edition, 2017	Part 1: 4. Project integration management: Inputs and Outputs; Part 1: 6. Project schedule management: Inputs and Outputs; Part 1: 10. Project communications management: Inputs and Outputs; Part 1: 11. Project risk management: Inputs and Outputs

Domain: Build, Acquire and Implement Management Objective: BAI02 — Managed Requirements Definition	Focus Area: Information Security
Description	
Identify solutions and analyze requirements before acquisition or creation to ensure that they align with enterprise strategic requirements covering business processes, applications, information/data, infrastructure and services. Coordinate the review of feasible options with affected stakeholders, including relative costs and benefits, risk analysis, and approval of requirements and proposed solutions.	
Purpose	
Create optimal solutions that meet enterprise needs while minimizing risk.	
Information Security Focus Area Relevance	
All relevant information security business, functional and technical requirements are identified, documented and implemented.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
BAI02.01 Define and maintain business functional and technical requirements. Based on the business case, identify, prioritize, specify and agree on business information, functional, technical and control requirements covering the scope/understanding of all initiatives required to achieve the expected outcomes of the proposed I&T-enabled business solution.	a. Percent of business requirements reworked due to information security requirements b. Percent of new information security requirements added due to business requirements
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Research, define and document information security requirements (i.e., confidentiality requirements, integrity requirements and availability requirements)	2
2. Research and analyze information security requirements with stakeholders, business sponsors and technical implementation personnel.	
3. Ensure that the business functional requirements take into account the need to protect the security of information (e.g., detect and prevent fraud, validate customer identity).	3
4. Ensure that the technical requirements take into account the need to protect the security of information (e.g., data storage and encryption requirements, hardening of servers, architecture design, penetration tests).	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SD2.1 Specifications of Requirements
ISO/IEC 27002:2013/Cor.2:2015(E)	14.1 Security requirements of information systems
ITIL V3, 2011	Service Design, 5.1 Requirements engineering
PMBOK Guide Sixth Edition, 2017	Part 1: 5. Project scope management
Management Practice	**Example Information Security-specific Metrics**
BAI02.02 Perform a feasibility study and formulate alternative solutions. Perform a feasibility study of potential alternative solutions, assess their viability and select the preferred option. If appropriate, implement the selected option as a pilot to determine possible improvements.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that information security requirements are included in the feasibility study.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
BAI02.03 Manage requirements risk. Identify, document, prioritize and mitigate functional, technical and information processing-related risk associated with the enterprise requirements, assumptions and proposed solution.	a. Percent of information security risk identified during the requirements definition (vs. total information security risk, including that identified at later stages)
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Identify the information security controls.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI02.04 Obtain approval of requirements and solutions. Coordinate feedback from affected stakeholders. At predetermined key stages, obtain approval and sign-off from the business sponsor or product owner regarding functional and technical requirements, feasibility studies, risk analyses and recommended solutions.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Validate information security requirements with stakeholders, business sponsors and technical implementation personnel.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
BAI02.01 Define and maintain business functional and technical requirements.	ISFA APO01.01	Information security and related policies	Information security requirements	ISFA APO02.03 ISFA APO04.04 ISFA APO07.06 ISFA APO08.05 ISFA APO09.05 ISFA APO13.02 ISFA BAI01.01 ISFA BAI02.04 ISFA BAI03.01 ISFA BAI03.04 ISFA BAI03.07 ISFA BAI03.09 ISFA BAI04.03 ISFA BAI05.01 ISFA MEA01.01 ISFA MEA03.01
	ISFA APO02.02	Information security capabilities		
	ISFA APO02.06	Information security plan/program		
	ISFA MEA03.01	External information security compliance requirements		
BAI02.02 Perform a feasibility study and formulate alternative solutions.	ISFA BAI01.01	Information security requirements in the feasibility study	Feasibility study report	Internal
BAI02.03 Manage requirements risk.	ISFA APO12.03	Information security risk profile	Risk mitigation actions	Internal
BAI02.04 Obtain approval of requirements and solutions.	ISFA BAI02.01	Information security requirements	Approval of information security requirements	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
PMBOK Guide Sixth Edition, 2017		Part 1: 5. Project management scope: Inputs and Outputs		

Domain: Build, Acquire and Implement Management Objective: BAI03 — Managed Solutions Identification and Build	Focus Area: Information Security
Description	
Establish and maintain identified products and services (technology, business processes and workflows) in line with enterprise requirements covering design, development, procurement/sourcing and partnering with vendors. Manage configuration, test preparation, testing, requirements management and maintenance of business processes, applications, information/data, infrastructure and services.	
Purpose	
Ensure agile and scalable delivery of digital products and services. Establish timely and cost-effective solutions (technology, business processes and workflows) capable of supporting enterprise strategic and operational objectives.	
Information Security Focus Area Relevance	
Information security requirements are identified, tested and embedded in solutions to help support achievement of business strategic and operational objectives.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
BAI03.01 Design high-level solutions. Develop and document high-level designs for the solution in terms of technology, business processes and workflows. Use agreed and appropriate phased or rapid Agile development techniques. Ensure alignment with the I&T strategy and enterprise architecture. Reassess and update the designs when significant issues occur during detailed design or building phases, or as the solution evolves. Apply a user-centric approach; ensure that stakeholders actively participate in the design and approve each version.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Define the information security specifications in line with high-level design.	2
2. Create predefined sets of information security specifications along with suggested solutions for common cases.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SD2.2 System Design
Management Practice	**Example Information Security-specific Metrics**
BAI03.02 Design detailed solution components. Develop, document and elaborate detailed designs progressively. Use agreed and appropriate phased or rapid Agile development techniques, addressing all components (business processes and related automated and manual controls, supporting I&T applications, infrastructure services and technology products, and partners/suppliers). Ensure that the detailed design includes internal and external service level agreements (SLAs) and operational level agreements (OLAs).	a. Number of solution designs revisited due to a lack of information security requirements or change in information security policy
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Integrate information security design into solution components.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SD2.2 System Design

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI03.03 Develop solution components. Develop solution components progressively in a separate environment, in accordance with detailed designs following standards and requirements for development and documentation, quality assurance (QA), and approval. Ensure that all control requirements in the business processes, supporting I&T applications and infrastructure services, services and technology products, and partner/vendor services are addressed.	a. Number of information security coding exceptions in the solution components
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure solution components are properly secured.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SD1.2 System Development Environments
ISO/IEC 27002:2013/Cor.2:2015(E)	14.2 Security in development and support processes
ITIL V3, 2011	Service Strategy, 5.5 IT service strategy and application development
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-3)
Management Practice	**Example Information Security-specific Metrics**
BAI03.04 Procure solution components. Procure solution components, based on the acquisition plan, in accordance with requirements and detailed designs, architecture principles and standards, and the enterprise's overall procurement and contract procedures, QA requirements, and approval standards. Ensure that all legal and contractual requirements are identified and addressed by the vendor.	a. Percent of suppliers that conform to security requirements
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Incorporate information security requirements into procurement planning and acquisition. Perform appropriate information security assessments.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SD2.3 Software Acquisition
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	3.4 Buying Decisions
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-4)
Management Practice	**Example Information Security-specific Metrics**
BAI03.05 Build solutions. Install and configure solutions and integrate with business process activities. During configuration and integration of hardware and infrastructure software, implement control, security, privacy and auditability measures to protect resources and ensure availability and data integrity. Update the product or services catalogue to reflect the new solutions.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Verify that information security requirements are built into the solution.	3
2. Implement controls to ensure security is addressed during the solution build/development.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	10.05 Security in Development & Support Processes
ISF, The Standard of Good Practice for Information Security 2016	SD2.4 System Build

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI03.06 Perform quality assurance (QA). Develop, resource and execute a QA plan aligned with the QMS to obtain the quality specified in the requirements definition and in the enterprise's quality policies and procedures.	a. Number of information security exceptions in the design and implementation
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Verify that the information security features are included in the QA plan.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SD1.3 Quality Assurance
Management Practice	**Example Information Security-specific Metrics**
BAI03.07 Prepare for solution testing. Establish a test plan and required environments to test the individual and integrated solution components. Include the business processes and supporting services, applications and infrastructure.	a. Number of additional tests for information security
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Include information security test cases in test plans.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	AD.DE Safeguard Development Environment
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.10 Maintenance (MA-2, MA-3)
Management Practice	**Example Information Security-specific Metrics**
BAI03.08 Execute solution testing. During development, execute testing continually (including control testing), in accordance with the defined test plan and development practices in the appropriate environment. Engage business process owners and end users in the test team. Identify, log and prioritize errors and issues identified during testing.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Validate that information security features match information security requirements.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	AD.ST Secure Development Testing
ISF, The Standard of Good Practice for Information Security 2016	SD2.5 System Testing; SD2.6 Security Testing
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.18 System and services acquisition (SA-11)
Management Practice	**Example Information Security-specific Metrics**
BAI03.09 Manage changes to requirements. Track the status of individual requirements (including all rejected requirements) throughout the project life cycle. Manage the approval of changes to requirements.	a. Number of approved changes to information security requirements
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Assess any solution change requests against information security-related requirements.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SD2.9 Post-implementation Review

A. Component: Process *(cont.)*		
Management Practice	**Example Information Security-specific Metrics**	
BAI03.10 Maintain solutions. Develop and execute a plan for the maintenance of solution and infrastructure components. Include periodic reviews against business needs and operational requirements.	a. Number of maintenance updates required due to new information security requirements	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. Verify that the solution is properly configured for inclusion in periodic information security reviews (e.g., vulnerability scan, patch monitoring, penetration test, controls testing, configuration review).		4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
ISO/IEC 27002:2013/Cor.2:2015(E)	14.3 Test data	
Management Practice	**Example Information Security-specific Metrics**	
BAI03.11 Define IT products and services and maintain the service portfolio. Define and agree on new or changed IT products or services and service level options. Document new or changed product and service definitions and service level options to be updated in the products and services portfolio.	a. Number of approved changes to service definitions and service level options resulting from approved changes to information security requirements	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. Define information security services in accordance with business needs and compliance/regulatory needs.		3
2. Define information security processes within I&T services.		
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
No related guidance for this management practice		
Management Practice	**Example Information Security-specific Metrics**	
BAI03.12 Design solutions based on the defined development methodology. Design, develop and implement solutions with the appropriate development methodology (i.e., waterfall, Agile or bimodal I&T), in accordance with the overall strategy and requirements.	a. Percent of projects leveraging waterfall, Agile or other project management methodologies	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. Verify that information security requirements definition, monitoring, QA and maintenance processes are applicable to each development methodology used within the enterprise.		4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
ISF, The Standard of Good Practice for Information Security 2016	SD1.1 System Development Methodology	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
BAI03.01 Design high-level solutions.	ISFA BAI01.01	Information security requirements in the feasibility study	Information security specifications in line with high-level design	ISFA BAI03.02
	ISFA BAI02.01	Information security requirements		
BAI03.02 Design detailed solution components.	ISFA BAI03.01	Information security specifications in line with high-level design	Information security design in the solution components	ISFA BAI03.03
BAI03.03 Develop solution components.	ISFA BAI03.02	Information security design in the solution components	Secure coding practices and secure infrastructure libraries	Internal
BAI03.04 Procure solution components.	ISFA APO10.01	Supplier catalog	Information security requirements within the procurement planning	Internal
	ISFA BAI02.01	Information security requirements		
BAI03.05 Build solutions.	There are no information security-specific inputs for this practice.		Secure solutions	Internal
BAI03.06 Perform quality assurance (QA).	ISFA APO11.03	Information security quality standards	Information security quality review results, exceptions and corrections	Internal
BAI03.07 Prepare for solution testing.	ISFA BAI02.01	Information security requirements	Information security test cases	Internal
BAI03.08 Execute solution testing.	ISFA APO01.01	Information security and related policies	Security acceptance report	Internal
BAI03.09 Manage changes to requirements.	ISFA BAI02.01	Information security requirements	Record of all approved and applied change requests	Internal
BAI03.10 Maintain solutions.	There are no information security-specific inputs for this practice.		Updated secure solutions	Internal
BAI03.11 Define IT products and services and maintain the service portfolio.	ISFA DSS05.01	Information security service catalog	Information security services	ISFA APO09.03 ISFA APO09.04
	Outside COBIT	Roles and responsibilities		
	Outside COBIT	Business mission/vision		
	Outside COBIT	Business goals and objectives		
BAI03.12 Design solutions based on the defined development methodology.	There are no information security-specific inputs or outputs for this practice.			
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this practice				

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI04 — Managed Availability and Capacity	Focus Area: Information Security
Description	
Balance current and future needs for availability, performance and capacity with cost-effective service provision. Include assessment of current capabilities, forecasting of future needs based on business requirements, analysis of business impacts, and assessment of risk to plan and implement actions to meet the identified requirements.	
Purpose	
Maintain service availability, efficient management of resources and optimization of system performance through prediction of future performance and capacity requirements.	
Information Security Focus Area Relevance	
Information security requirements are defined, incorporated and optimized in the availability, performance and capacity management plans.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
BAI04.01 Assess current availability, performance and capacity and create a baseline. Assess availability, performance and capacity of services and resources to ensure that cost-justifiable capacity and performance are available to support business needs and deliver against service level agreements (SLAs). Create availability, performance and capacity baselines for future comparison.	a. Percent of information security commitments met
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Identify the technical and procedural information security issues related to availability, performance and capacity.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	DP.CP Capacity Planning
ISF, The Standard of Good Practice for Information Security 2016	SY2.2 Performance and Capacity Management
ISO/IEC 20000-1:2011(E)	6.5 Capacity management
ITIL V3, 2011	Service Design, 4.4 Availability Management; 4.5 Capacity Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.14 Planning (PL-10, PL-11)
Management Practice	**Example Information Security-specific Metrics**
BAI04.02 Assess business impact. Identify important services to the enterprise. Map services and resources to business processes and identify business dependencies. Ensure that the impact of unavailable resources is fully agreed on and accepted by the customer. For vital business functions, ensure that availability requirements can be satisfied per service level agreement (SLA).	a. Percent of availability, performance and capacity incidents per year caused by information security controls
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Assess the information security impact of potential unavailability, underperformance and lack of capacity.	4
2. Assess the business impact of potential unavailability, underperformance and lack of capacity due to introduction of information security controls.	
3. Assess the business impact of potential unavailability, underperformance and lack of capacity due to a potential information security incident.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 20000-1:2011(E)	6.3 Service continuity and availability management

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI04.03 Plan for new or changed service requirements. Plan and prioritize availability, performance and capacity implications of changing business needs and service requirements.	a. Number of information security changes resulting from new or changed service requirements
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Assess the impact of new or changed service requirements on information security.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 20000-1:2011(E)	5. Design and transition of new changed services
Management Practice	**Example Information Security-specific Metrics**
BAI04.04 Monitor and review availability and capacity. Monitor, measure, analyze, report and review availability, performance and capacity. Identify deviations from established baselines. Review trend analysis reports identifying any significant issues and variances. Initiate actions where necessary and ensure that all outstanding issues are addressed.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
BAI04.05 Investigate and address availability, performance and capacity issues. Address deviations by investigating and resolving identified availability, performance and capacity issues.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Assess and investigate any information security issue that impacts availability, performance and capacity.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
BAI04.01 Assess current availability, performance and capacity and create a baseline.	ISFA APO02.02	Information security capabilities	List of technical and procedural information security issues related to availability, performance and capacity	ISFA BAI04.02
BAI04.02 Assess business impact.	ISFA BAI04.01	List of technical and procedural information security issues related to availability, performance and capacity	Availability, performance and capacity information security impact assessments	ISFA BAI04.03
BAI04.03 Plan for new or changed service requirements.	ISFA BAI02.01	Information security requirements	Updates to information security requirements	Internal
	ISFA BAI04.02	Availability, performance and capacity information security impact assessments		
BAI04.04 Monitor and review availability and capacity.	There are no information security-specific inputs or outputs for this practice.			
BAI04.05 Investigate and address availability, performance and capacity issues.	There are no information security-specific inputs for this practice.		Updates to corrective actions to close capacity issues	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this practice				

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI05 — Managed Organizational Change	Focus Area: Information Security
Description	
Maximize the likelihood of successfully implementing sustainable enterprisewide organizational change quickly and with reduced risk. Cover the complete life cycle of the change and all affected stakeholders in the business and IT.	
Purpose	
Prepare and commit stakeholders for business change and reduce the risk of failure.	
Information Security Focus Area Relevance	
An information security culture is created, enabled, driven and maintained through the organizational change processes and programs.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
BAI05.01 Establish the desire to change. Understand the scope and impact of the desired change. Assess stakeholder readiness and willingness to change. Identify actions that will motivate stakeholder acceptance and participation to make the change work successfully.	a. Ratio of information security alerts relative to information security awareness trainings offered or to total training attendance. b. Percent of users appropriately trained for information security changes
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Establish a proactive information security culture.	2
2. Identify current and desired future information security states.	
3. Provide visible leadership through executive (C-level, highest-level) commitment to information security for facilitating change.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PROSCI® 3-Phase Change Management Process	Phase 1. Preparing for change—Define your change management strategy
Management Practice	**Example Information Security-specific Metrics**
BAI05.02 Form an effective implementation team. Establish an effective implementation team by assembling appropriate members, creating trust, and establishing common goals and effectiveness measures.	a. Number of qualified information security professionals on the implementation team b. Percent of identified information security roles filled with a qualified information security professional
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Designate qualified information security professionals to serve on implementation teams.	3
2. Develop a common vision for the information security team.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PROSCI® 3-Phase Change Management Process	Phase 1. Preparing for change—Prepare your change management team
Management Practice	**Example Information Security-specific Metrics**
BAI05.03 Communicate desired vision. Communicate the desired vision for the change in the language of those affected by it. The communication should be made by senior management and include the rationale for, and benefits of, the change; the impacts of not making the change; and the vision, the road map and the involvement required of the various stakeholders.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Communicate the information security vision.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI05.04 Empower role players and identify short-term wins. Empower those with implementation roles by assigning accountability. Provide training and align organizational structures and HR processes. Identify and communicate short-term wins that are important from a change-enablement perspective.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Align information security functions to support the strategy.	2
2. Communicate roles and responsibilities for information security team members.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
BAI05.05 Enable operation and use. Plan and implement all technical, operational and usage aspects so all those who are involved in the future state environment can exercise their responsibility.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Develop and implement an information security operations plan.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PROSCI® 3-Phase Change Management Process	Phase 2. Managing change
Management Practice	**Example Information Security-specific Metrics**
BAI05.06 Embed new approaches. Embed new approaches by tracking implemented changes, assessing the effectiveness of the operation and use plan, and sustaining ongoing awareness through regular communication. Take corrective measures as appropriate (which may include enforcing compliance).	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Monitor and adjust information security-related measures as necessary.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PROSCI® 3-Phase Change Management Process	Phase 3. Reinforcing change
Management Practice	**Example Information Security-specific Metrics**
BAI05.07 Sustain changes. Sustain changes through effective training of new staff, ongoing communication campaigns, continued commitment of top management, monitoring of adoption and sharing of lessons learned across the enterprise.	a. Percent of users who have completed an information security awareness program
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Inform and train staff at periodic intervals based on information security needs.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PROSCI® 3-Phase Change Management Process	Phase 3. Reinforcing change

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
BAI05.01 Establish the desire to change.	ISFA APO01.01	Information security and related policies	Communication plan with senior management	Internal
	ISFA BAI02.01	Information security requirements	Agreed-on change control process aligned with best practice guidance	Internal
BAI05.02 Form an effective implementation team.	Outside COBIT	Personnel skills	Information security implementation teams	Internal
BAI05.03 Communicate desired vision.	ISFA APO02.06	Information security plan/program	Information security vision communication plan	ISFA BAI05.04
	Outside COBIT	Corporate vision/mission statements		
BAI05.04 Empower role players and identify short-term wins.	ISFA APO02.05	Information security strategic road map	List of potential short-term wins	ISFA BAI05.05
	ISFA APO02.06	Information security plan/program		
	ISFA BAI05.03	Information security vision communication plan		
BAI05.05 Enable operation and use.	ISFA BAI05.04	List of potential short-term wins	Practical information security measures	ISFA BAI05.06
BAI05.06 Embed new approaches.	ISFA BAI05.05	Practical information security measures	Information security operational practices	Internal
BAI05.07 Sustain changes.	There are no information security-specific inputs for this practice.		Reviews of operational use	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this practice				

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI06 — Managed IT Changes	Focus Area: Information Security
Description	
Manage all changes in a controlled manner, including standard changes and emergency maintenance relating to business processes, applications and infrastructure. This includes change standards and procedures, impact assessment, prioritization and authorization, emergency changes, tracking, reporting, closure, and documentation.	
Purpose	
Enable fast and reliable delivery of change to the business. Mitigate the risk of negatively impacting the stability or integrity of the changed environment.	
Information Security Focus Area Relevance	
Information security requirements and risk are identified and addressed throughout the change life cycle.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
BAI06.01 Evaluate, prioritize and authorize change requests. Evaluate all requests for change to determine the impact on business processes and I&T services, and to assess whether change will adversely affect the operational environment and introduce unacceptable risk. Ensure that changes are logged, prioritized, categorized, assessed, authorized, planned and scheduled.	a. Number of information security-relevant changes and number of changes that had an information security impact (good or bad) b. Number of information security requirements that have not been met after the change
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that the information security policy adapts to business goals within an enterprise.	2
2. Ensure that changes conform with the information security policy.	
3. Ensure that assessment of the potential impact of changes on information security is undertaken.	3
4. Develop practices to consider the information security impact of emerging trends and technologies.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SY2.4 Change Management
ISO/IEC 20000-1:2011(E)	9.2 Change management
ITIL V3, 2011	Service Transition, 4.2 Change Management
PMBOK Guide Sixth Edition, 2017	Part 1: 4.6 Perform Integrated Change Control
Management Practice	**Example Information Security-specific Metrics**
BAI06.02 Manage emergency changes. Carefully manage emergency changes to minimize further incidents. Ensure the emergency change is controlled and takes place securely. Verify that emergency changes are appropriately assessed and authorized after the change.	a. Number of information security incidents related to emergency changes
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Develop measures that will address emergency changes and maintenance without compromising information security.	3
2. To assure proper follow-up, maintain an information risk register when new risk is introduced in an emergency change.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI06.03 Track and report change status. Maintain a tracking and reporting system to document rejected changes and communicate the status of approved, in-process and complete changes. Make certain that approved changes are implemented as planned.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	IP.CC Apply Change Control
Management Practice	**Example Information Security-specific Metrics**
BAI06.04 Close and document the changes. Whenever changes are implemented, update the solution, user documentation and procedures affected by the change.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
BAI06.01 Evaluate, prioritize and authorize change requests.	ISFA APO01.01	Information security and related policies	Impact assessments	Internal
BAI06.02 Manage emergency changes.	There are no information security-specific inputs for this practice.		Post-implementation information security review of emergency changes	Internal
BAI06.03 Track and report change status.	There are no information security-specific inputs for this practice.		Updated change request status reports	Internal
BAI06.04 Close and document the changes.	There are no information security-specific inputs or outputs for this practice.			
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this practice				

Domain: Build, Acquire and Implement Management Objective: BAI07 — Managed IT Change Acceptance and Transitioning	Focus Area: Information Security
Description	
Formally accept and make operational new solutions. Include implementation planning, system and data conversion, acceptance testing, communication, release preparation, promotion to production of new or changed business processes and I&T services, early production support, and a post-implementation review.	
Purpose	
Implement solutions safely and in line with the agreed expectations and outcomes.	
Information Security Focus Area Relevance	
Changes that impact information security are tested, assessed, approved, implemented and monitored.	

A. Component: Process		
Management Practice	**Example Information Security-specific Metrics**	
BAI07.01 Establish an implementation plan. Establish an implementation plan that covers system and data conversion, acceptance testing criteria, communication, training, release preparation, promotion to production, early production support, a fallback/back-up plan, and a post-implementation review. Obtain approval from relevant parties.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. Include information security aspects in planning.		3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
ITIL V3, 2011	Service Transition, 4.1 Transition Planning and Support	
Management Practice	**Example Information Security-specific Metrics**	
BAI07.02 Plan business process, system and data conversion. Prepare for business process, I&T service data and infrastructure migration as part of the enterprise's development methods. Include audit trails and a recovery plan should the migration fail.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. Ensure security of data during conversion and migration.		3
2. Ensure proper disposal of data not needed after migration.		4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
ITIL V3, 2011	Service Transition, 4.1 Transition Planning and Support	
Management Practice	**Example Information Security-specific Metrics**	
BAI07.03 Plan acceptance tests. Establish a test plan based on enterprisewide standards that define roles, responsibilities, and entry and exit criteria. Ensure that the plan is approved by relevant parties.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. Ensure that information security acceptance criteria are part of the test plan.		3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
No related guidance for this management practice		

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI07.04 Establish a test environment. Define and establish a secure test environment representative of the planned business process and IT operations environment in terms of performance, capacity, security, internal controls, operational practices, data quality, privacy requirements and workloads.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
BAI07.05 Perform acceptance tests. Test changes independently, in accordance with the defined test plan, prior to migration to the live operational environment.	a. Percent of information security testing completed
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Transition, 4.5 Service Validation and Testing
Management Practice	**Example Information Security-specific Metrics**
BAI07.06 Promote to production and manage releases. Promote the accepted solution to the business and operations. Where appropriate, run the solution as a pilot implementation or in parallel with the old solution for a defined period and compare behavior and results. If significant problems occur, revert to the original environment based on the fallback/back-up plan. Manage releases of solution components.	a. Percent of information security changes accepted and included in releases
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Confirm that information security features remain intact during migration to production.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 20000-1:2011(E)	9.3 Release and deployment management
ITIL V3 2011	Service Transition, 4.4 Release and Deployment Management
Management Practice	**Example Information Security-specific Metrics**
BAI07.07 Provide early production support. For an agreed period of time, provide early support to users and I&T operations to resolve issues and help stabilize the new solution.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Provide support to address early release information security-related events.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI07.08 Perform a post-implementation review. Conduct a post-implementation review to confirm outcome and results, identify lessons learned, and develop an action plan. Evaluate actual performance and outcomes of the new or changed service against expected performance and outcomes anticipated by the user or customer.	a. Percent of unresolved information security issues in release
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that information security is included in a post-implementation review.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Transition, 4.6 Change Evaluation

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
BAI07.01 Establish an implementation plan.	Outside COBIT	IT implementation plan	Updated I&T implementation plan	Internal
BAI07.02 Plan business process, system and data conversion.	There are no information security-specific inputs or outputs for this practice.			
BAI07.03 Plan acceptance tests.	Outside COBIT	Test plans	Information security measures within the test environment	Internal
BAI07.04 Establish a test environment.	Outside COBIT	Test data and environment architecture	Secure test environments	Internal
BAI07.05 Perform acceptance tests.	Outside COBIT	Acceptance tests	Updated acceptance tests	Internal
BAI07.06 Promote to production and manage releases.	Outside COBIT	Release plans	Updated release plans	Internal
BAI07.07 Provide early production support.	There are no information security-specific inputs or outputs for this practice.			
BAI07.08 Perform a post-implementation review.	Outside COBIT	Post-implementation review reports	Updated post-implementation review reports	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this practice				

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI08 — Managed Knowledge	Focus Area: Information Security
Description	
Maintain the availability of relevant, current, validated and reliable knowledge and management information to support all process activities and to facilitate decision making related to the governance and management of enterprise I&T. Plan for the identification, gathering, organizing, maintaining, use and retirement of knowledge.	
Purpose	
Provide the knowledge and information required to support all staff in the governance and management of enterprise I&T and allow for informed decision making.	
Information Security Focus Area Relevance	
Information security knowledge and information are created, developed, acquired, controlled, maintained and secured.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
BAI08.01 Identify and classify sources of information for governance and management of I&T. Identify, validate and classify diverse sources of internal and external information required to enable governance and management of I&T, including strategy documents, incident reports and configuration information that progresses from development to operations before going live.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
BAI08.02 Organize and contextualize information into knowledge. Organize information based on classification criteria. Identify and create meaningful relationships among information elements and enable use of information. Identify owners, and leverage and implement enterprise-defined information levels of access to management information and knowledge resources.	a. Percent of information security categories covered b. Percent of data not properly classified
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Map roles to knowledge areas and ensure that proper access control is in place for relevant information.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
COSO Enterprise Risk Management, June 2017	10. Information, Communication, and Reporting - Principle 18
Management Practice	**Example Information Security-specific Metrics**
BAI08.03 Use and share knowledge. Propagate available knowledge resources to relevant stakeholders and communicate how these resources can be used to address different needs (e.g., problem solving, learning, strategic planning and decision making).	a. Number of employees trained in information security
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure the proper measures for data loss prevention (DLP).	3
2. Implement access controls through the use of policies and processes to restrict unauthorized use and sharing of information.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	PP.IS Apply Information Sharing; IR.ES Ensure Information sharing
ITIL V3, 2011	Service Transition, 4.7 Knowledge Management
PMBOK Guide Sixth Edition, 2017	Part 1: 4.4 Manage project knowledge

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI08.04 Evaluate and update or retire information. Measure the use and evaluate the currency and relevance of information. Update information or retire obsolete information.	a. Percent of data securely destroyed b. Percent of data securely archived

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Securely dispose of information. Include deletion of traceability, especially in the case of personally identifiable information (PII), in conformance with relevant and applicable privacy laws and regulations	3
2.Maintain and document a solid/accepted audit trail for information.	
3. Align information security measures relevant to classification.	
4. Develop secure information-destruction policies and processes.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
BAI08.01 Identify and classify sources of information for governance and management of I&T.	There are no information security-specific inputs for this practice.		Updated classification of information sources	Internal ISFA APO14.04
BAI08.02 Organize and contextualize information into knowledge.	There are no information security-specific inputs for this practice.		Published knowledge repositories	Internal
BAI08.03 Use and share knowledge.	There are no information security-specific inputs for this practice.		Updated access control	Internal
BAI08.04 Evaluate and update or retire information.	There are no information security-specific inputs for this practice.		Updated rules for knowledge retirement	Internal

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this practice	

Domain: Build, Acquire and Implement Management Objective: BAI09 — Managed Assets	Focus Area: Information Security
Description	
Manage I&T assets through their life cycle to make sure that their use delivers value at optimal cost, they remain operational (fit for purpose), and they are accounted for and physically protected. Ensure that those assets that are critical to support service capability are reliable and available. Manage software licenses to ensure that the optimal number are acquired, retained and deployed in relation to required business usage, and the software installed is in compliance with license agreements.	
Purpose	
Account for all I&T assets and optimize the value provided by their use.	
Information Security Focus Area Relevance	
All I&T assets are appropriately secured according to their information security requirements.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
BAI09.01 Identify and record current assets. Maintain an up-to-date, accurate record of all I&T assets that are required to deliver services and that are owned or controlled by the organization with an expectation of future benefit (including resources with economic value, such as hardware or software). Ensure alignment with configuration management and financial management.	a. Number of identified unauthorized assets b. Number of undocumented assets discovered through routine security scans c. Frequency of reviews of information security requirements

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Visualize and document enterprise I&T assets to include data flow.	2
2. Identify information security requirements for current assets.	
3. Address information security for I&T assets, data and forms, etc.	3
4. Verify that a comprehensive and accurate asset inventory informs the implementation of security processes (patch management, vulnerability management, etc.).	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	RI.AD Asset Discovery & Identification
ISF, The Standard of Good Practice for Information Security 2016	BA1.1 Business Application Register
ISO/IEC 27002:2013/Cor.2:2015(E)	8.1 Responsibility for assets
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.13 Physical and environmental protection (PE-9)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 1: Inventory of Authorized and Unauthorized Devices; CSC 2: Inventory of Authorized and Unauthorized Software

Management Practice	Example Information Security-specific Metrics
BAI09.02 Manage critical assets. Identify assets that are critical in providing service capability. Maximize their reliability and availability to support business needs.	a. Percent of assets with assigned owners b. Percent of assets with defined security classification in the asset inventory

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Define criticality levels and identify asset criticality in an asset register.	2
2. Enforce information security requirements on assets.	3
3. Include security measures (e.g., data center security reviews) that address third-party access to enterprise I&T facilities for on-site and off-site activities. Ensure appropriate security and privacy conditions, especially in the context of outsourcing.	
4. Ensure that the security classification of data is embedded in the asset inventory.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	ID.AM Asset Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.13 Physical and environmental protection (PE-20)

A. Component: Process *(cont.)*		
Management Practice	**Example Information Security-specific Metrics**	
BAI09.03 Manage the asset life cycle. Manage assets from procurement to disposal. Ensure that assets are utilized as effectively and efficiently as possible and are accounted for and physically protected until appropriately retired.	a. Number of information security-noncompliant assets	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. Identify and communicate the risk of information security noncompliance related to the asset life cycle.		2
2. Ensure that information security measures and requirements are met throughout the asset life cycle.		3
3. Identify end-of-life systems and plan for related information security risk.		4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
CMMI Cybermaturity Platform, 2018	DP.ML Manage Asset Lifecycle	
ISF, The Standard of Good Practice for Information Security 2016	IM2.1 Document Management; PA1.1 Hardware Life Cycle Management	
ITIL V3, 2011	Service Transition, 4.3 Service Asset and Configuration Management	
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	PR.MA Maintenance	
Management Practice	**Example Information Security-specific Metrics**	
BAI09.04 Optimize asset value. Regularly review the overall asset base to identify ways to optimize value in alignment with business needs.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.		N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
No related guidance for this management practice		
Management Practice	**Example Information Security-specific Metrics**	
BAI09.05 Manage licenses. Manage software licenses to maintain the optimal number of licenses and support business requirements. Ensure that the number of licenses owned is sufficient to cover the installed software in use.	a. Percent of unauthorized software discovered during regular network checks	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. Establish a procedure for control of software installations and other I&T assets.		3
2. Perform regular network checks for unauthorized software.		4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
No related guidance for this management practice		

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
BAI09.01 Identify and record current assets.	**From**	**Description**	**Description**	**To**
	Outside COBIT	Asset inventory	Information security requirements for I&T assets	ISFA BAI09.02
			Results of physical inventory checks	ISFA DSS05.03
BAI09.02 Manage critical assets.	ISFA BAI09.01	Information security requirements for I&T assets	Criticality levels for I&T asset	ISFA BAI09.03
BAI09.03 Manage the asset life cycle.	ISFA BAI09.02	Criticality levels for I&T assets	Updated asset management procedures	Internal
BAI09.04 Optimize asset value.	There are no information security-specific inputs or outputs for this practice.			
BAI09.05 Manage licenses.	There are no information security-specific inputs for this practice.		Updated register of software licenses	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this practice				

Page intentionally left blank

Domain: Build, Acquire and Implement Management Objective: BAI10 — Managed Configuration	Focus Area: Information Security
Description	
Define and maintain descriptions and relationships among key resources and capabilities required to deliver I&T-enabled services. Include collecting configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository.	
Purpose	
Provide sufficient information about service assets to enable the service to be effectively managed. Assess the impact of changes and deal with service incidents.	
Information Security Focus Area Relevance	
Information security configurations for I&T assets are defined, applied, verified, monitored and maintained according to the information security requirements.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
BAI10.01 Establish and maintain a configuration model. Establish and maintain a logical model of the services, assets, infrastructure and recording of configuration items (CIs), including the relationships among them. Include the CIs considered necessary to manage services effectively and to provide a single, reliable description of the assets in a service.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Provide the information security-related configuration, settings and system hardening to ensure that the information security posture of a given system is based on a set of requirements or architectural designs.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes - Configuration Management
ISF, The Standard of Good Practice for Information Security 2016	SY1 System Configuration
ISO/IEC 20000-1:2011(E)	9.1 Configuration management
ITIL V3, 2011	Service Transition, 4.3 Service Asset and Configuration Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-6)
Management Practice	**Example Information Security-specific Metrics**
BAI10.02 Establish and maintain a configuration repository and baseline. Establish and maintain a configuration management repository and create controlled configuration baselines.	a. Number of baseline changes needed due to changes in security posture b. Number of discrepancies between standard information security baselines and actual configurations c. Frequency of baseline updates
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Include an information security configuration for configurable items such as servers/hardware, network devices and endpoint devices.	3
2. Identify information security requirements for current assets and take into account the dependencies.	
3. Secure all I&T baselines.	
4. Monitor compliance with established and approved secure configuration baselines and updates.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	IP.CB Apply Configuration Baselines
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.4 Implementation (Task 2)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.19 System and service acquisition (SA-10)

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI10.03 Maintain and control configuration items. Maintain an up-to-date repository of configuration items (CIs) by populating any configuration changes.	a. Percent of changes that would cause a security impact
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-2)
Management Practice	**Example Information Security-specific Metrics**
BAI10.04 Produce status and configuration reports. Define and produce configuration reports on status changes of configuration items.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-3)
Management Practice	**Example Information Security-specific Metrics**
BAI10.05 Verify and review integrity of the configuration repository. Periodically review the configuration repository and verify completeness and correctness against the desired target.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.5 Configuration management (CM-4)

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
BAI10.01 Establish and maintain a configuration model.	There are no information security-specific inputs for this practice.		Information security alerts	Internal
BAI10.02 Establish and maintain a configuration repository and baseline.	Outside COBIT	Information security configuration requirements	Vulnerability assessment report	Internal
BAI10.03 Maintain and control configuration items.	There are no information security-specific inputs for this practice.		Configuration management plan	Internal
BAI10.04 Produce status and configuration reports.	There are no information security-specific inputs or outputs for this practice.			
BAI10.05 Verify and review integrity of the configuration repository.	There are no information security-specific inputs or outputs for this practice.			
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.4 Implementation (Task 2): Inputs and Outputs			

Domain: Build, Acquire and Implement Management objective: BAI11 — Managed Projects	Focus Area: Information Security
Description	
Manage all projects that are initiated within the enterprise in alignment with enterprise strategy and in a coordinated way based on the standard project management approach. Initiate, plan, control and execute projects, and close with a post-implementation review.	
Purpose	
Realize defined project outcomes and reduce the risk of unexpected delays, costs and value erosion by improving communications to and involvement of business and end users. Ensure the value and quality of project deliverables and maximize their contribution to the defined programs and investment portfolio.	
Information Security Focus Area Relevance	
Information security requirements are considered and incorporated into all enterprise projects.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
BAI11.01 Maintain a standard approach for project management. Maintain a standard approach for project management that enables governance and management review, decision-making and delivery-management activities. These activities should focus consistently on business value and goals (i.e., requirements, risk, costs, schedule and quality targets).	a. Percent of projects that have a security risk assessment and an information security plan to address the risk
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Incorporate information security requirements in the feasibility study for each project within programs.	2
2. Establish a process to ensure that all project-related information that is gathered or produced as part of the project is secured.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-2)
Management Practice	**Example Information Security-specific Metrics**
BAI11.02 Start up and initiate a project. Define and document the nature and scope of the project to confirm and develop a common understanding of project scope among stakeholders. The definition should be formally approved by the project sponsors.	a. Number of projects undertaken without security implications documented in the business case
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Plan information security activities for each project.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 4.1 Develop project charter; Part 1: 6. Project schedule management
Management Practice	**Example Information Security-specific Metrics**
BAI11.03 Manage stakeholder engagement. Manage stakeholder engagement to ensure an active exchange of accurate, consistent and timely information that reaches all relevant stakeholders. This includes planning, identifying and engaging stakeholders and managing their expectations.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Develop and communicate sufficient criteria and processes to ensure information security participation as necessary.	2
2. Develop controls to enable the information security function to monitor planned projects and provide the appropriate level of project engagement.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 13. Project stakeholder management Part 1: 10. Project communications management

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI11.04 Develop and maintain the project plan. Establish and maintain a formal, approved, integrated project plan (covering business and IT resources) to guide project execution and control throughout the life of the project. The scope of projects should be clearly defined and tied to building or enhancing business capability.	a. Frequency of information security-project status reviews
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Incorporate information security into the project plan, identifying the information security environment and controls to be implemented by the project team to protect organizational assets.	2
2. Include the necessary resource(s), including human resources, infrastructure and funding, to identify and implement information security requirements effectively.	
3. Engage business stakeholders early in integrated project plan development.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 4.2 Develop project management plan
Management Practice	**Example Information Security-specific Metrics**
BAI11.05 Manage project quality. Prepare and execute a quality management plan, processes and practices that align with quality management standards (QMS). Describe the approach to project quality and implementation. The plan should be formally reviewed and agreed on by all parties concerned and incorporated into the integrated project plans.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 8. Project quality management
Management Practice	**Example Information Security-specific Metrics**
BAI11.06 Manage project risk. Eliminate or minimize specific risk associated with projects through a systematic process of planning, identifying, analyzing, responding to, monitoring and controlling the areas or events with potential to cause unwanted change. Define and record any risk faced by project management.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Integrate information security projects in the enterprise's project management process.	2
2. Incorporate information security risk and remediation actions into the project risk register.	3
3. Manage and maintain a project risk register to manage project risk.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.15 Program management (PM-4)
PMBOK Guide Sixth Edition, 2017	Part 1: 11. Project risk management

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
BAI11.07 Monitor and control projects. Measure project performance against key project performance criteria such as schedule, quality, cost and risk. Identify any deviations from expected targets. Assess the impact of deviations on the project and overall program and report results to key stakeholders.	a. Frequency of information security project status reviews
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Perform periodic independent assessments of projects to ensure that information security requirements are implemented effectively.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 4.5 Monitor and control project work
Management Practice	**Example Information Security-specific Metrics**
BAI11.08 Manage project resources and work packages. Manage project work packages by placing formal requirements on authorizing and accepting work packages and assigning and coordinating appropriate business and IT resources.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 4.3 Direct and manage project work
Management Practice	**Example Information Security-specific Metrics**
BAI11.09 Close a project or iteration. At the end of each project, release or iteration, require the project stakeholders to ascertain whether the project, release or iteration delivered the required results in terms of capabilities and contributed as expected to program benefits. Identify and communicate any outstanding activities required to achieve planned results of the project and/or benefits of the program. Identify and document lessons learned for future projects, releases, iterations and programs.	a. Percent of project data not in conformance with data destruction or retention policies or procedures
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that project information is appropriately destroyed or archived.	2
2. Ensure that project-related equipment and technology, if no longer needed, are disposed of securely (e.g., prototypes, hard drives, etc.).	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 4.7 Close project or phase

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
BAI11.01 Maintain a standard approach for project management.	ISFA APO02.02	Information security capabilities	There are no information security-specific outputs for this practice.	
	ISFA APO02.06	Information security plan/program	There are no information security-specific outputs for this practice.	
	ISFA BAI02.01	Information security requirements	There are no information security-specific outputs for this practice.	
BAI11.02 Start up and initiate a project.	There are no information security-specific inputs for this practice.		Project business case including mandatory information security activities	ISFA BAI11.04 ISFA BAI11.05
BAI11.03 Manage stakeholder engagement.	There are no information security-specific inputs or outputs for this practice.			
BAI11.04 Develop and maintain the project plan.	ISFA APO02.06	Information security plan/program	Project plan including the information security goals, objectives and requirements	ISFA BAI11.06
	ISFA BAI11.02	Project business case including mandatory information security activities		
BAI11.05 Manage project quality.	ISFA BAI11.02	Project business case including mandatory information security activities	There are no information security-specific outputs for this practice.	
BAI11.06 Manage project risk.	ISFA BAI11.04	Project plan including the information security goals, objectives and requirements	Information security risk log included as part of the overall project risk log	Internal
BAI11.07 Monitor and control projects.	ISFA APO01.01	Information security and related policies	Information security project assessment report identifying control weaknesses and recommended corrective action plans	Internal
	ISFA APO02.06	Information security plan/program		
	ISFA APO12.03	Information security risk profile		
BAI11.08 Manage project resources and work packages.	There are no information security-specific inputs or outputs for this practice.			
BAI11.09 Close a project or iteration.	There are no information security-specific inputs or outputs for this practice.			

Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
PMBOK Guide Sixth Edition, 2017	Part 1: 4. Project integration management: Inputs and Outputs; Part 1: 6. Project schedule management: Inputs and Outputs; Part 1: 10. Project communications management: Inputs & Outputs; Part 1: 11. Project risk management: Inputs and Outputs

4.4 Deliver, Service and Support (DSS)

Page intentionally left blank

Domain: Deliver, Service and Support Management Objective: DSS01— Managed Operations	Focus Area: Information Security
Description	
Coordinate and execute the activities and operational procedures required to deliver internal and outsourced I&T services. Include the execution of predefined standard operating procedures and the required monitoring activities.	
Purpose	
Deliver I&T operational product and service outcomes as planned.	
Information Security Focus Area Relevance	
Information security operations are performed, monitored and managed.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
DSS01.01 Perform operational procedures. Maintain and perform operational procedures and operational tasks reliably and consistently.	a. Number of information security issues not addressed by information security standards b. Number of information security and privacy incidents caused by operational problems c. Number of information security standards not addressed and met by the information security operational plan d. Percent of information security measures that are appropriately implemented and still valid

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Verify that relevant information security operational procedures are included in the regular operational procedures.	2
2. Ensure that the information processing life cycle (receipt, processing, storage and output) incorporates the information security policy and regulatory requirements.	3
3. Ensure that information security operations are planned, performed, tested and controlled in line with the operational plan.	
4. Apply information security and access rights to all data.	

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	TP.SE Safeguard Operational Environment
HITRUST CSF version 9, September 2017	09.01 Document Operating Procedures
ISO/IEC 27002:2013/Cor.2:2015(E)	12.1 Operational procedures and responsibilities
ITIL V3, 2011	Service Operation, 4.1 Event Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.13 Physical and environmental protection (PE-13, PE-14, PE-15)

Management Practice	Example Information Security-specific Metrics
DSS01.02 Manage outsourced I&T services. Manage the operation of outsourced I&T services to maintain the protection of enterprise information and reliability of service delivery.	a. Number of incidents related to third-party noncompliance with enterprise information security policies, standards and requirements

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Incorporate information security requirements into contracts.	3
2. Actively monitor third-party compliance with enterprise information security policies, standards and requirements.	4

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
ISF, The Standard of Good Practice for Information Security 2016	SC1.2 Outsourcing
ISO/IEC 20000-1:2011(E)	4.2 Governance of processes operated by other parties

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
DSS01.03 Monitor I&T infrastructure. Monitor the I&T infrastructure and related events. Store sufficient chronological information in operations logs to reconstruct and review time sequences of operations and other activities surrounding or supporting operations.	a. Number and/or percent of false positives discovered during information security monitoring b. Number and/or percent of events discovered during information security monitoring and related to third-party noncompliance with enterprise information security policies, standards and requirements
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Actively monitor information security aspects of I&T infrastructure, including configuration, operations, access and use.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.10 Maintenance (MA-2, MA-3)
Management Practice	**Example Information Security-specific Metrics**
DSS01.04 Manage the environment. Maintain measures for protection against environmental factors. Install specialized equipment and devices to monitor and control the environment.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that environmental management adheres to information security requirements.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	2.1 System and system elements; 3.2 Categorization (Task 5, 6)
Management Practice	**Example Information Security-specific Metrics**
DSS01.05 Manage facilities. Manage facilities, including power and communications equipment, in line with laws and regulations, technical and business requirements, vendor specifications, and health and safety guidelines.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that facilities management adheres to information security requirements.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
DSS01.01 Perform operational procedures.	ISFA APO03.05	Information security architecture service implementation guidance	Information security operational procedures	Internal
DSS01.02 Manage outsourced I&T services.	ISFA APO01.01	Information security and related policies	Third-party assurance plans	Internal
DSS01.03 Monitor I&T infrastructure.	Outside COBIT	Asset monitoring rules and event conditions	Updated asset monitoring rules	Internal
DSS01.04 Manage the environment.	Outside COBIT	Environmental policies	Updated environmental policies	Internal
DSS01.05 Manage facilities.	Outside COBIT	Facilities assessment reports	Updated facilities assessment reports	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017		3.2 Categorization (Task 5, 6): Inputs and Outputs		

Domain: Deliver, Service and Support Management Objective: DSS02— Managed Service Requests and Incidents	Focus Area: Information Security
Description	
Provide timely and effective response to user requests and resolution of all types of incidents. Restore normal service; record and fulfil user requests; and record, investigate, diagnose, escalate and resolve incidents.	
Purpose	
Achieve increased productivity and minimize disruptions through quick resolution of user queries and incidents. Assess the impact of changes and deal with service incidents. Resolve user requests and restore service in response to incidents.	
Information Security Focus Area Relevance	
Information security incidents and service requests are managed in line with enterprise information security requirements.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
DSS02.01 Define classification schemes for incidents and service requests. Define classification schemes and models for incidents and service requests.	a. Frequency of information security incident response plan testing
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Define and communicate the characteristics of potential security incidents to aid recognition; determine potential impact to facilitate a proportionate response.	3
2. Define criteria and implement processes for regulatory reporting of security incidents.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	IA.IP Implement Incident Investigation Processes
HITRUST CSF version 9, September 2017	11.01 Reporting Information Security Incidents and Weaknesses
ISF, The Standard of Good Practice for Information Security 2016	TM2 Security Incident Management
ISO/IEC 20000-1:2011(E)	8.1 Incident and service request management
ISO/IEC 27002:2013/Cor.2:2015(E)	16. Information security incident management
Management Practice	**Example Information Security-specific Metrics**
DSS02.02 Record, classify and prioritize requests and incidents. Identify, record and classify service requests and incidents and assign a priority according to business criticality and service agreements.	a. Number of information security incidents open/closed and their risk rankings b. Mean time to detect information security incidents c. Cost of information security incidents d. Completeness of information security incident information
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Maintain an information security incident investigation and response procedure.	2
2. Ensure that measures are in place to protect the confidentiality of information related to information security incidents.	
3. Implement a process to allow users to request information security guidance.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
DSS02.03 Verify, approve and fulfill service requests. Select the appropriate request procedures and verify that the service requests fulfill defined request criteria. Obtain approval, if required, and fulfill the requests.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Operation, 4.3 Request Fulfilment

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
DSS02.04 Investigate, diagnose and allocate incidents. Identify and record incident symptoms, determine possible causes, and allocate for resolution.	a. Number of deviations in evidence collection from local forensic evidence rules b. Number of staff qualified to operate within the local forensic rules c. Number and/or percent of false positives identified from information security incidents
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Maintain a procedure for evidence collection in line with applicable forensic evidence rules and regulations.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
DSS02.05 Resolve and recover from incidents. Document, apply and test the identified solutions or workarounds. Perform recovery actions to restore the I&T-related service.	a. Percent of incidents requiring configuration or procedural changes b. Mean time to resolve information security incidents c. Deviation from Recovery Time Objectives (RTOs) d. Deviation from Recovery Point Objectives (RPOs) e. Time to determine solution following incident alert f. Number of incident response cases opened vs. incident response cases closed or pending
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Execute the information security incident response plan.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Service Operation, 4.2 Incident Management
National Institute of Standards and Technology Framework for Improving Critical Infrastructure Cybersecurity v1.1, April 2018	RC.RP Recovery Planning
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.9 Incident response (IR-4, IR-5, IR-6)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 19: Incident Response and Management
Management Practice	**Example Information Security-specific Metrics**
DSS02.06 Close service requests and incidents. Verify satisfactory incident resolution and/or fulfilment of requests, and close.	a. Number of postmortems or root cause evaluations performed on critical information security incidents b. Number of regulatory incident report filings not performed c. Number of regulatory incident report-filing deadlines missed
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
DSS02.07 Track status and produce reports. Regularly track, analyze and report incidents and fulfilment of requests. Examine trends to provide information for continual improvement.	a. Frequency of follow-up actions required for information security incidents
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that information security incidents and appropriate follow-up actions, including root cause analysis, adhere to existing incident and problem management processes.	3
2. Drive resolution of investigations for information security-related incidents.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	MI.IM Ensure Incident Mitigation; IR.IR Incident Reporting
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.9 Incident response (IR-7, IR-8)

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
DSS02.01 Define classification schemes for incidents and service requests.	ISFA APO01.01	Information security and related policies	Information security incident classification scheme	ISFA DSS02.02
DSS02.02 Record, classify and prioritize requests and incidents.	ISFA DSS02.01	Information security incident classification scheme	Classified and prioritized information security incidents and service requests	ISFA APO08.03 ISFA APO12.01 ISFA APO13.03 ISFA DSS02.07
	ISFA DSS05.07	Security incident tickets		
DSS02.03 Verify, approve and fulfil service requests.	There are no information security-specific inputs or outputs for this practice.			
DSS02.04 Investigate, diagnose and allocate incidents.	There are no information security-specific inputs for this practice.		Evidence collection procedure	Internal
DSS02.05 Resolve and recover from incidents.	Outside COBIT	Business impact assessment, organizational risk management policy, incident classification scheme	Incident response plan	ISFA DSS02.07
DSS02.06 Close service requests and incidents.	There are no information security-specific inputs or outputs for this practice.			
DSS02.07 Track status and produce reports.	ISFA DSS02.02	Classified and prioritized information security incidents and service requests	Lessons learned	Internal
	ISFA DSS02.05	Incident response plan		
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this practice				

Page intentionally left blank

Domain: Deliver, Service and Support Management Objective: DSS03— Managed Problems	Focus Area: Information Security
Description	
Identify and classify problems and their root causes. Provide timely resolution to prevent recurring incidents. Provide recommendations for improvements.	
Purpose	
Increase availability, improve service levels, reduce costs, improve customer convenience and satisfaction by reducing the number of operational problems, and identify root causes as part of problem resolution.	
Information Security Focus Area Relevance	
Information security problems are managed in line with enterprise information security requirements.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
DSS03.01 Identify and classify problems. Define and implement criteria and procedures to identify and report problems. Include problem classification, categorization and prioritization.	a. Number of new information security discoveries that were logged
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Classify, categorize and prioritize information security problems.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 20000-1:2011(E)	8.2 Problem management
Management Practice	**Example Information Security-specific Metrics**
DSS03.02 Investigate and diagnose problems. Investigate and diagnose problems using relevant subject matter experts to assess and analyze root causes.	a. Number of recurring information security problems that remain unresolved b. Number of identified information security problems that are determined to be false positives
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Investigate causes of and effects attributed to information security problems.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
DSS03.03 Raise known errors. As soon as root causes of problems are identified, create known-error records, document appropriate workarounds and identify potential solutions.	a. Percent of information security problems escalated
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Escalate information security problems as necessary.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
DSS03.04 Resolve and close problems. Identify and initiate sustainable solutions addressing the root cause. Raise change requests via the established change management process, if required, to resolve errors. Ensure that the personnel affected are aware of the actions taken and the plans developed to prevent future incidents from occurring.	a. Number of critical information security-related problems resolved
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Conduct root cause analysis, resolve information security problems and update the incident response plan.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
DSS03.05 Perform proactive problem management. Collect and analyze operational data (especially incident and change records) to identify emerging trends that may indicate problems. Log problem records to enable assessment.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	MI.IC Ensure Incident Containment
ITIL V3, 2011	Service Operation, 4.4 Problem Management

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
DSS03.01 Identify and classify problems.	**From**	**Description**	**Description**	**To**
	Outside COBIT	Vulnerability assessments	Information security problems classification scheme	ISFA DSS03.04
DSS03.02 Investigate and diagnose problems.	There are no information security-specific inputs for this practice.		Updated root cause of problems	Internal
DSS03.03 Raise known errors.	There are no information security-specific inputs for this practice.		Updated known error records	Internal
DSS03.04 Resolve and close problems.	ISFA DSS03.01	Information security problems classification scheme	Root causes of problems	ISFA DSS03.05
DSS03.05 Perform proactive problem management.	ISFA DSS03.04	Root causes of problems	Implementation of information security policies, procedures and action plans to address root causes	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this practice				

Domain: Deliver, Service and Support Management Objective: DSS04—Managed Continuity	Focus Area: Information Security
Description	
Establish and maintain a plan to enable the business and IT organizations to respond to incidents and quickly adapt to disruptions. This will enable continued operations of critical business processes and required I&T services and maintain availability of resources, assets and information at a level acceptable to the enterprise.	
Purpose	
Adapt rapidly, continue business operations and maintain availability of resources and information at a level acceptable to the enterprise in the event of a significant disruption (e.g., threats, opportunities, demands).	
Information Security Focus Area Relevance	
Information security functions continue to operate and provide the required information security services in the event of a significant disruption.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
DSS04.01 Define the business continuity policy, objectives and scope. Define business continuity policy and scope, aligned with enterprise and stakeholder objectives, to improve business resilience.	a. Number of critical information security systems covered by the business continuity plan b. Number of defined events that triggered a business continuity event c. Number of information security requirements included in the business impact analysis
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Incorporate information security into business continuity activities.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	12.01 Information Security Aspects of Business Continuity Management
ISF, The Standard of Good Practice for Information Security 2016	BC1.1 Business Continuity Strategy; BC1.2 Business Continuity Program
ISO/IEC 27002:2013/Cor.2:2015(E)	17. Information security aspects of business continuity management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-1)
Management Practice	**Example Information Security-specific Metrics**
DSS04.02 Maintain business resilience. Evaluate business resilience options and choose a cost-effective and viable strategy that will ensure enterprise continuity, disaster recovery and incident response in the face of a disaster or other major incident or disruption.	a. Number of critical information security systems covered by the disaster recovery plan
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Include information security scenarios in business resilience activities.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	BC1.3 Resilient Technical Environments
ITIL V3, 2011	Service Design, 4.6 IT Continuity Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-2)

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
DSS04.03 Develop and implement a business continuity response. Develop a business continuity plan (BCP) and disaster recovery plan (DRP) based on the strategy. Document all procedures necessary for the enterprise to continue critical activities in the event of an incident.	a. Number of critical information security requirements in the business continuity plan
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Include information security requirements in the BCP and DRP.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	BC1.4 Crisis Management; BC2.1 Business Continuity Planning
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-6, CP-9, CP-10)
Management Practice	**Example Information Security-specific Metrics**
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP). Test continuity on a regular basis to exercise plans against predetermined outcomes, uphold business resilience and allow innovative solutions to be developed.	a. Number of information security issues tested as part of the BCP and/or DRP
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	PP.RS Develop and Maintain Response Plans; PP.RP Develop and Maintain Recovery Plans
ISF, The Standard of Good Practice for Information Security 2016	BC2.3 Business Continuity Testing
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 20: Penetration Tests and Red Team Exercises
Management Practice	**Example Information Security-specific Metrics**
DSS04.05 Review, maintain and improve the continuity plans. Conduct a management review of the continuity capability at regular intervals to ensure its continued suitability, adequacy and effectiveness. Manage changes to the plans in accordance with the change control process to ensure that continuity plans are kept up to date and continually reflect actual business requirements.	a. Number of business continuity plan updates triggered by a security incident b. Frequency with which the business continuity plans are updated c. Frequency with which the disaster recovery plans are updated
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Evaluate prior information security incidents to improve the BCP.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
DSS04.06 Conduct continuity plan training. Provide all concerned internal and external parties with regular training sessions regarding procedures and their roles and responsibilities in case of disruption.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-4)

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
DSS04.07 Manage backup arrangements. Maintain availability of business-critical information.	a. Number of information security requirements included in the backup and restore arrangements
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that information security requirements are included in the backup and restore arrangements.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	IP.BP Apply Backup Processes
HITRUST CSF version 9, September 2017	09.05 Information Back-Up
ISF, The Standard of Good Practice for Information Security 2016	SY2.3 Backup
ISO/IEC 27002:2013/Cor.2:2015(E)	12.3 Backup
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.6 Contingency planning (CP-3)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 10: Data Recovery Capability
Management Practice	**Example Information Security-specific Metrics**
DSS04.08 Conduct post-resumption review. Assess the adequacy of the business continuity plan (BCP) and disaster response plan (DRP) following successful resumption of business processes and services after a disruption.	a. Number of disaster declarations based on information security incidents
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
DSS04.01 Define the business continuity policy, objectives and scope.	Outside COBIT	Policy for business continuity	Updated policy for business continuity	Internal
DSS04.02 Maintain business resilience.	Outside COBIT	BIA	Updated BIA	Internal
DSS04.03 Develop and implement a business continuity response.	Outside COBIT	BCP	Updated BCP	Internal
DSS04.04 Exercise, test and review the business continuity plan (BCP) and disaster response plan (DRP).	There are no information security-specific inputs or outputs for this practice.			
DSS04.05 Review, maintain and improve the continuity plans.	Outside COBIT	BCP	Updated BCP	Internal
DSS04.06 Conduct continuity plan training.	There are no information security-specific inputs or outputs for this practice.			
DSS04.07 Manage backup arrangements.	Outside COBIT	Test results of backup data	Updated test results of backup data	Internal
DSS04.08 Conduct post-resumption review.	Outside COBIT	Post-resumption review reports	Updated post-resumption review reports	Internal
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this practice				

Page intentionally left blank

Domain: Deliver, Service and Support Management Objective: DSS05—Managed Security Services	Focus Area: Information Security
Description	
Protect enterprise information to maintain the level of information security risk acceptable to the enterprise in accordance with the security policy. Establish and maintain information security roles and access privileges. Perform security monitoring.	
Purpose	
Minimize the business impact of operational information security vulnerabilities and incidents.	
Information Security Focus Area Relevance	
The business impact of operational information security vulnerabilities and incidents is minimized to preserve confidentiality, integrity and availability of enterprise information.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
DSS05.01 Protect against malicious software. Implement and maintain preventive, detective and corrective measures (especially up-to-date security patches and virus control) across the enterprise to protect information systems and technology from malicious software (e.g., malware, ransomware, viruses, worms, spyware, spam).	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that a vulnerability management program, including patch and configuration management, is in place.	3
2. Ensure that antivirus, appropriate sandboxing and other advanced threat protection (ATP) measures are selected, deployed, monitored and maintained.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	DP.DC Detect Malicious Code; RI.VT Vulnerability and Threat Identification
HITRUST CSF version 9, September 2017	09.04 Protection Against Malicious & Mobile Code
ISF, The Standard of Good Practice for Information Security 2016	TS1 Security Solutions
ISO/IEC 27002:2013/Cor.2:2015(E)	12.2 Protection against malware
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 4: Continuous Vulnerability Assessment and Remediation; CSC 8: Malware Defenses
Management Practice	**Example Information Security-specific Metrics**
DSS05.02 Manage network and connectivity security. Use security measures and related management procedures to protect information over all methods of connectivity.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	AC.MI Manage Network Integrity & Segregation; CM.MN Monitor Networks; AC.CP Manage Communication Protections
HITRUST CSF version 9, September 2017	01.04 Network Access Control
ISF, The Standard of Good Practice for Information Security 2016	PA2.3 Mobile Device Connectivity; NC1.1 Network Device Configuration
ISO/IEC 27002:2013/Cor.2:2015(E)	13.1 Network security management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.20 System and information integrity (SI-8)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 9: Limitation and Control of Network Ports, Protocols, and Services; CSC 11: Secure Configurations for Network Devices such as Firewalls, Routers, and Switches

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
DSS05.03 Manage endpoint security. Ensure that endpoints (e.g., laptop, desktop, server, and other mobile and network devices or software) are secured at a level that is equal to or greater than the defined security requirements for the information processed, stored or transmitted.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	IP.MM Apply Mobile Device Management; TP.MP Apply Media Protection; DP.DP Detect Mobile Code and Browser Protection
ISF, The Standard of Good Practice for Information Security 2016	PM1.3 Remote Working; PA2.1 Mobile Device Configuration; PA2.4 Employee-owned Devices; PA2.5 Portable Storage Devices; NC1.6 Remote Maintenance
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.4 Assessment, authorization and monitoring (CA-8, CA-9); 3.19 System and communications protection (SC-10)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 3: Secure Configurations for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers; CSC 7: Email and Web Browser Protections
Management Practice	**Example Information Security-specific Metrics**
DSS05.04 Manage user identity and logical access. Ensure that all users have information access rights in accordance with business requirements. Coordinate with business units that manage their own access rights within business processes.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	10.03 Cryptographic Controls
ISF, The Standard of Good Practice for Information Security 2016	PM1.1 Employment Life Cycle; SA1 Access Management
ISO/IEC 27002:2013/Cor.2:2015(E)	7.3 Termination and change of employment; 9. Access control
ITIL V3, 2011	Service Operation, 4.5 Access Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.1 Access control (AC-11, AC-12); 3.11 Media protection (MP-2, MP-4, MP-7); 3.13 Physical and environmental protection (PE-2, PE-3, PE-6)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 1: Inventory of Authorized and Unauthorized Devices; CSC 2: Inventory of Authorized and Unauthorized Software; CSC 5: Controlled Use of Administrative Privileges; CSC 16: Account Monitoring and Control

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
DSS05.05 Manage physical access to I&T assets. Define and implement procedures (including emergency procedures) to grant, limit and revoke access to premises, buildings and areas, according to business need. Access to premises, buildings and areas should be justified, authorized, logged and monitored. This requirement applies to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors or any other third party.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	AC.MA Manage Access; ID.DI Determine Impacts
HITRUST CSF version 9, September 2017	01.01 Business Requirement for Access Control; 01.02 Authorized Access to Information Systems; 02.0 Human Resources Security
ISF, The Standard of Good Practice for Information Security 2016	NC1.2 Physical Network Management
ISO/IEC 27002:2013/Cor.2:2015(E)	11. Physical and environmental security
Management Practice	**Example Information Security-specific Metrics**
DSS05.06 Manage sensitive documents and output devices. Establish appropriate safeguards in relation to sensitive I&T assets, such as negotiable instruments, special-purpose printers or security tokens.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	CM.Ph Monitor Physical
HITRUST CSF version 9, September 2017	01.06 Application & Information Access Control; 01.07 Mobile Computing & Teleworking; 08.0 Physical & Environmental Security; 10.03 Cryptographic Controls; 10.04 Security of System Files
ISF, The Standard of Good Practice for Information Security 2016	IR2.3 Business Impact Assessment - Confidentiality Requirements; IR2.4 Business Impact Assessment - Integrity Requirements; IR2.5 Business Impact Assessment - Availability Requirements; IM2.2 Sensitive Physical Information; PA2.2 Enterprise Mobility Management
ISO/IEC 27002:2013/Cor.2:2015(E)	10. Cryptography
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.1 Access control (AC-2, AC-3, AC-4, AC-5, AC-6, AC-13, AC-24); 3.7 Identification and authentication (IA-2, IA-10, IA-11)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 15: Wireless Access Control
Management Practice	**Example Information Security-specific Metrics**
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events. Using a portfolio of tools and technologies (e.g., intrusion detection tools), manage vulnerabilities and monitor the infrastructure for unauthorized access. Ensure that security tools, technologies and detection are integrated with general event monitoring and incident management.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A

A. Component: Process *(cont.)*	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	IR2.6 Threat Profiling
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.7 Identification and authentication (IA-3); 3.11 Media protection (MP-1); 3.13 Physical and environmental protection (PE-5); 3.19 System and communications protection (SC-15)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 6: Maintenance, Monitoring, and Analysis of Audit Logs

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
DSS05.01 Protect against malicious software.	There are no information security-specific inputs for this practice. The COBIT 2019 core-model inputs are applicable.		Information security management reports	ISFA APO02.02 ISFA APO02.03
			Information security service catalog	ISFA APO04.01 ISFA APO09.01 ISFA BAI03.11
DSS05.02 Manage network and connectivity security.	There are no information security-specific inputs or outputs for this practice. The COBIT 2019 core-model inputs and/or outputs are applicable.			
DSS05.03 Manage endpoint security.	There are no information security-specific inputs or outputs for this practice. The COBIT 2019 core-model inputs and/or outputs are applicable.			
DSS05.04 Manage user identity and logical access.	There are no information security-specific inputs or outputs for this practice. The COBIT 2019 core-model inputs and/or outputs are applicable.			
DSS05.05 Manage physical access to I&T assets.	There are no information security-specific inputs or outputs for this practice. The COBIT 2019 core-model inputs and/or outputs are applicable.			
DSS05.06 Manage sensitive documents and output devices.	There are no information security-specific inputs or outputs for this practice. The COBIT 2019 core-model inputs and/or outputs are applicable.			
DSS05.07 Manage vulnerabilities and monitor the infrastructure for security-related events.	There are no information security-specific inputs or outputs for this practice. The COBIT 2019 core-model inputs and/or outputs are applicable.			
Related Guidance (Standards, Frameworks, Compliance Requirements)		**Detailed Reference**		
No related guidance for this practice				

Domain: Deliver, Service and Support Management Objective: DSS06—Managed Business Process Controls	Focus Area: Information Security
Description	
Define and maintain appropriate business process controls to ensure that information related to and processed by in-house or outsourced business processes satisfies all relevant information control requirements. Identify the relevant information control requirements. Manage and operate adequate input, throughput and output controls (application controls) to ensure that information and information processing satisfy these requirements.	
Purpose	
Maintain information integrity and the security of information assets handled within business processes in the enterprise or its outsourced operation.	
Information Security Focus Area Relevance	
Information security requirements and objectives are incorporated and integrated into business processes and controls.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
DSS06.01 Align control activities embedded in business processes with enterprise objectives. Continually assess and monitor the execution of business process activities and related controls (based on enterprise risk), to ensure that processing controls align with business needs.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Identify and prioritize IT and operational technology (OT) information security processes in line with business risk, compliance, etc.	2
2. Identify and implement needed application controls.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 10, 11)
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 14: Controlled Access Based on the Need to Know
Management Practice	**Example Information Security-specific Metrics**
DSS06.02 Control the processing of information. Operate the execution of the business process activities and related controls, based on enterprise risk. Ensure that information processing is valid, complete, accurate, timely and secure (i.e., reflects legitimate and authorized business use).	a. Number of information security-related incidents due to inadequate information security controls in place
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	13.01 Openness and Transparency; 13.02 Individual Choice and Participation
ISF, The Standard of Good Practice for Information Security 2016	BA1.4 Information Validation

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority. Manage business roles, responsibilities, levels of authority and segregation of duties needed to support the business process objectives. Authorize access to all information assets related to business information processes, including those under the custody of the business, IT and third parties. This ensures that the business knows where the data are and who is handling data on its behalf.	a. Percent of access holders with inappropriate system privileges b. Percent of access holders with intentional segregation of duties (SoD) violations c. Percent of access reviews completed d. Percent of systems managed with automated identity and access management tools
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Allocate access rights on the basis of need-to-know and least-privilege principles and job requirements.	3
2. Periodically review authorizations.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	13.04 Collection, Use and Disclosure
ISO/IEC 27002:2013/Cor.2:2015(E)	7. Human resource security
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 5: Controlled Use of Administrative Privileges
Management Practice	**Example Information Security-specific Metrics**
DSS06.04 Manage errors and exceptions. Manage business process exceptions and errors and facilitate remediation, executing defined corrective actions and escalating as necessary. This treatment of exceptions and errors provides assurance of the accuracy and integrity of the business information process.	a. Percent of access granted or revoked due to emergencies b. Percent of emergency access not revoked when emergency ends
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Remove access in emergency situations.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
DSS06.05 Ensure traceability and accountability for information events. Ensure that business information can be traced to an originating business event and associated with accountable parties. This discoverability provides assurance that business information is reliable and has been processed in accordance with defined objectives.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Deploy a security incident and event management (SIEM) tool.	3
2. Implement endpoint, switch and router logging and network timing protocol.	4
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
DSS06.06 Secure information assets. Secure information assets accessible by the business through approved methods, including information in electronic form (e.g., portable media devices, user applications and storage devices, or other methods that create new assets in any form), information in physical form (e.g., source documents or output reports) and information during transit. This benefits the business by providing end-to-end safeguarding of information.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. Enforce data classification, acceptable use, and information security policies and procedures to support information asset protection.	3

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Cybermaturity Platform, 2018	AC.MP Manage Access Permissions
The CIS Critical Security Controls for Effective Cyber Defense Version 6.1, August 2016	CSC 18: Application Software Security

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
DSS06.01 Align control activities embedded in business processes with enterprise objectives.	There are no information security-specific inputs for this practice.		Secure application controls	Internal
DSS06.02 Control the processing of information.	There are no information security-specific inputs or outputs for this practice.			
DSS06.03 Manage roles, responsibilities, access privileges and levels of authority.	ISFA APO13.01	Information security management system (ISMS) scope statement	Updated roles, responsibilities, access privileges and levels of authority	Internal
	ISFA DSS05.05	Access logs		
	Outside COBIT	Allocated roles and responsibilities		
DSS06.04 Manage errors and exceptions.	There are no information security-specific inputs for this practice.		Updated access privileges	Internal
DSS06.05 Ensure traceability and accountability for information events.	There are no information security-specific inputs or outputs for this practice.			
DSS06.06 Secure information assets.	Outside COBIT	Asset inventory	Reports of violations	ISFA DSS05.03

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 10, 11): Inputs and Outputs

Page intentionally left blank

4.5 Monitor, Evaluate and Assess (MEA)

01 Managed Performance and Conformance Monitoring

02 Managed System of Internal Control

03 Managed Compliance With External Requirements

04 Managed Assurance

Page intentionally left blank

Domain: Monitor, Evaluate and Assess Management Objective: MEA01 — Managed Performance and Conformance Monitoring	Focus Area: Information Security
Description	
Collect, validate and evaluate enterprise and alignment goals and metrics. Monitor that processes and practices are performing against agreed performance and conformance goals and metrics. Provide reporting that is systematic and timely.	
Purpose	
Provide transparency of performance and conformance and drive achievement of goals.	
Information Security Focus Area Relevance	
Information security practices align with internal performance and conformance requirements and are monitored and reported to stakeholders on an ongoing basis.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
MEA01.01 Establish a monitoring approach. Engage with stakeholders to establish and maintain a monitoring approach to define the objectives, scope and method for measuring business solution and service delivery and contribution to enterprise objectives. Integrate this approach with the corporate performance management system.	a. Date of last CISO review and approval of monitoring approach
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes - Measurement and Analysis
SF, The Standard of Good Practice for Information Security 2016	SI2 Security Performance
ISO/IEC 27001:2013/Cor.2:2015(E)	9.1 Monitoring, measurement, analysis and evaluation
ISO/IEC 27004:2016(E)	6. Characteristics; 7. Types of measures; 8. Processes
ISO/IEC 38500:2015(E)	5.5 Principle 4: Performance; 5.6 Principle 5: Conformance
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.1 Preparation (Task 13); 3.3 Selection (Task 2); 3.7 Monitoring (Task 1)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.4 Assessment, authorization and monitoring (CA-2, CA-7); 3.20 System and information integrity (SI-4)
Management Practice	**Example Information Security-specific Metrics**
MEA01.02 Set performance and conformance targets. Work with stakeholders to define, periodically review, update and approve performance and conformance targets within the performance measurement system.	a. Percent of security performance targets aligned with overall I&T performance standards
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Define information security performance targets consistent with overall I&T performance standards.	2
2. Communicate information security performance and conformance targets with key due diligence stakeholders.	
3. Evaluate whether the information security goals and metrics are adequate: specific, measurable, achievable, relevant and time-bound.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes - Process Management
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.4 Assessment, authorization and monitoring (CA-5)

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
MEA01.03 Collect and process performance and conformance data. Collect and process timely and accurate data aligned with enterprise approaches.	a. Number of information security breaches related to noncompliance with information security-related legislation and regulation b. Percent of information security practices that satisfy internal compliance requirements c. Percent of business processes that meet defined information security requirements d. Number of information security incidents and problems
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Collect and analyze performance and conformance data relating to information security and information risk management (e.g., information security metrics, information security reports).	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.20 System and information integrity (SI-2)
Management Practice	**Example Information Security-specific Metrics**
MEA01.04 Analyze and report performance. Periodically review and report performance against targets. Use a method that provides a succinct all-around view of I&T performance and fits within the enterprise monitoring system.	a. Percent of performance values meeting targets and benchmarks b. Percent of reports that are delivered on time c. Percent of stakeholders satisfied with reporting
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Design, implement and agree on a range of information security performance reports.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes - Measurement and Analysis
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.3 Audit and accountability (AU-6)
Management Practice	**Example Information Security-specific Metrics**
MEA01.05 Ensure the implementation of corrective actions. Assist stakeholders in identifying, initiating and tracking corrective actions to address anomalies.	a. Number of information security corrective-action projects
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Develop a tracking process for corrective actions on information security issues.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ITIL V3, 2011	Continual Service Improvement, 4.1 The 7-Step Improvement Process
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.7 Monitoring (Task 3)
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.3 Audit and accountability (AU-5)

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
MEA01.01 Establish a monitoring approach.	ISFA APO01.01	Information security and related policies	Information security monitoring process and procedure	ISFA MEA01.02
	ISFA BAI02.01	Information security requirements		
	Outside COBIT	Information security standards and regulations		
MEA01.02 Set performance and conformance targets.	ISFA MEA01.01	Information security monitoring process and procedure	Agreed-on information security metrics and targets	ISFA APO07.04 ISFA MEA01.04
MEA01.03 Collect and process performance and conformance data.	Outside COBIT	Applicable regulations	Processed monitoring data	Internal
MEA01.04 Analyze and report performance.	ISFA MEA01.02	Agreed-on information security metrics and targets	Information security reports and corrective-action plans updated	ISFA APO01.11
MEA01.05 Ensure the implementation of corrective actions.	Outside COBIT	Escalation guidelines	Tracking process for corrective actions on information security issues	Internal

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.1 Preparation (Task 13): Inputs and Outputs; 3.3 Selection (Task 2): Inputs and Outputs; 3.7 Monitoring (Task 1, Task 3): Inputs and Outputs

Page intentionally left blank

Domain: Monitor, Evaluate and Assess Management Objective: MEA02 — Managed System of Internal Control	Focus Area: Information Security
Description	
Continuously monitor and evaluate the control environment, including self-assessments and self-awareness. Enable management to identify control deficiencies and inefficiencies and to initiate improvement actions. Plan, organize and maintain standards for internal control assessment and process control effectiveness.	
Purpose	
Obtain transparency for key stakeholders on the adequacy of the system of internal controls and thus provide trust in operations, confidence in the achievement of enterprise objectives and an adequate understanding of residual risk.	
Information Security Focus Area Relevance	
Information security controls form part of the enterprise control environment and are self-assessed, monitored and reviewed for effectiveness, with deficiencies reported to stakeholders.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
MEA02.01 Monitor internal controls. Continuously monitor, benchmark and improve the I&T control environment and control framework to meet organizational objectives.	a. Frequency of information security policy and procedures reviews b. Percent of processes that satisfy information security control requirements c. Number of internal control gaps vs. open issues/items
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Perform a periodic review of information security and related policies and procedures.	3
2. Determine the assurance scope (i.e., scope of information security controls to be assessed).	
3. Establish a formal approach to information security assurance.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	09.10 Monitoring
ISO/IEC 38502:2017(E)	5.5 Governance and internal control
National Institute of Standards and Technology Special Publication 800-53, Revision 5 (Draft), August 2017	3.3 Audit and accountability (AU-2)
Management Practice	**Example Information Security-specific Metrics**
MEA02.02 Review effectiveness of business process controls. Review the operation of controls, including monitoring and test evidence, to ensure that controls within business processes operate effectively. Include activities to maintain evidence of the effective operation of controls through mechanisms such as periodic testing, continuous monitoring, independent assessments, command and control centers, and network operation centers. This evidence assures the enterprise that controls meet requirements related to business, regulatory and social responsibilities.	a. Percent of controls in which information security control requirements are met b. Frequency of reviews of applications, systems and networks c. Percent of incidents in which a security control failed
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Measure the effectiveness of information security controls.	3
2. Perform regular reviews of applications, systems and networks against defined information security requirements.	
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
MEA02.03 Perform control self-assessments. Encourage management and process owners to improve controls proactively through a continuing program of self-assessment that evaluates the completeness and effectiveness of management's control over processes, policies and contracts.	a. Number of information security self-assessments performed
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Perform information security assurance assessments (independent and self-assessment) to identify control weaknesses.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISO/IEC 27001:2013/Cor.2:2015(E)	9.3 Management review
National Institute of Standards and Technology Special Publication 800-37, Revision 2 (Draft), May 2018	3.7 Monitoring (Task 2)
Management Practice	**Example Information Security-specific Metrics**
MEA02.04 Identify and report control deficiencies. Identify control deficiencies and analyze and identify their underlying root causes. Escalate control deficiencies and report to stakeholders.	a. Number of control deficiencies determined in security incident reports
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Review information security incident reports for control deficiencies. Report and address noted deficiencies.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
MEA02.01 Monitor internal controls.	ISFA APO01.01	Information security and related policies	Defined information security assurance scope and approach to assess internal controls	ISFA MEA02.03
	ISFA APO13.03	ISMS audit reports		
	Outside COBIT	Independent external		
MEA02.02 Review effectiveness of business process controls.	There are no information security-specific inputs for this practice.		Evidence of effectiveness of information security controls	Internal
MEA02.03 Perform control self-assessments.	ISFA MEA02.01	Defined information security assurance scope and approach to assess internal controls	Information security assurance assessments	ISFA MEA02.04
MEA02.04 Identify and report control deficiencies.	ISFA MEA02.03	Information security assurance assessments	Assessment results and remedial actions	ISFA MEA04.08
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
National Institute of Standards and Technology Special Publication 800-37, Revision 2, September 2017	3.7 Monitoring (Task 2): Inputs and Outputs			

Domain: Monitor, Evaluate and Assess Management Objective: MEA03 — Managed Compliance With External Requirements	Focus Area: Information Security
Description	
Evaluate that I&T processes and I&T-supported business processes are compliant with laws, regulations and contractual requirements. Obtain assurance that the requirements have been identified and complied with; integrate IT compliance with overall enterprise compliance.	
Purpose	
Ensure that the enterprise is compliant with all applicable external requirements.	
Information Security Focus Area Relevance	
Compliance with applicable information security, cybersecurity, privacy, and data breach legislation and regulations is evidenced.	

A. Component: Process		
Management Practice	**Example Information Security-specific Metrics**	
MEA03.01 Identify external compliance requirements. On a continuous basis, monitor changes in local and international laws, regulations and other external requirements and identify mandates for compliance from an I&T perspective.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
1. Establish arrangements for monitoring information security compliance to external requirements.		2
2. Determine external compliance requirements to be met (including legal, regulatory, privacy and contractual requirements).		
3. Identify and communicate sources of information security material to help meet external compliance requirements.		3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
CMMI Cybermaturity Platform, 2018	BC.RR Determine Legal / Regulatory Requirements	
HITRUST CSF version 9, September 2017	06.01 Compliance with Legal Requirements	
ISF, The Standard of Good Practice for Information Security 2016	SM2.3 Legal and Regulatory Compliance	
Management Practice	**Example Information Security-specific Metrics**	
MEA03.02 Optimize response to external requirements. Review and adjust policies, principles, standards, procedures and methodologies to ensure that legal, regulatory and contractual requirements are addressed and communicated. Consider adopting and adapting industry standards, codes of good practice, and good practice guidance.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.		N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas - Principle 13	
Management Practice	**Example Information Security-specific Metrics**	
MEA03.03 Confirm external compliance. Confirm compliance of policies, principles, standards, procedures and methodologies with legal, regulatory and contractual requirements.	a. Percent of information security practices that satisfy external compliance requirements	
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)		**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.		N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**	
No related guidance for this management practice		

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
MEA03.04 Obtain assurance of external compliance. Obtain and report assurance of compliance and adherence with policies, principles, standards, procedures and methodologies. Confirm that corrective actions to address compliance gaps are closed in a timely manner.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.

Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	Capability Level
1. In the absence of third-party assurance, obtain evidence of compliance from third parties.	2

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
CMMI Data Management Maturity Model, 2014	Supporting Processes - Process Quality Assurance
ISO/IEC 27002:2013/Cor.2:2015(E)	18. Compliance

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
MEA03.01 Identify external compliance requirements.	ISFA BAI02.01	Information security requirements	External information security compliance requirements	ISFA BAI02.01
	Outside COBIT	Information security standards and regulations		
MEA03.02 Optimize response to external requirements.	Outside COBIT	Applicable regulations	Updated external requirements	Internal
MEA03.03 Confirm external compliance.	There are no information security-specific inputs for this practice.		Information security compliance report	Internal
MEA03.04 Obtain assurance of external compliance.	There are no information security-specific inputs for this practice.		Compliance assurance reports	Internal

Related Guidance (Standards, Frameworks, Compliance Requirements)	Detailed Reference
No related guidance for this practice	

Domain: Monitor, Evaluate and Assess Management Objective: MEA04 — Managed Assurance	Focus Area: Information Security
Description	
Plan, scope and execute assurance initiatives to comply with internal requirements, laws, regulations and strategic objectives. Enable management to deliver adequate and sustainable assurance in the enterprise by performing independent assurance reviews and activities.	
Purpose	
Enable the organization to design and develop efficient and effective assurance initiatives, providing guidance on planning, scoping, executing and following up on assurance reviews, using a road map based on well-accepted assurance approaches.	
Information Security Focus Area Relevance	
Independent assurance is provided on the effectiveness of the enterprise information security function capabilities.	

A. Component: Process	
Management Practice	**Example Information Security-specific Metrics**
MEA04.01 Ensure that assurance providers are independent and qualified. Ensure that the entities performing assurance are independent from the function, groups or organizations in scope. The entities performing assurance should demonstrate an appropriate attitude and appearance, competence in the skills and knowledge necessary to perform assurance, and adherence to codes of ethics and professional standards.	a. Percent of certified security professionals providing assurance
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Establish information security competencies and qualifications.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
HITRUST CSF version 9, September 2017	06.03 Information System Audit Considerations
Management Practice	**Example Information Security-specific Metrics**
MEA04.02 Develop risk-based planning of assurance initiatives. Determine assurance objectives based on assessments of the internal and external environment and context, the risk of not achieving enterprise goals, and the opportunities associated achievement of the same goals.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
King IV Report on Corporate Governance for South Africa, 2016	Part 5.4: Governance functional areas—Principle 15
Management Practice	**Example Information Security-specific Metrics**
MEA04.03 Determine the objectives of the assurance initiative. Define and agree with all stakeholders on the objectives of the assurance initiative.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Agree on the objectives of the information security assurance review.	2
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Data Management Maturity Model, 2014	Supporting Processes - Process Quality Assurance

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
MEA04.04 Define the scope of the assurance initiative. Define and agree with all stakeholders on the scope of the assurance initiative, based on the assurance objectives.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
CMMI Cybermaturity Platform, 2018	TP.LA Apply Logging and Audit Processes
Management Practice	**Example Information Security-specific Metrics**
MEA04.05 Define the work program for the assurance initiative. Define a detailed work program for the assurance initiative, structured according to the management objectives and governance components in scope.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
MEA04.06 Execute the assurance initiative, focusing on design effectiveness. Execute the planned assurance initiative. Validate and confirm the design of the internal controls in place. Additionally, and specifically in internal audit assignments, consider the cost-effectiveness of the governance component design.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SI1 Security Audit
ISO/IEC 27001:2013/Cor.2:2015(E)	9.2 Internal audit
Management Practice	**Example Information Security-specific Metrics**
MEA04.07 Execute the assurance initiative, focusing on operating effectiveness. Execute the planned assurance initiative. Test whether the internal controls in place are appropriate and sufficient. Test the outcome of the key management objectives in scope of the assurance initiative.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
ISF, The Standard of Good Practice for Information Security 2016	SI1 Security Audit
SO/IEC 27001:2013/Cor.2:2015(E)	9.2 Internal audit

A. Component: Process *(cont.)*	
Management Practice	**Example Information Security-specific Metrics**
MEA04.08 Report and follow up on the assurance initiative. Provide positive assurance opinions, where appropriate, and recommendations for improvement relating to identified operational performance, external compliance and internal control weaknesses.	a. Number of information security-related issues in assurance reports
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
1. Ensure that information security elements are addressed in any audit activity and are therefore addressed in assurance reporting.	3
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	
Management Practice	**Example Information Security-specific Metrics**
MEA04.09 Follow up on recommendations and actions. Agree on, follow up and implement the identified recommendations for improvement.	Additional information security-specific metrics have not been identified for this practice. The COBIT 2019 core metrics are applicable.
Information Security-specific Activities (in addition to COBIT 2019 core-model activities)	**Capability Level**
Additional information security-specific activities have not been identified for this practice. The COBIT 2019 core activities are applicable.	N/A
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**
No related guidance for this management practice	

C. Component: Information Flows and Items				
Management Practice	**Information Security-specific Inputs**		**Information Security-specific Outputs**	
	From	**Description**	**Description**	**To**
MEA04.01 Ensure that assurance providers are independent and qualified.	There are no information security-specific inputs for this practice.		Competence in skills and knowledge	Internal
MEA04.02 Develop risk-based planning of assurance initiatives.	There are no information security-specific inputs or outputs for this practice.			
MEA04.03 Determine the objectives of the assurance initiative.	Outside COBIT	Engagement plan	Updated engagement plan	Internal
MEA04.04 Define the scope of the assurance initiative.	Outside COBIT	Engagement plan	Updated engagement plan	Internal
MEA04.05 Define the work program for the assurance initiative.	There are no information security-specific inputs or outputs for this practice.			
MEA04.06 Execute the assurance initiative, focusing on design effectiveness.	There are no information security-specific inputs or outputs for this practice.			
MEA04.07 Execute the assurance initiative, focusing on operating effectiveness.	There are no information security-specific inputs or outputs for this practice.			
MEA04.08 Report and follow up on the assurance initiative.	ISFA DSS05.02	Results of penetration tests	Audit information security report and recommendations	Internal ISFA APO13.02
	ISFA MEA02.04	Assessment results and remedial actions		
MEA04.09 Follow up on recommendations and actions.	There are no information security-specific inputs or outputs for this practice.			
Related Guidance (Standards, Frameworks, Compliance Requirements)	**Detailed Reference**			
No related guidance for this practice				

Page intentionally left blank