Chapter 1

Introduction and Background

This chapter introduces cybersecurity and discusses why it has become a top concern for boards of directors, senior management, and others. This chapter also provides an overview of an examination of an entity's cybersecurity risk management processes and controls (referred to as an entity's *cybersecurity risk management program*) and related report designed by the AICPA to meet the informational needs of intended users. Finally, the chapter discusses the professional standards practitioners are required to follow when performing the examination.

Introduction

1.01 Almost every day a new cyberattack is announced in the media. Nation states, hackers, organized crime, and malicious insiders are attacking entities because of who they are, what they do, or the information they possess. Sometimes, the attacks are launched simply to cause a business disruption or broader economic interruption. Banks, big-box retailers, government agencies... it seems that none are immune from cyberattacks. Along with the increased number of reported attacks, the number of victims and the amount of information compromised by each attack is also increasing.

1.02 Cybersecurity has become a top concern for boards of directors and senior executives of many entities throughout the country, regardless of their size or the industry in which they operate. In addition, governmental officials are also concerned about cybersecurity at governmental agencies and departments. For most entities, cybersecurity is a significant business risk that needs to be identified, assessed, and managed along with other business risks the entity faces, and it is management's responsibility to ensure that all employees throughout the entity, not only those in the information technology department, address cybersecurity risks. Managing this business issue is especially challenging because even an entity with a highly sophisticated cybersecurity risk management program has a residual risk that a material cybersecurity breach can occur and not be detected in a timely manner. In other words, an effective cybersecurity risk management program provides reasonable, but not absolute, assurance that material breaches are prevented or detected, and mitigated in a timely manner. Furthermore, the combined effects of entity's dependency on information technology, the complexity of information technology networks and business applications, extensive reliance on third parties, and human nature (for instance, susceptibility to social engineering) are only likely to increase the need for effective cybersecurity risk management programs in the foreseeable future.

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

Potential Users of Cybersecurity Information and Their Interests

1.03 To achieve the entity's business objectives, senior management, as well as others within the entity, frequently need information about the effectiveness of the entity's cybersecurity risk management program, including the processes and controls designed, implemented, and operated to mitigate threats against the entity's sensitive information and systems.

1.04 Members of a board of directors (board members)[1] need information about the cybersecurity risks an entity faces and the cybersecurity risk management program that management implements to help them fulfill their oversight responsibilities. They also want information from independent third-party assessors that will help them evaluate management's effectiveness in managing cybersecurity risks.

1.05 Others may also need information about an entity's cybersecurity risks and its cybersecurity risk management program to make informed decisions. For example,

- analysts and investors may benefit from information about an entity's cybersecurity risk management program. This information is intended to help them understand the cybersecurity risks that could threaten the achievement of the entity's operational, reporting, and compliance (legal and regulatory) objectives and, consequently, have an adverse impact on the entity's value and stock price.
- business partners may need information about the entity's cybersecurity risk management program as part of their overall risk assessment. This information is intended to help business partners determine matters such as whether there is a need for multiple suppliers for a good or service and the extent to which they choose to extend credit to the entity.[2]
- some industry regulators may benefit from information about an entity's cybersecurity risk management program to support their oversight role.

1.06 Analysts, investors, business partners, and regulators recognize that entity management is responsible for identifying, assessing, and mitigating cybersecurity risks. However, many are not in a position to require management

---

[1] This guide uses the term *board members* to refer to the governing body of an entity, which may take the form of a board of directors or supervisory board for a corporation, board of trustees for a not-for-profit entity, board of governors or commissioners for government entities, general partners for a partnership, or owner for a small business.

[2] Some business partners may need a detailed understanding of controls implemented by the entity and the operating effectiveness of those controls to enable them to design and operate their own control activities. For example, business partners whose IT systems are interconnected with systems at the entity may need to understand the specific logical access protection over the interconnected systems implemented by the entity.

This guide is not intended to meet the needs of business partners who need a detailed understanding of the entity's specific controls and their operating effectiveness. AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* provides guidance for practitioners engaged to examine and report on system controls at a *service organization*.

to provide information about an entity's cybersecurity measures to enable them to make better decisions; they must rely on publicly available information, such as that found in general-purpose reports or regulatory filings, to meet their needs. In response to requests from these third parties, corporate directors and senior management have begun requesting general purpose reports from independent third-party assessors on the effectiveness of the entity's cybersecurity risk management program.

1.07 The potential users described in the previous paragraph are the primary users to whom general purpose reports on the effectiveness of the entity's cybersecurity risk management program are directed. Individuals acting in a personal capacity often have different information needs and desires. For example, they might want information about how an entity protects credit card information used to purchase an item on the internet. Therefore, a general purpose report on the effectiveness of an entity's cybersecurity risk management program may not always meet the information needs of such individuals. In addition, a general purpose report may include additional information that may not be easily understood by all individuals. Accordingly, although these individuals may find the report useful, they are not the primary intended users of such a report.

Cybersecurity Risk Management Examination

1.08 To enable practitioners to provide a general purpose report on the effectiveness of an entity's cybersecurity risk management program, the AICPA has developed the *cybersecurity risk management examination* described in this guide. In conjunction with this guide, the AICPA has also developed description criteria for use when preparing and evaluating the description of the entity's cybersecurity risk management program and control criteria intended to be used when evaluating the effectiveness of controls within the entity's cybersecurity risk management program.

1.09 In the cybersecurity risk management examination, there are two distinct but complementary subject matters: (1) the description of the entity's cybersecurity risk management program and (2) the effectiveness of controls within that program to achieve the entity's cybersecurity objectives. As the responsible party, management prepares the description and makes an assertion about the subject matters. Specifically, management's assertion addresses whether the description was prepared in accordance with description criteria and whether the controls within the program were effective to achieve the entity's cybersecurity objectives based on the control criteria. The practitioner examines and reports on that information in accordance with the attestation standards.[3]

1.10 The practitioner performs the cybersecurity risk management examination described in this guide in accordance with the AICPA's attestation standards. In the examination, the practitioner designs and performs procedures to obtain sufficient appropriate evidence about whether the description is presented in accordance with the description criteria and whether the

[3] In certain circumstances, the practitioner may be engaged to report on the description and on the suitability of the design of controls within the entity's cybersecurity risk management program, but not on the effectiveness of the controls. Such an examination (design-only examination) is discussed further beginning in paragraph 1.42.

controls were effective to achieve the entity's cybersecurity objectives based on the control criteria.

1.11 Furthermore, in an examination performed under the attestation standards, the practitioner examines and reports on subject matter that is the responsibility of another party. An attestation engagement is predicated on the concept that a party other than the practitioner (that is, the responsible party) makes an assertion about whether the subject matter is measured or evaluated in accordance with suitable criteria. In a cybersecurity risk management examination, management is ordinarily the responsible party.

1.12 The cybersecurity risk management examination results in the issuance of a *cybersecurity risk management examination report*. The cybersecurity risk management examination report includes three key components:

- *Management's description of the entity's cybersecurity risk management program*. The first component is a management-prepared narrative description of the entity's cybersecurity risk management program (description). This description is designed to provide information about how the entity identifies its information assets, the ways in which the entity manages the cybersecurity risks that threaten it, and the key security policies and processes implemented and operated to protect the entity's information assets against those risks. The description provides the context needed for users to understand the conclusions expressed by management in its assertion and by the practitioner in his or her report.[4] Management uses the description criteria to prepare and evaluate an entity's cybersecurity risk management program. The use of description criteria in the cybersecurity risk management examination is discussed further beginning in paragraph 1.33.
- *Management's assertion*. The second component is an assertion provided by management, which may be as of a point in time or for a specified period of time. Specifically, the assertion addresses whether
  - — the description is presented in accordance with the description criteria and
  - — the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

The AICPA has also developed control criteria for use when evaluating whether the controls within the program were effective to achieve the entity's cybersecurity objectives. The use of control criteria in the cybersecurity risk management examination is discussed further beginning in paragraph 1.33.

- *Practitioner's report.* The third component is a practitioner's report, which contains an opinion that addresses both subject

[4] For this reason, practitioners should not accept a cybersecurity risk management examination if management is unwilling to prepare the description of the entity's cybersecurity risk management program or to include it in the cybersecurity risk management examination report. However, the practitioner may be able to perform a different examination in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*).

matters in the examination. Specifically, the opinion addresses whether

- — the description is presented in accordance with the description criteria and
- — the controls within the entity's cybersecurity risk management program were effective[5] to achieve the entity's cybersecurity objectives based on the control criteria.

1.13 Because the practitioner's report is designed to be included in the cybersecurity risk management examination report, which is intended for broad or general distribution, the practitioner's report is intended for general use. Nevertheless, as discussed throughout this guide, practitioners may decide to restrict the use of the report to specified users.

1.14 Although this guide specifically discusses the AICPA's cybersecurity risk management examination, a practitioner is not prohibited from performing a different examination on an entity's cybersecurity efforts in accordance with the attestation standards. The practitioner may still find much of the guidance in this guide helpful when performing and reporting in such an examination.

Difference Between Cybersecurity and Information Security

1.15 Before the widespread use of the Internet and the World Wide Web, most businesses had only limited connectivity with information systems outside their organizations. As a result, an entity's information security focused on the protection of its IT systems and data against unauthorized access, use, and changes from within the entity. Today, most entities conduct portions of their business in cyberspace; therefore, their IT systems are highly interconnected with other organizations. For the purposes of this guide, *cyberspace* is defined as an interdependent network of information system infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers through which entities interact to conduct business and share information.

1.16 An entity's cybersecurity risks are the subset of its information security risks that arise specifically from threats and vulnerabilities related to the connection to and use of cyberspace. *Cybersecurity* refers to the processes and controls implemented by an entity to manage cybersecurity risks. Because the processes and controls that address cybersecurity risks also address the vast majority of the entity's other information security risks, the terms *cybersecurity* and *information security* are often used interchangeably. The main difference between information security and cybersecurity is that information security also addresses risks that arise from computer systems that are physically isolated from other electronic systems and the protection of information stored in a format that is not accessible through electronic means (such as printed paper stored in filing cabinets). From a practical standpoint, however, the difference is minor because most entities store, process, use, and transmit information

[5] Throughout this guide, the term *effective* (as it relates to controls) encompasses both the suitability of design of controls and the operating effectiveness of controls. This is discussed further in paragraph 1.28.

electronically. For the purposes of this guide, there is no distinction between the two terms.

1.17 By using the term *cybersecurity* instead of *information security*, board members and senior management are acknowledging the new and magnified risks inherent with doing business in cyberspace. Additionally, they recognize that the cyberspace environment is becoming increasingly hostile. The almost daily appearance of new threat actors who exploit the vulnerabilities of cyberspace for criminal or malicious purposes—and their use of new technologies to implement their attacks—increases the risks of operating in cyberspace. Thus, entities have to continually develop more effective and more targeted processes and controls to respond to those risks. This requires board members and senior management to think well beyond the traditional IT areas of networks, applications, and data stores.

Description of the Entity's Cybersecurity Risk Management Program

1.18 As previously discussed, management's description of the entity's cybersecurity risk management program is designed to provide users with information about the environment in which the entity operates and the process used to develop its cybersecurity objectives, identify its information assets and the threats against them, and the processes within the cybersecurity risk management program that the entity has designed and implemented to respond to those risks. The description is intended to enable users to understand the cybersecurity risk management program and the conclusions expressed by management in its assertion and by the practitioner in his or her report. It does not, however, provide a detailed narrative of the entity's controls nor a listing of tests of controls performed by the practitioner and the results thereof.

1.19 As used in this guide, an entity's *cybersecurity risk management program* is defined as the set of policies, processes, and controls designed to protect *information and systems* from *security events* that could *compromise* the achievement of the entity's *cybersecurity objectives* and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented.

1.20 Italicized terms are defined as follows:

- *Information and systems* refers to information in electronic form during its use, processing, transmission, and storage and the systems that use such information to process, transmit or transfer, and store information. A *system* refers to infrastructure, software, people, processes, and data that are designed, implemented, and operated to work together to achieve one or more specific business objectives (for example, delivery of services or production of goods) in accordance with management-specified requirements. As used in this document, systems include manual, automated, and partially automated systems that are used for information processing, manufacturing and production, inventory management and distribution, information storage, and support functions within an organization. Systems that have cybersecurity risks include, for example,

  - manufacturing and production systems that are automated or partially automated (including the industrial control systems components);
  - inventory management or distribution systems; and
  - treasury and funds management and other types of back office systems.

- A *security event* is an occurrence, arising from actual or attempted unauthorized access or use by internal or external parties, that impairs or could impair the availability, integrity, or confidentiality of information or systems, result in unauthorized disclosure or theft of information or other assets, or cause damage to systems. A security incident is a security event that requires action on the part of an entity in order to protect information and other assets and resources.
- A *compromise* refers to a loss of confidentiality, integrity, or availability of information, including any resultant impairment of
  - processing integrity or availability of systems or
  - the integrity or availability of system inputs or outputs.
- An entity's *cybersecurity objectives* are those objectives that the entity establishes to address cybersecurity risks that could otherwise threaten the achievement of the entity's overall business objectives (including compliance, reporting, and operational objectives). Understanding the entity's cybersecurity objectives is integral to the assessment and evaluation of whether controls are effective. Cybersecurity objectives are discussed in more detail later in this chapter.

1.21 The definition in paragraph 1.19 acknowledges a fundamental tenet of cybersecurity: *an entity that operates in cyberspace is likely to experience one or more security events or breaches at some point in time, regardless of the effectiveness of the entity's cybersecurity controls*. Understanding this tenet is essential to dispelling user misconceptions that an effective cybersecurity risk management program will prevent all security events from occurring. In fact, because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that security events are prevented and, for those not prevented, that they are detected, responded to, mitigated against, and recovered from on a timely basis. In other words, an effective cybersecurity risk management program is one that enables the entity to detect security events on a timely basis and to respond to and recover from such events with minimal disruption to the entity's operations.

The Entity's Cybersecurity Objectives

1.22 According to the Committee of Sponsoring Organizations of the Treadway Commission (COSO), in its 2013 *Internal Control—Integrated Framework* (COSO framework), internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of the entity's business objectives. Because of this relationship between internal control and objectives, the COSO framework states that management specifies suitable objectives so

that the risks that threaten the achievement of the entity's overall business objectives can be identified, assessed, and managed.

1.23 According to the COSO framework, there are three categories of objectives:

- *Operations objectives*. These pertain to the effectiveness and efficiency of the entity's operations, including operational and financial performance goals and safeguarding assets against loss.
- *Reporting objectives*. These pertain to internal and external financial and nonfinancial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the entity's policies.
- *Compliance objectives*. These pertain to adherence to laws and regulations to which the entity is subject.

1.24 Cybersecurity risks are one of the types of risks that threaten the achievement of an entity's overall business objectives. Consequently, entities often establish cybersecurity objectives that address their specific cybersecurity risks. Generally, the nature of an entity's cybersecurity objectives varies depending on the environment in which the entity operates, the entity's mission and vision, the overall business objectives established by management, risk appetite, and other factors. For example, a telecommunications entity may have a cybersecurity objective related to the reliable functioning of those aspects of its operations that are deemed to be critical infrastructure, whereas an entity that promotes online dating is likely to regard the confidentiality of personal information collected from its customers as a critical factor toward the achievement of its operating objectives.

1.25 Management is responsible for establishing, and including in the description, the entity's cybersecurity objectives with sufficient clarity to enable users to understand how the processes and controls within the entity's cybersecurity risk management program were designed, implemented, and operated effectively to provide reasonable assurance of achieving those objectives. Because of the importance of the cybersecurity objectives to the cybersecurity risk management examination, the cybersecurity objectives established by management should be suitable for the engagement. Chapter 2, "Accepting and Planning a Cybersecurity Risk Management Examination," discusses the attributes of suitable cybersecurity objectives.

1.26 The practitioner is responsible for determining whether the cybersecurity objectives established by management are suitable for the engagement prior to engagement acceptance. Chapter 2 also discusses that responsibility in further detail.

Effectiveness of Controls Within the Entity's Cybersecurity Risk Management Program

1.27 In addition to providing a description of the entity's cybersecurity risk management program, the cybersecurity risk management examination report also provides information about whether the controls the entity has designed, implemented, and operated to mitigate those risks were effective throughout the period of time covered by the engagement. For that reason, one of the subject matters of the cybersecurity risk management examination is the

effectiveness of controls within an entity's cybersecurity risk management program to achieve the entity's cybersecurity objectives.

1.28 As used throughout this guide, the term *effectiveness of controls* encompasses both the suitability of the design of controls and their operating effectiveness:

- *Controls were suitably designed.* Suitably designed controls, if complied with satisfactorily, provide reasonable assurance of achieving the entity's cybersecurity objectives based on the control criteria. Suitably designed controls operate as designed by persons who have the necessary authority and competence to perform the controls.
- *Controls operated effectively*. Suitably designed controls operate effectively if they provide reasonable assurance of achieving the entity's cybersecurity objectives based on the control criteria.

1.29 Because there are specific considerations when evaluating each, chapter 3, Performing the Cybersecurity Risk Management Examination," of this guide contains separate discussions of suitability of design and operating effectiveness to support the practitioner's overall opinion on the effectiveness of controls to achieve the entity's cybersecurity objectives.

Overview of the Cybersecurity Risk Management Examination

1.30 The cybersecurity risk management examination is performed in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*).

1.31 There are two subject matters in the cybersecurity risk management examination:

1. A description of the entity's cybersecurity risk management program and
2. The effectiveness of the controls within that program to achieve the entity's cybersecurity objectives

1.32 As previously mentioned, management is usually the responsible party (that is, the party responsible for the subject matter) in a cybersecurity risk management examination because management is ultimately responsible for the entity's cybersecurity risk management program; therefore, it is management's responsibility to develop and present the description of the entity's cybersecurity risk management program. The cybersecurity risk management examination is predicated on the fact that management will prepare a written description of the entity's cybersecurity risk management program[6] and a written assertion[7] about whether the description is presented in accordance with

[6] If management is unwilling to prepare the description of the entity's cybersecurity risk management program or to include it in the cybersecurity risk management examination report, a practitioner cannot perform the cybersecurity risk management examination. However, the practitioner may be able to perform a different examination engagement in accordance with AT-C section 105 and AT-C section 205.

[7] As discussed further beginning in paragraph 1.37, management may make its assertion as of a *point in time* or *for a specified period of time*.

the description criteria and whether the controls were effective to achieve the entity's cybersecurity objectives.

1.33 Paragraph .10 of AT-C section 105 defines *criteria* as "the benchmarks used to measure or evaluate the subject matter." To enable the preparation and evaluation of the cybersecurity information, two distinct yet complementary sets of criteria are used in the cybersecurity risk management examination:

1. *Description criteria* are used to prepare, and evaluate the presentation of, the description of the entity's cybersecurity risk management program.
2. *Control criteria* are used to evaluate the effectiveness of controls to achieve the entity's cybersecurity objectives.

1.34 Management is responsible for selecting the criteria to be used. AT-C section 105 states that criteria used in an examination engagement must be both suitable and available[8] before a practitioner can accept the examination. Chapter 2 of this guide provides guidance for determining whether the criteria used in the cybersecurity risk management examination are suitable and available. It also discusses other responsibilities of management and the practitioner in the examination.

1.35 The performance and reporting guidance in this guide focuses on a cybersecurity risk management examination in which (*a*) the description criteria presented in appendix C are used to prepare the description and (*b*) the trust services criteria for security, availability, and confidentiality presented in appendix D are used as the control criteria. Nevertheless, this guidance may also be helpful to a practitioner engaged to perform a cybersecurity risk management examination in which management has elected to use other description and control criteria.

Other Information About the Cybersecurity Risk Management Examination

1.36 In the cybersecurity risk management examination, the practitioner expresses an opinion on whether (*a*) the description is presented in accordance with the description criteria and (*b*) the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria. However, the practitioner does not express an opinion on certain matters related to compliance, privacy, or processing integrity matters. For example, in the cybersecurity risk management examination, the practitioner does *not*

1. *Express an opinion on compliance with laws and regulations.* The cybersecurity risk management examination is not designed to enable a practitioner to opine on whether an entity has complied with laws and regulations. However, it does address IT controls the entity has designed, implemented, and operated to support compliance with those laws or regulations. For example, if an entity has designed and implemented controls over its system to protect the protected health information (PHI) of its customers in accordance with the Health Insurance Portability and Accountability

[8] Paragraph .A42 of AT-C section 105 states that criteria are *suitable* if they are *relevant, objective, measurable*, and *complete*. Paragraph .25*b*ii of AT-C section 105 indicates that criteria used in an examination engagement must be *available* to intended users of the practitioner's report.

Act, the cybersecurity risk management examination would address those controls. In fact, the illustrative cybersecurity objectives described in paragraph 2.59 include a cybersecurity objective related to compliance with applicable laws and regulations, which involves the protection of information subject to privacy requirements from unauthorized access and disclosure.

2. *Express an opinion with regard to privacy and processing integrity criteria.* Similar to the previous example, the cybersecurity risk management examination is not designed to enable a practitioner to express an opinion on whether an entity's controls operated effectively to achieve the entity's cybersecurity objectives based on the processing integrity or privacy criteria included in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).[9] However, it does address the effectiveness of cybersecurity controls that would support the achievement of the entity's processing integrity and privacy objectives. For example, if a drug manufacturer has designed and implemented policies, processes, and controls over its online prescription ordering systems to maintain the confidentiality of customers' PHI during the online ordering process, the cybersecurity risk management examination would address those controls. However, it would not address privacy-specific procedures such as the provision of notice and obtaining consent for use of PHI.

Time Frame of Examination

1.37 Paragraph .A1 of AT-C section 105 states that the subject matter of an attestation examination may be as of a *point in time* or for a *period of time*. Management is responsible for determining the time frame to be covered by the description. Regardless of the time frame selected, the cybersecurity risk management examination contemplates that the time frame is the same for both the description and management's assertion. Furthermore, the cybersecurity risk management examination in this guide contemplates that management elects a specified period of time; accordingly, in this guide, the guidance on evaluating the description and the effectiveness of controls is based on a specified period of time. When reporting on a point in time, the practitioner should use professional judgment when designing his or her examination procedures.

Comparison of the Cybersecurity Risk Management Examination With an Audit of Internal Control Over Financial Reporting That is Integrated With an Audit of Financial Statements

1.38 The cybersecurity risk management examination ordinarily addresses all of the entity's overall business objectives, including operations, compliance, and reporting. In contrast, an audit of internal control over financial reporting that is integrated with an audit of financial statements (integrated

[9] Appendix D of this guide includes TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). TSP section 100 provides criteria for evaluating controls related to security, availability, processing integrity, confidentiality, and privacy (trust services criteria). In TSP section 100, these five attributes are known as *categories*.

audit) only addresses the entity's external financial reporting objectives. Accordingly, the auditor's procedures on IT controls in an integrated audit are not sufficient to enable him or her to provide an opinion on whether controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria.[10]

Cybersecurity Risk Management Examination that Addresses only a Portion of the Entity's Cybersecurity Risk Management Program

1.39 Although the cybersecurity risk management examination discussed in this guide usually addresses an entity-wide cybersecurity risk management program, there may be circumstances in which management may engage the practitioner to examine and report on only a portion of that program, such as one of the following:

- One or more specific business units, segments, or functions of an entity
  - — when those units, segments, or functions operate under an *entity-wide* cybersecurity risk management program or
  - — when those units, segments, or functions operate under an *independent* cybersecurity risk management program
- One or more specific types of information used by the entity

1.40 For example, assume an entity is selling a particular division of its business that operates under a separate, independent cybersecurity risk management program, and potential buyers have expressed concerns about the cybersecurity risks they may be taking on through the potential purchase. In response to those concerns, management might engage a practitioner to examine and report on the cybersecurity risk management program of that division only.

1.41 Chapter 2 discusses in further detail accepting a cybersecurity risk management examination when the cybersecurity risk management examination addresses only a portion of the entity-wide cybersecurity risk management program.

Cybersecurity Risk Management Examination That Addresses Only the Suitability of the Design of Controls (Design-Only Examination)

1.42 There may be circumstances in which management may not be prepared to make an assertion about whether the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives. In such circumstances, rather than making an assertion about whether controls were effective to achieve the entity's cybersecurity objectives, management may make an assertion only about the suitability of the design of controls that have been implemented within the program and engage the practitioner to examine and report on such information.

---

[10] Center for Audit Quality (CAQ) Alert #2014-3, "Cybersecurity and the External Audit," discusses the differences between the scope of IT controls considered in a financial statement audit and a cybersecurity engagement. http://thecaq.org/sites/default/files/caqalert_2014_03.pdf

1.43 In this guide, such an examination is referred to as a *design-only cybersecurity risk management examination* (or a design-only examination) and includes the following two subject matters: (1) the description of the entity's cybersecurity risk management program and (2) the suitably of the design of controls implemented within that program to achieve the entity's cybersecurity objectives. Accordingly, a design-only examination would not provide report users with sufficient information to assess the effectiveness of controls within the entity's cybersecurity risk management program. However, it may be useful to report users who want to obtain an understanding of the entity's cybersecurity risk management program and the key security policies and processes within that program that the entity has implemented to achieve its cybersecurity objectives.

1.44 Chapter 2 discusses circumstances in which a design-only examination might be appropriate and factors that practitioners consider when accepting such an engagement.

Other Engagements Related to Controls Over Security, Availability, Processing Integrity, Confidentiality, or Privacy

1.45 Although the focus of this guide is on a practitioner engaged to perform and report on the cybersecurity risk management examination, there are other engagements a practitioner may be engaged to perform that also address an entity's controls over the security, availability, processing integrity, confidentiality, and privacy of information. This section describes other types of engagements and discusses the differences between them and the cybersecurity risk management examination.

SOC 2 Engagements

1.46 An entity's management is responsible for assessing and addressing risks faced by the entity related to reporting, compliance with laws and regulations, and the efficiency and effectiveness of its operations. When an entity engages a service provider (referred to as a *service organization* in this context) to perform certain processes or functions, the entity (referred to as a *user entity*) exposes itself to additional risks related to the service organization's system. Although management of a user entity can delegate tasks or functions to a service organization, the ownership and responsibility for the product or service provided to customers of the user entity cannot be delegated. Management of the user entity is held responsible by those charged with governance (for example, board members), customers, shareholders, regulators, and other affected parties for establishing effective internal control over outsourced functions.

1.47 To assess and address the risks associated with an outsourced service, management of the user entity needs information about the service organization's controls over the system through which the services are provided. When assessing controls at a service organization that may be relevant to and affect the services provided to user entities, management of a user entity may ask the service organization for a service auditor's report on a description of the service organization's system and the design and operating effectiveness of controls over the service organization's system that may be relevant to the security, availability, or processing integrity of the system or the system's ability to maintain the confidentiality or privacy of the information processed for

user entities. Obtaining a service auditor's report from a service organization provides management of the user entity with information that may be useful in assessing risk but does not relieve the user entity of its responsibilities with regard to an effective system of internal control.

1.48 In a SOC 2 engagement, the service auditor examines and reports on management's description of a service organization's system and the suitability of the design and operating effectiveness of the controls over its system relevant to security, availability, processing integrity, confidentiality, or privacy against the trust services criteria in TSP section 100. AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* provides guidance to service auditors engaged to perform a SOC 2 engagement.

Comparison of a Cybersecurity Risk Management Examination and a SOC 2 Engagement

1.49 Appendix B presents a comparison of the cybersecurity risk management examination with a SOC 2 engagement and related report.

Engagements Under the AICPA Consulting Standards

1.50 In addition to examination engagements, practitioners may be engaged to perform procedures on an entity's cybersecurity risk management program in accordance with CS section 100, *Consulting Services: Definitions and Standards* (AICPA, *Professional Standards*). A nonassurance consulting engagement may provide information and recommendations to management and often precedes an attestation engagement. Practitioners may find the description criteria presented in appendix C, the control criteria presented in appendix D, and the performance and reporting guidance in this guide helpful when conducting such engagements.

Professional Standards

1.51 This guide provides guidance for practitioners performing the cybersecurity risk management examination under the attestation standards. In addition to the performance and reporting guidance in the attestation standards, practitioners performing a cybersecurity risk management examination are required to comply with the requirements of other professional standards, such as professional ethics and quality control standards. This section discusses each of the professional standards that apply to a cybersecurity risk management examination.

Attestation Standards

1.52 AT-C section 105 applies to all engagements in which a practitioner in the practice of public accounting is engaged to issue, or does issue, an attestation report on subject matter or an assertion about subject matter that is the responsibility of another party. AT-C section 205 contains performance, reporting, and application guidance that applies to all examination engagements under the attestation standards. Therefore, a practitioner engaged to perform a cybersecurity risk management examination should comply with all relevant requirements in both of those AT-C sections.

1.53 When a cybersecurity risk management examination is performed for the benefit of a government body or agency, or the practitioner agrees to follow specified government standards, guides, procedures, statutes, rules, or regulations, paragraph .17 of AT-C section 105 requires the practitioner to comply with those governmental requirements as well as with other applicable AT-C sections.

1.54 This guide provides additional application guidance to assist practitioners engaged to perform and report on a cybersecurity risk management examination. Because this guide is an interpretive publication, paragraph .21 of AT-C section 105 requires the practitioner to consider this guidance when planning and performing a cybersecurity risk management examination.

1.55 In some cases, this guide repeats or refers to the requirements in AT-C section 105 and AT-C section 205 when describing those requirements in the context of a cybersecurity risk management examination. Although not all of the requirements in AT-C section 105 and AT-C section 205 are repeated or referred to in this guide, the practitioner is responsible for complying with all relevant requirements contained in those sections.

Code of Professional Conduct

1.56 The AICPA Code of Professional Conduct (code) provides guidance and rules that apply to all members in the performance of their professional responsibilities. The code includes the fundamental principles that govern the performance of all professional services performed by CPAs and, among other things, call for CPAs to maintain high ethical standards and to exercise due care in the performance of all services. When providing attestation services, the "Considering or Subsequent Employment or Association With an Attest Client" subtopic (AICPA, *Professional Standards*, ET sec. 1.279) of the "Independence Rule" also requires CPAs to be independent in both fact and appearance. Independence in a cybersecurity risk management examination is discussed in more detail beginning in paragraph 2.66 of this guide.

Quality in the Cybersecurity Risk Management Examination

1.57 Paragraphs .06–.07 of AT-C section 105 discuss the relationship between the attestation standards and the AICPA quality control standards. Quality control systems, policies, and procedures are the responsibility of a firm when conducting its attestation practice. Under QC section 10, *A Firm's System of Quality Control* (AICPA, *Professional Standards*), a CPA firm has an obligation to establish and maintain a system of quality control to provide it with reasonable assurance that

a. the firm and its personnel comply with professional standards and applicable legal and regulatory requirements and

b. reports issued by the firm are appropriate in the circumstances.

1.58 QC section 10 additionally states that the firm should establish criteria against which all engagements are to be evaluated to determine whether an engagement quality control review should be performed. If the engagement meets the established criteria, the nature, timing, and extent of the engagement quality control review should follow the guidance discussed in that standard and the requirements in paragraph .42 of AT-C section 105.

1.59 Paragraph .33 of AT-C section 105 states that the engagement partner should take responsibility for the overall quality of the attestation engagement, including matters such as client acceptance and continuance, compliance with professional standards, and maintenance of appropriate documentation, among others. As part of those responsibilities, paragraph .32 of AT-C section 105 states that the engagement partner should be satisfied that all members of the engagement team, including external specialists, have the competence and capabilities to perform the engagement in accordance with professional standards. Chapter 2 discusses assessing the competence and capabilities that members of the engagement team need to possess to perform the cybersecurity risk management examination.

Chapter 2

Accepting and Planning a Cybersecurity Risk Management Examination

Management and the practitioner each have specific responsibilities in the cybersecurity risk management examination. This chapter describes the practitioner's responsibilities, including the preconditions of engagement acceptance and the need to obtain a written assertion from and establish an understanding about the terms of the engagement with management. As part of establishing the terms of the engagement, it is helpful for the practitioner to understand management's responsibilities in the engagement; therefore, this chapter also provides a brief overview of management's responsibilities.

Introduction

2.01 Prior to accepting a cybersecurity risk management examination, AT-C section 105, *Concepts Common to All Attestation Engagements* (AICPA, *Professional Standards*), requires the practitioner to determine that certain preconditions are met. Among other things, those preconditions require the practitioner to determine whether the engagement team meets the ethical and competency requirements set forth in the professional standards and whether the engagement meets the relevant requirements of the attestation standards. Prior to engagement acceptance, a practitioner is also required to establish an understanding with management about its responsibilities and those of the practitioner in the cybersecurity risk management examination.

2.02 Once an engagement has been accepted, AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*), sets forth the requirements for developing an overall strategy and planning the engagement. This chapter discusses considerations for accepting and planning the cybersecurity risk management examination.

Understanding Management's Responsibilities

2.03 As previously stated, the practitioner is required to establish, prior to acceptance of the cybersecurity risk management examination, an understanding with management about management's responsibilities and those of the practitioner. This section provides an overview of management's responsibilities.

2.04 Management is responsible for the entity's cybersecurity risk management program, which generally involves the following:

- Identifying the types of information created, used, and stored by the entity and the systems used that are subject to cybersecurity risks
- Identifying the entity's cybersecurity objectives
- Identifying and analyzing the risks that could prevent the entity from achieving its cybersecurity objectives based on the entity's

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

business objectives, including the cyber risks arising from interactions with third parties with access to one or more of the entity's information systems

- Designing, implementing, operating, monitoring, and documenting controls that are effective to achieve the entity's cybersecurity objectives

2.05 Additionally, the practitioner may choose to include in the understanding with management its responsibilities for the following:

- Defining the scope of the engagement, including whether the examination will cover the entity's cybersecurity risk management program or only a portion of that program,[1] and the time frame of the examination[2]
- Selecting the description criteria against which the presentation of the description will be evaluated and the control criteria against which the effectiveness of controls[3] within the cybersecurity risk management program will be evaluated and stating both in management's assertion
- Preparing the description of the entity's cybersecurity risk management program in accordance with the description criteria
- Preparing a written assertion, to accompany the description, about whether
  - — the description is presented in accordance with the description criteria and
  - — the controls were effective to achieve the entity's cybersecurity control objectives based on the control criteria
- Having a reasonable basis[4] for its assertion
- Agreeing to provide the practitioner with the following:
  - — Access to all information of which management is aware, such as records and documentation, including service-level agreements, that is relevant to the description of the entity's cybersecurity risk management program and the assertion
  - — Access to additional information that the practitioner may request from management for the purpose of the cybersecurity risk management examination
  - — Unrestricted access to persons within the entity from whom the practitioner determines it is necessary to

---

[1] Paragraph 2.17 discusses situations in which management may engage the practitioner to examine and report on only a portion of the entity's cybersecurity risk management program.

[2] As discussed in chapter 1, "Introduction and Background," management is responsible for selecting the specified period of time or point of time to be covered by the cybersecurity risk management examination report.

[3] Paragraph 2.24 discusses situations in which management may engage a practitioner to examine and report on only the suitability of the design of controls the entity has implemented within its cybersecurity risk management program.

[4] Determining whether management is likely to have a reasonable basis for its assertion is discussed beginning in paragraph 2.28 of this guide.

obtain evidence relevant to the cybersecurity risk management examination

- Written acknowledgment that internal auditors providing direct assistance will be allowed to follow the practitioner's instructions without management intervention, if the practitioner intends to use internal auditors to provide direct assistance
- Written representations at the conclusion of the engagement, which will include the following:
  - All known matters that might contradict the presentation of the description in accordance with the description criteria or the effectiveness of controls to achieve the cybersecurity objectives
  - Any communication from regulatory agencies or others related to the presentation of the description or effectiveness of controls relevant to the cybersecurity risk management program
  - All deficiencies in internal control relevant to the engagement, of which management is aware
  - Any known actual, suspected, or alleged fraud[5] or noncompliance with laws or regulations affecting the description or the effectiveness of controls
  - Any known events subsequent to the period covered by the engagement up to the date of the practitioner's report that would have a material effect on the description or the effectiveness of controls
  - Other matters the practitioner deems appropriate (for example, discussion of matters considered material)

2.06 Management acknowledges these responsibilities in an engagement letter or other suitable form of written communication.

2.07 Appendix A, "Information for Entity Management," provides further information about management's responsibilities in the cybersecurity risk management examination.

Practitioner's Responsibilities

2.08 During engagement acceptance and planning, the practitioner is responsible for the following:

- Determining whether to accept or continue a cybersecurity risk management examination for a particular client. In making this determination, the practitioner needs to consider whether the preconditions for accepting an examination engagement as discussed in paragraph 2.10 have been met.

---

[5] As defined in paragraph .10 of AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*), fraud is an intentional act involving the use of deception that results in a misstatement in the subject matter or the assertion.

- Establishing an understanding with management regarding the engagement, including the responsibilities of management and the responsibilities of the practitioner. (See paragraph 2.74)
- Reaching an understanding with management regarding their willingness and ability to provide a written assertion at the conclusion of the engagement. (See paragraph 2.65)
- Establishing an overall strategy for the cybersecurity risk management examination that sets the scope, timing, and direction of the engagement and guides the development of the engagement plan, including the consideration of materiality and the identification of the risks of material misstatement. (See paragraph 2.86)
- To support the practitioner's risk assessment procedures, obtaining an understanding of the entity's cybersecurity objectives and how the cybersecurity risk management program is designed, implemented, and operated to achieve those objectives. (See paragraph 2.100)

Accepting or Continuing an Engagement

2.09 In determining whether to accept or continue the engagement, the practitioner should apply the policies and procedures the firm has developed in response to the requirement in paragraph .27 of QC section 10, *A Firm's System of Quality Control* (AICPA, *Professional Standards*). Such policies often include consideration of the integrity and reputation of entity management and significant shareholders or principal owners to determine whether the firm's reputation is likely to suffer by association. Generally, the practitioner will accept or continue a client relationship only after he or she has considered the integrity of entity management, significant shareholders, or principal owners and has no information that would lead the practitioner to believe that the client lacks integrity. Absent such information, a practitioner generally would conclude that it is unlikely that association with the client would expose the practitioner to undue risk of damage to his or her professional reputation or financial loss.

Preconditions of a Cybersecurity Risk Management Examination

2.10 Paragraphs .24–.25 of AT-C section 105 set forth a number of preconditions that should be met before accepting or continuing an attest engagement. In the cybersecurity risk management examination, the practitioner should accept or continue the engagement only if each of the following conditions is met:

a. The practitioner is independent in accordance with the AICPA Code of Professional Conduct. (See paragraph 2.66)

b. Management accepts responsibility for the

  i. preparation of the description of the entity's cybersecurity risk management program in accordance with the description criteria and

  ii. effectiveness of the controls within that program in achieving the entity's cybersecurity objectives.

c. The subject matters of the cybersecurity risk management examination are appropriate.

d. The criteria used to prepare and evaluate the subject matters are both suitable and available to users of the report. (See paragraph 2.42)

e. The practitioner expects to be able to obtain the evidence needed to arrive at his or her opinion on the description and on the effectiveness of controls and will have

i. access to all information relevant to the measurement, evaluation, or disclosure of the subject matter;

ii. access to additional information that he or she may request; and

iii. unrestricted access to entity personnel.

2.11 If one or more of the preconditions in paragraph 2.10 of this guide are not present, the practitioner should discuss the matter with management and attempt to resolve the issue *before* accepting or continuing the engagement. Paragraph .28 of AT-C section 105 provides guidance to a practitioner who discovers, after the engagement is accepted, that one or more of the preconditions are not present.

2.12 In addition to the preconditions discussed in paragraph 2.10 of this guide, the practitioner should accept or continue a cybersecurity risk management examination only when the practitioner has

a. no reason to believe that relevant ethical requirements (including independence) in the AICPA Code of Professional Conduct will not be satisfied. (See paragraph 2.66)

b. determined that the individuals performing the engagement have the appropriate competence and capabilities to perform it. (See paragraph 2.70)

c. reached an understanding with the engaging party about the terms of the engagement. (See paragraph 2.74)

d. plans to include a written opinion expressed in the practitioner's report included in the cybersecurity risk management examination report. (Chapter 4, "Forming the Opinion and Preparing the Practitioner's Report," of this guide discusses reporting in a cybersecurity risk management examination.)

2.13 Because of the immaturity of many entities' cybersecurity risk management programs, management may not have realistic expectations about the performance of the engagement and the conclusions the practitioner will express at the end of the engagement. This is particularly true when there is a likelihood that the practitioner's opinion (on the description, the effectiveness of controls, or both) may require qualification or other modification because of the lack of appropriate controls or sufficient appropriate evidence. During engagement acceptance, the practitioner may wish to discuss these factors with management in order to assist management in forming its expectations.

2.14 The practitioner may also wish to consider whether management is experiencing excessive pressure that may affect its actions during the course of the engagement. For example, such pressure may arise from a transaction that is contingent upon the receipt of an unmodified practitioner's opinion by a certain date. In such a situation, management may be under pressure to not fully disclose all relevant information to the practitioner. In response, the

practitioner may decline to accept the engagement or may conclude that the increase in attestation risk resulting from such pressures warrants modification of the nature, timing, and extend of the practitioner's procedures to address the risks.

Determining Whether the Subject Matter is Appropriate for the Cybersecurity Risk Management Examination

2.15 Determining whether the subject matter is appropriate in the specific cybersecurity risk management examination involves consideration of the following:

- When management has requested that the subject matter of the engagement be less than the entity-wide program, whether information about only a portion of the entity's cybersecurity risk management program is likely to meet the needs of report users
- When management has requested that, in addition to the description, the subject matter of the engagement only be the suitability of the design of controls implemented by the entity, whether information about only the suitability of design of controls within the entity's cybersecurity risk management program is likely to meet the needs of report users
- Whether management is likely to have a reasonable basis for its assertion

2.16 As previously stated, there are two distinct but complementary subject matters in the cybersecurity risk management examination: (1) the description of the entity's cybersecurity risk management program and (2) the effectiveness of the controls within that program in achieving the entity's cybersecurity objectives. When determining whether the subject matters of the engagement are appropriate in the particular circumstances, the practitioner may consider factors such as whether

- users of the cybersecurity risk management examination report are likely to understand other factors related to the engagement, such as the nature of the engagement.
- the description criteria used to evaluate the presentation of the description can be understood by the users.
- the effect of third parties (customers, vendors, business partners, and others) with access to the entity's systems on the entity's cybersecurity risks is addressed by the cybersecurity risk management program and can be understood by the users.
- the control criteria used to evaluate the effectiveness of controls can be understood by the users.
- the period of time over which the engagement is to be performed will meet the information needs of the users.

If report users are unlikely to understand these factors or the period covered will not meet their needs, a greater potential exists for them to misunderstand the report. Consequently, the practitioner may decide not to accept the engagement or to restrict the use of the report.

Determining Whether the Subject Matter of the Engagement is Appropriate When the Cybersecurity Risk Management Examination Addresses Only a Portion of the Entity's Cybersecurity Risk Management Program

2.17 Management is responsible for determining whether the cybersecurity risk management examination will be performed on the entity-wide cybersecurity risk management program or on only a portion of that program. When making this determination, management needs to obtain an understanding of the needs of intended users of the cybersecurity risk management examination report to determine whether the subject matters of the engagement are likely to meet their needs.

2.18 As discussed in chapter 1, "Introduction and Background," although the cybersecurity risk management examination discussed in this guide usually addresses an entity-wide cybersecurity risk management program, there may be circumstances in which management may engage the practitioner to examine and report on only a portion of that program. The cybersecurity risk management examination may be limited to any of the following:

- One or more specific business units, segments, or functions of an entity
  - — when those units, segments, or functions operate under an *entity-wide* cybersecurity risk management program; or
  - — when those units, segments, or functions operate under an *independent* cybersecurity risk management program
- One or more specific types of information used by the entity

2.19 For example, an entity plans to sell a particular division of its business that operates under a separate, independent cybersecurity risk management program, and potential buyers have expressed concerns about the cybersecurity risks they may be taking on through the purchase. In response to those concerns, management might engage a practitioner to examine and report on the cybersecurity risk management program of that division only.

2.20 Paragraph .25 of AT-C section 105 indicates that one of the preconditions for accepting an attestation engagement is that the subject matter is appropriate for the engagement. Paragraph .A41 of AT-C section 205 provides guidance useful to a practitioner if management engages the practitioner to examine a portion of the entity's cybersecurity risk management program, as described in paragraph 2.17. If the practitioner has concerns about whether a report addressing only a portion of the entity's cybersecurity risk management program is likely to meet the information needs of the intended users, the practitioner may decide not to accept the engagement. If the practitioner decides to accept the engagement, he or she may consider whether there is a risk that the report may be misunderstood by all but a limited number of report users. In that case, the practitioner may decide to restrict the use of the report to those limited users.

2.21 In the example described in paragraph 2.19, it would be reasonable for a practitioner to conclude that a cybersecurity risk management examination report addressing only the cybersecurity risk management program of the

division to be sold is an appropriate subject matter for the engagement because such a report is likely to meet the informational needs of the potential buyers of the division. But the practitioner would likely conclude that the use of the report should be restricted to such buyers.

2.22 In making a determination about whether the subject matter is appropriate, the practitioner may become aware of information that causes him or her to believe management has limited the scope of the examination because of its belief that an examination of the entity-wide cybersecurity risk management program would result in a qualified or adverse opinion (on the description, the effectiveness of controls, or both). If the practitioner believes that users of the report are likely to misunderstand the limitation on the scope of the engagement and, as a result, the cybersecurity risk management examination report because of the omission of relevant factors regarding the entity's overall cybersecurity risk management program, the practitioner may determine not to accept the engagement.

2.23 When the cybersecurity risk management examination will address only a portion of the entity's cybersecurity risk management program, the language used in management's assertion and in the practitioner's report should be tailored to reduce the risk of misunderstanding by report users by clearly identifying the portion of the entity's cybersecurity risk management program addressed in the examination.

Determining Whether the Subject Matter is Appropriate When the Examination Addresses Only the Suitability of the Design of Controls Within the Entity's Cybersecurity Risk Management Program (Design-Only Examination)

2.24 As discussed in chapter 1, there may be circumstances in which management may not be prepared to make an assertion about whether the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives. In such circumstances, rather than making an assertion about whether controls were effective to achieve the entity's cybersecurity objectives, management may make an assertion about the suitability of the design of controls within the program.

2.25 Such an examination, referred to in this guide as a design-only cybersecurity risk management examination (design-only examination), would include the following two subject matters: (1) the description of the entity's cybersecurity risk management program and (2) the suitably of design of the controls implemented within that program to achieve the entity's cybersecurity objectives. Accordingly, a design-only examination would not provide report users with sufficient information to assess the effectiveness of controls within that program. However, the resulting report (design-only report) may be useful to report users who want to obtain an understanding of the entity's cybersecurity risk management program and an overview of the security policies and processes implemented within that program.

2.26 The following are circumstances in which a design-only report might be useful:

- The entity's cybersecurity risk management program has not been in operation for a sufficient length of time to enable the practitioner to gather sufficient appropriate evidence about the

effectiveness of controls to achieve the entity's cybersecurity risk management program.

- The entity has recently made significant changes to its cybersecurity risk management program and the controls within that program and does not have a sufficient history with a stable program to enable an opinion on the effectiveness of controls to achieve the entity's cybersecurity risk management program.

2.27 Before accepting such an engagement, the practitioner should consider the informational needs of report users and whether such users may potentially misunderstand the practitioner's opinion on the description and design only. The practitioner may consider restricting the use of a design-only report to board members, management, others within the organization, and specific third parties (specified parties) who are likely to understand it.

Determining Whether Management is Likely to Have a Reasonable Basis for the Assertion

2.28 Paragraph 2.10 indicates that, as one of the preconditions of the cybersecurity risk management examination, the practitioner should determine whether the subject matters are appropriate for the engagement. According to paragraph .A36 of AT-C section 105, one element of the appropriateness of the subject matters is the existence of a reasonable basis for measuring or evaluating the subject matters.

2.29 Management is responsible for having a reasonable basis for its assertion about the description and the effectiveness of controls within that program. Furthermore, because management's assertion generally addresses the effectiveness of controls over a period of time, management's basis for its assertion covers the same time frame.

2.30 The attestation standards do not require the practitioner to perform specific procedures to determine whether management has a reasonable basis for its assertion. However, because of the relationship between the monitoring and assessment of controls and their effectiveness in achieving the entity's cybersecurity objectives, the practitioner ordinarily discusses with management the basis for its assertion prior to engagement acceptance. This will assist the practitioner in determining whether the basis appears reasonable for the size and complexity of the entity's cybersecurity risk management program and whether the practitioner expects to be able to obtain sufficient appropriate evidence to arrive at his or her opinion (on the description, the effectiveness of controls, or both), which is also a precondition of the examination.

2.31 In the cybersecurity risk management examination, the practitioner's consideration of whether management has a reasonable basis for its assertion is likely to be more challenging than in other types of examination engagements. That is because of

- the evolving nature of most entities' cybersecurity risk management programs;
- the nature and complexity of risks those programs are designed to address and the evolving nature of those risks; and
- the breadth and complexity of the subject matter.

The remainder of this section discusses additional considerations when evaluating whether management has a reasonable basis for its assertion in a cybersecurity risk management examination.

2.32 The implementation of an effective cybersecurity risk management program is a significant endeavor for most entities, requiring the design and operation of technology solutions and complex processes and procedures, including those governing interactions with third parties (customers, vendors, business partners, and others) and their information systems. Because of these complexities, controls within the entity's cybersecurity risk management program are unlikely to be effective without regular monitoring and assessment of controls. Therefore, monitoring and assessment of controls is ordinarily a key component of management's basis for its assertion.

2.33 For those reasons, management generally will need to perform a formal assessment of the effectiveness of its controls to make its assertion. In most cases, during the assessment process, management will do the following:

a. Evaluate the effectiveness of the entity's procedures for identifying
   i. cybersecurity objectives based on the entity's business objectives (for instance, delivery of services, production of goods, or protection of assets);
   ii. information and other assets of the entity at risk, based on the scope of the engagement and defined cybersecurity objectives; and
   iii. the threats to the information and other assets based on internal and external threat intelligence data, inherent vulnerabilities of information assets and other assets, and the linkages between such vulnerabilities and identified threats.

b. Evaluate the effectiveness of the processes it uses to design and implement controls to mitigate risks. Evaluating the effectiveness of such processes may involve comparing the results of monitoring activities and reviewing the results of independent assessments and other activities designed to continuously improve controls based on lessons learned from security events.

c. Assess the effectiveness of controls, particularly controls that monitor the effectiveness of other controls, to provide reasonable assurance of achieving the entity's cybersecurity objectives. (This is particularly important when aspects of the entity's cybersecurity risk management program controls have been outsourced to service providers. Paragraph 2.37 further discusses third-party considerations.)

2.34 In addition to the factors discussed in paragraph 2.31, the effectiveness of the entity's cybersecurity controls is highly dependent on the existence of an accurate and complete inventory of the entity's information assets[6] and standard acquisition processes and configuration settings. If these do not exist,

[6] As used in this guide, the term *information assets* refers to data and associated software and infrastructure used to process, transmit, and store information. Examples of information assets include employees' personally identifiable information, protected health information, customers' credit card information, and the systems that process, transmit, and store such information.

it may be difficult, or even impossible, for management to have a reasonable basis for its assertion.

2.35 Management's basis for its assertion usually relies heavily on monitoring of controls. Such monitoring activities typically include ongoing activities, separate evaluations, or a combination of the two. Ongoing monitoring activities are ordinarily built into the normal recurring activities of an entity's cybersecurity risk management program and include activities such as the regular review by management of key system reports and participation in incident management processes. In addition, monitoring activities may include the periodic evaluations of controls through (*a*) assessments performed by the internal audit function or by knowledgeable personnel who are independent of the function being evaluated, (*b*) performance of penetration testing, and (*c*) review of reports of independent certifications made against established specifications (for example, International Standardization Organization and International Electrotechnical Commission [ISO/IEC] Standard 27001 and HITRUST CSF). When such monitoring activities do not exist or they appear to be inadequate, it may be difficult for management to have a reasonable basis for its assertion.

2.36 Management generally documents the assessment in a variety of ways, such as through the use of policy manuals, narratives, flowcharts, decision tables, procedural write-ups, or questionnaires. The nature and extent of documentation usually varies, depending on the size and complexity of the entity and its monitoring activities.

Consideration of Third Parties

2.37 Monitoring activities are of increased importance if the entity has identified cybersecurity threats and vulnerabilities arising from interactions with third parties. As used in this guide, third parties include customers, vendors, business partners, and others who have access to one or more of the entity's information systems, store confidential entity information on their systems, or otherwise transmit information back and forth between, or on behalf of, the entity.

2.38 Therefore, it is important for management to assess the cybersecurity risks arising from interactions with third parties, particularly when third parties operate controls necessary to achieve the entity's cybersecurity objectives.

2.39 If management determines the risks associated with third parties are likely to be material to the achievement of the entity's cybersecurity objectives (for example, due to the nature of access the third party has to the entity's systems and information assets, or because of the controls the third party operates on behalf of the entity), monitoring controls at the entity are needed to allow management to determine whether the processes and controls performed by the third parties effectively address the identified risks. Such monitoring controls may include, but are not limited to, a combination of the following:

- Conducting assessments of whether third-party contractual agreements are in accordance with the entity's policies
- Conducting periodic discussions with third parties and their employees
- Inspecting completed third-party security questionnaires and submitted documents to support their responses

- Conducting regular site visits to the third parties' locations to observe the execution of controls
- Inspecting results of internal audit tests over the third parties' controls
- Inspecting type 2 SOC 2 reports on aspects of the third parties' operations that relate to their security, availability, and confidentiality controls pursuant to AT-C section 205

2.40 Management is responsible for the effectiveness of all of the processes and controls related to the entity's cybersecurity risk management program, regardless of who performs the specific processes and controls. Therefore, unless management has processes and controls that monitor the effectiveness of the processes and controls performed by third parties, it may be difficult for management to have a reasonable basis for its assertion. For that reason, the practitioner ordinarily would discuss with management the use of third parties, including the nature and extent of the entity's monitoring controls, to determine whether such controls are likely to be sufficient in the circumstances. If adequate monitoring controls do not exist, or if the practitioner believes that such controls are unlikely to be effective, it is unlikely that management would have a reasonable basis for making its assertion.

2.41 If the practitioner believes that management does not have reasonable basis for its assertion, or that sufficient appropriate evidence to support the basis is unlikely to be available, the practitioner should not accept or continue the engagement.

Assessing the Suitability and Availability of Criteria and the Related Cybersecurity Objectives

2.42 As discussed in chapter 1, two distinct sets of criteria are used in the cybersecurity risk management examination: description criteria and control criteria. As stated in paragraph 2.05, management is responsible for selecting the criteria to be used in the cybersecurity risk management examination. Management may select any description and control criteria that are suitable and available to intended users.

2.43 According to paragraph .A42 of AT-C section 105, criteria are suitable when they exhibit all of the following characteristics:

- *Relevance.* Criteria are relevant to the subject matter.
- *Objectivity.* Criteria are free from bias.
- *Measurability.* Criteria permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
- *Completeness.* Criteria are complete when subject matters prepared in accordance with them do not omit relevant factors that could reasonably be expected to affect decisions of the report users made on the basis of that subject matter.

The relative importance of each characteristic to a particular engagement is a matter of professional judgment.

2.44 Criteria also need to be available to report users to allow them to understand how the entity has prepared its description and evaluated the effectiveness of controls in achieving the entity's cybersecurity objectives. Criteria

that are available publicly, included in the description, or included in the practitioner's report are all considered available to report users. Sometimes, criteria are available only to certain report users; in this case, the practitioner's report should include an alert restricting the use of the report to those parties, as required by AT-C section 205.

Description Criteria

2.45 Appendix C, "Description Criteria for Use in the Cybersecurity Risk Management Examination" of this guide presents description criteria that may be used by management when preparing and evaluating the description of the entity's cybersecurity risk management program and by the practitioner when evaluating that description. Applying the description criteria in actual situations requires judgment. Therefore, in addition to the description criteria, appendix C presents implementation guidance for each criterion. The implementation guidance presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. The implementation guidance does not address all possible situations; therefore, users should carefully consider the facts and circumstances of the entity and its environment in actual situations when applying the description criteria.

2.46 The description criteria in appendix C were promulgated by the Assurance Services Executive Committee (ASEC), which is designated by the Council of the AICPA under the AICPA Code of Professional Conduct to issue measurement criteria. Therefore, such criteria are considered suitable for use in the cybersecurity risk management examination. Because the description criteria are published by the AICPA and made available to the general public, they are considered available to report users. Therefore, the description criteria are both suitable and available criteria for the cybersecurity risk management examination.

2.47 The performance and reporting guidance in this guide assumes the use of the criteria presented in appendix C as the description criteria. However, as cybersecurity services continue to evolve, other description criteria may be developed. If management believes that other description criteria are suitable (that is, that other criteria exhibit the characteristics of suitable criteria in paragraph 2.43), management could select and use such criteria when developing and assessing the presentation of the description in the cybersecurity risk management examination. However, prior to accepting a cybersecurity risk management examination in which other criteria will be used, the practitioner is responsible for determining whether or not he or she agrees with management's assessment about the suitability of the other criteria. In making his or her determination about the relevance, objectivity, measurability, and completeness of management's selected description criteria, the practitioner may find it useful to compare the other description criteria identified by management to the description criteria in appendix C.

Control Criteria

2.48 When selecting the control criteria to be used in the evaluation of the effectiveness of controls within the entity's cybersecurity risk management program, management may select any suitable control criteria. Management may select the criteria for security, availability, and confidentiality categories in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), as the

control criteria. The trust services criteria for security, availability and confidentiality are presented in appendix D, "Trust Services Criteria for Security, Availability, and Confidentiality for Use as Control Criteria in the Cybersecurity Risk Management Examination" of this guide.

2.49 Applying the trust services criteria in actual situations requires judgment. Therefore, in addition to the trust services criteria, appendix D also presents points of focus for each criterion. The Committee of Sponsoring Organizations of the Treadway Commission (COSO), in their 2013 *Internal Control—Integrated Framework* (COSO framework), states that points of focus represent important characteristics of the criteria. Consistent with the COSO framework, the points of focus in appendix D may assist management when designing, implementing, and operating controls over security, availability, and confidentiality. In addition, the points of focus may assist both management and the practitioner when evaluating whether the controls were suitably designed and operated to meet the entity's cybersecurity risk management objectives based on the trust services criteria.

2.50 The trust services criteria for security, availability, and confidentiality in appendix D were promulgated by the ASEC. The ASEC has determined that the trust services criteria for security, availability, and confidentiality are suitable for use in the cybersecurity risk management examination. Because they are also made available to general users, the control criteria are both suitable and available criteria for the cybersecurity risk management examination.

2.51 The performance and reporting guidance in this guide assumes the trust services criteria presented in appendix D are used as the control criteria, and all references hereafter to control criteria refer to the trust services criteria for security, availability, and confidentiality. Thus, examples and illustrations throughout the guide are based on these criteria. A practitioner engaged to perform a cybersecurity risk management examination in which other description or control criteria will be used should adapt this guidance as appropriate.

2.52 If management selects different criteria as the control criteria, the practitioner is responsible for determining whether he or she agrees with management's assessment about the suitability and availability of the other control criteria. When making that determination, the practitioner should consider whether the other control criteria selected by management are relevant to the subject matter, objective, consistently measureable, and complete, as discussed in paragraph 2.43.

2.53 When considering whether the other control criteria are suitable for the engagement, the practitioner may find it helpful to compare the control criteria selected by management to the trust services criteria to determine whether the control criteria selected by management address substantially the same aspects of the entity's cybersecurity risk management program as the trust services criteria for security, availability, and confidentiality.

2.54 If the practitioner determines that the selected criteria are not suitable, the practitioner typically works with management of the entity to identify suitable criteria. If management refuses to select suitable and available criteria for the engagement, the practitioner should not accept or continue the engagement.

Assessing the Suitability of the Entity's Cybersecurity Objectives

2.55 As discussed in chapter 1, the achievement of the entity's overall business objectives depends upon the identification, assessment, and management of the risks that threaten their achievement. One type of risk is the entity's cybersecurity risks. Consequently, entities often establish sub-objectives, known as *cybersecurity objectives*, that address their specific cybersecurity risks. Similar to the entity's overall business objectives, the cybersecurity objectives established by management need to be suitable to enable both management and the practitioner to evaluate whether controls within the entity's cybersecurity risk management program are effective to achieve those objectives.

2.56 Management is responsible for establishing, and including in the description, suitable cybersecurity objectives to enable report users to understand the context in which the entity's cybersecurity risk management program operates. Because control activities are designed and operated to address the risks that would prevent an entity's cybersecurity objectives from being achieved, the practitioner is responsible for evaluating whether the cybersecurity objectives established by management are suitable to permit the practitioner to form a conclusion on the effectiveness of controls based on the control criteria. In making that evaluation, the practitioner should consider the attributes of suitable objectives described in the COSO framework. According to the COSO framework, suitable objectives are

- *specific.* The objectives provide a clear understanding of the cybersecurity risks that need to be mitigated.
- *measurable or observable.* The objectives permit an objective determination about whether each cybersecurity objective has been met.
- *attainable.* The objectives permit the implementation of controls that, if suitably designed and operated effectively, provide reasonable assurance of achieving each objective.
- *relevant.* The achievement of each cybersecurity objective supports the entity's efforts to achieve its overall objectives.
- *time-bound.* The objectives reflect the desired operation of cybersecurity controls over time.

2.57 As discussed earlier, cybersecurity objectives are established to address the cybersecurity risks that could otherwise threaten the achievement of the entity's overall objectives. Consequently, in establishing the entity's cybersecurity objectives, management also considers whether the cybersecurity objectives completely address those risks. Because the achievement of the entity's overall objectives depends on the achievement of the cybersecurity objectives, the cybersecurity objectives also need to meet one additional attribute: completeness. To be complete, the set of cybersecurity objectives established by management needs to address the significant cybersecurity risks that threaten the achievement of the entity's overall business objectives.

2.58 Management is likely to establish cybersecurity objectives that address several basic matters, regardless of the nature of the business and the industry in which the entity operates. Basic matters that management may consider when establishing the entity's cybersecurity objectives include the following:

- Commitments made to third parties (customers, vendors, business partners, and others) related to the security and availability of information and systems, including commitments related to critical infrastructure and extended supply chains
- Laws and regulations to which the entity is subject as a result of the types of information it possesses or uses (for instance, protected health information and personally identifiable information)
- Commitments made as part of a certification and authorization process for government agencies and other parties
- Industry standards to which the entity is subject as a result of the types of information it uses (for instance, Payment Card Industry Data Security Standards for entities that accept or process credit card transactions)
- Other business initiatives

2.59 To assist management with the development and disclosure of the entity's cybersecurity objectives, description criterion 3 (*The entity's principal cybersecurity risk management program objectives [cybersecurity objectives] related to availability, confidentiality, integrity of data, and integrity of processing*), presented in appendix C, includes as implementation guidance the following example of cybersecurity objectives an entity might establish:

Availability

Enabling timely, reliable, and continuous access to and use of information and systems to do the following:

- Comply with applicable laws and regulations
- Meet contractual obligations and other commitments
- Provide goods and services to customers without disruption
- Safeguard entity assets and assets held in custody for others
- Facilitate decision making in a timely manner

Confidentiality

Protecting information from unauthorized access and disclosure, including means for protecting proprietary information and personal information subject to privacy requirements, to do the following:

- Comply with applicable laws and regulations
- Meet contractual obligations and other commitments
- Safeguard the informational assets of an entity

Integrity of Data

Guarding against improper information modification or destruction of information to support the following:

- The preparation of reliable financial information for external reporting purposes
- The preparation of reliable information for internal use

- Information nonrepudiation and authenticity
- The completeness, accuracy, and timeliness of processing
- Management holding employees and users accountable for their actions
- The operation of processes addressing the privacy of personal information

Integrity of Processing

Guarding against improper use, modification, or destruction of systems to support the following:

- The accuracy, completeness, and reliability of information, goods, and services produced
- The safeguarding of entity assets
- The safeguarding of life and health

2.60 In the cybersecurity risk management examination, management would tailor those cybersecurity objectives to reflect the entity's business objectives based on the nature of the business and the industry in which it operates, the entity's mission and vision, and the entity's cybersecurity risk appetite.

2.61 Because of the close relationship among the entity's cybersecurity objectives, the practitioner's opinion on the effectiveness of controls, and report users' understanding of the practitioner's opinion, the practitioner should consider whether the cybersecurity objectives are suitable and complete. If the practitioner believes that the cybersecurity objectives established by management are not suitable and complete, the practitioner should discuss the matter with management. If management is unwilling to revise the cybersecurity objectives to address the practitioner's concerns, the practitioner may decide (*a*) to refuse to accept the engagement or (*b*) to restrict the use of the report to those users who are able to understand the risks not addressed by the entity's cybersecurity objectives. Chapter 3, "Performing the Cybersecurity Risk Management Examination," discusses the situation when, after accepting the engagement, the practitioner obtains evidence that causes him or her to believe that the entity's cybersecurity objectives are not suitable for the engagement.

Requesting a Written Assertion and Representations From Management

2.62 Paragraph .10 of AT-C section 205 requires the practitioner to request a written assertion from the responsible party that addresses both subject matters in the cybersecurity risk management examination. Specifically, the assertion addresses whether (1) the description is presented in accordance with the description criteria and (2) the controls within the program were effective to achieve the entity's cybersecurity objectives.

2.63 Management's assertion is included in the cybersecurity risk management examination report along with management's description and the practitioner's report. Because of the important role that the assertion plays in the engagement, it may be useful for the practitioner to provide management with an example of a written assertion prior to engagement acceptance. Such an example can be found in appendix E, "Illustrative Management Assertion in the Cybersecurity Risk Management Examination."

2.64 If management refuses to provide a written assertion, paragraph .82 of AT-C section 205 requires the practitioner to withdraw from the engagement when withdrawal is possible under applicable laws and regulations.[7] Consequently, it is important to obtain management's agreement to provide the written assertion prior to engagement acceptance. If law or regulation does not allow the practitioner to withdraw, the practitioner should disclaim an opinion on the description and the effectiveness of controls.

2.65 Management is also required to provide the practitioner with written representations at the conclusion of the engagement. It may be useful for the practitioner to provide management with an example of the expected representations prior to engagement acceptance.

Considering Practitioner Independence

2.66 Paragraph .24 of AT-C section 105 and paragraph .06 of AT-C section 205 state that a practitioner must be independent when performing an attestation engagement such as the cybersecurity risk management examination. The only exception to this requirement is when the practitioner is required by law or regulation to accept the engagement and report on the subject matter. In that case, practitioner is required to disclaim an opinion on the description and the effectiveness of controls and to specifically state in the report that the practitioner is not independent.

2.67 The "Independence Rule" (ET sec. 1.200.001)[8,9] of the AICPA Code of Professional Conduct establishes independence requirements for attestation engagements. The "Independence Standards for Engagements Performed in Accordance with Statements on Standards for Attestation Engagements" subtopic (ET sec. 1.297) of the "Independence Rule" establishes special independence requirements for a practitioner who provides services under the attestation standards. In addition, the "Conceptual Framework Approach" subtopic (ET sec. 1.210) of the "Independence Rule" discusses threats to independence not specifically detailed elsewhere. The code specifies that, in some circumstances, no safeguards can reduce an independence threat to an acceptable level. For

---

[7] If management is not the engaging party, paragraph .10 of AT-C section 205 provides an exception to the requirement that the practitioner withdraw from the engagement when management refuses to provide a written assertion. Because a written assertion is one of three key elements of the cybersecurity risk management examination report, that exception does not apply in the examination described in this guide. Therefore, management's failure to provide a written assertion would prevent the practitioner from performing the cybersecurity risk management examination.

[8] All ET sections can be found in AICPA *Professional Standards*.

[9] The "Independence Rule" (ET sec. 1.200.001) and its interpretations apply to all attest engagements. However, when performing engagements in which independence is required in accordance with the attestation standards, the covered member needs to be independent with respect to the responsible party(ies), as defined in those standards. If the individual or entity that engages the covered member is not the responsible party, the covered member need not be independent of that individual or entity. However, the covered member should consider the "Conflicts of Interest" interpretation (ET sec. 1.110.010) of the "Integrity and Objectivity Rule" with regard to any relationships that may exist with the individual or entity that engages the covered member to perform these services. When providing nonattest services that would otherwise impair independence under the interpretations of the "Nonattest Services" subtopic (ET sec. 1.295) of the "Independence Rule," threats would be at an acceptable level and independence would not be impaired if the following safeguards are met:

- Nonattest services do not relate to the specific subject matter of the attestation engagement.
- The "General Requirements for Performing Nonattest Services" interpretation (ET sec. 1.295.040) of the "Independence Rule" are met when providing the nonattest service.

example, the code specifies that a covered member may not own even an immaterial direct financial interest in an attest client because there is no safeguard to reduce the self-interest threat to an acceptable level. A member may not use the conceptual framework to overcome this prohibition or any other prohibition or requirement in an independence interpretation.

2.68 When assessing independence in a cybersecurity risk management examination, the practitioner might consider matters including, but not limited to, (*a*) advisory work performed for the client that may directly or indirectly affect the entity's cybersecurity risk management program, (*b*) fee arrangements for all services provided to the client, (*c*) firm and individual financial relationships, (*d*) firm business relationships, and (*e*) alumni and familial relationships with the client and client personnel. Because of the breadth of a cybersecurity risk management program and its relationship to all aspects of information technology, the practitioner needs to be particularly attentive to other services provided to the entity that may impair independence.

2.69 It is anticipated that, in most cybersecurity risk management examinations, management will be both the engaging party (client) and the responsible party; thus, management will accept responsibility for the description of the entity's cybersecurity risk management program and its assertion about the effectiveness of the controls within that program. In some engagements, however, the engaging party may be someone other than management. For example, in a proposed acquisition, the engaging party might be the party interested in acquiring the entity. As part of its due diligence on the target company, the engaging party might want information about the entity's cybersecurity risk management program to evaluate the additional risks the engaging party might be taking on in the event of a security breach at the entity. In such a situation, the practitioner is not required to be independent of the engaging party; however, the Code of Professional Conduct requires the practitioner to consider the applicable interpretation regarding conflicts of interest prior to accepting the engagement.

Considering the Competence of Engagement Team Members

2.70 Chapter 1 of this guide discusses quality in the cybersecurity risk management examination. Maintaining appropriate quality in the engagement involves having the work performed by engagement team members with the appropriate competence and capabilities. For that reason, as discussed in paragraph 2.12, the practitioner should not accept the cybersecurity risk management examination unless he or she has determined that the individuals performing the particular engagement have the appropriate competence and capabilities to perform it.

2.71 When considering the competence and capabilities of engagement team members, the engagement partner should consider whether the team assigned to the engagement collectively has, or can acquire, the following:

- An understanding, or the ability to obtain an understanding, of information security or cybersecurity risk management examinations gained through experience with engagements of a similar nature and complexity or through appropriate training and participation

- Knowledge of the entity's industry and business, including whether the industry in which the entity operates is subject to specific types of or unusual cybersecurity risks
- Knowledge of relevant IT systems and technology, such as but not limited to mainframes, networking, firewalls or firewall techniques, security protocols, and operating systems
- Knowledge of any uncommon technologies or industry-specific technology used by the entity
- An understanding of IT processes and controls, such as the management of operating systems, networking, and virtualization software and related security techniques; security principles and concepts; software development; and incident management and information risk management
- Experience with evaluating the effectiveness of controls an entity has designed and implemented
- An understanding of professional standards and the ability to apply professional skepticism and judgment in the cybersecurity risk management examination
- An understanding of legal and regulatory requirements that are relevant to the cybersecurity risk management examination

2.72 In addition, the engagement partner should make sure that team members are informed of their responsibilities, including the objectives of the procedures that they are to perform and matters that may affect the nature, timing, and extent of such procedures. The engagement partner should also be satisfied that engagement team members have been directed to bring to his or her attention any significant questions raised during the engagement.

2.73 The engagement partner may decide to supplement the knowledge and skills of the engagement team with the use of specialists. Planning to use the work of a practitioner's specialist is discussed in paragraph 2.139.

Establishing the Terms of the Engagement

2.74 Paragraph .07 of AT-C section 205 requires the practitioner to agree on, and document in a written communication, the terms of the engagement with the engaging party. Such a written communication reduces the risk that either the practitioner or management (who generally is the engaging party in the cybersecurity risk management examination) may misinterpret the needs or expectations of the other party. For example, it reduces the risk that management may intend to rely on the practitioner work to protect the entity against certain risks or to perform certain management functions. In addition, the practitioner's preliminary understanding of the terms of the cybersecurity risk management examination enables the practitioner to identify whether there are any indications that either the scope of the engagement or the criteria to be used in the examination are unlikely to meet the information needs of report users.

2.75 According to paragraph .08 of AT-C section 205, the agreed-upon terms of the engagement should include, at a minimum, the following:

a. The objective and scope of the engagement

b. The responsibilities of the practitioner

c. A statement that the engagement will be conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants

d. The responsibilities of management and the responsibilities of the engaging party, if different

e. A statement about the inherent limitations of the cybersecurity risk management examination

f. Identification of the description criteria against which management's description will be evaluated and the control criteria against which the effectiveness of the controls within the cybersecurity risk management program will be evaluated

g. An acknowledgment that management (and the engaging party, if other than management) agrees to provide the practitioner with a representation letter at the conclusion of the engagement

2.76 In addition to these matters, the practitioner may decide to include other matters in the understanding, such as the identification of the entity's cybersecurity objectives. Additional matters that may affect the practitioner's understanding of the terms of the engagement and how the terms should be documented in a recurring engagement are discussed in paragraph .09 of AT-C section 205.

2.77 Paragraph .07 of AT-C section 205 states that the understanding with management should be documented in sufficient detail in an engagement letter or other appropriate form of written communication.

2.78 In certain circumstances, a practitioner is required by paragraph .64 of AT-C section 205 to include in his or her report an alert that restricts the use of the report to specified parties. In other circumstances, the practitioner may elect to restrict the use of the report, even though standards do not require it. An alert is designed to avoid misunderstandings related to the use of the report, particularly if the report is taken out of the context in which the report is intended to be used. If an alert is expected to be included in the cybersecurity risk management examination report, the practitioner may decide to inform management (and the engaging party, if different) and specified parties (and document in the engagement letter) that the report is not intended for distribution to parties other than those specified in the report. Nevertheless, a practitioner is not responsible for controlling, and cannot control, the distribution of his or her report after its release.

2.79 If the practitioner plans to use internal auditors to provide direct assistance, paragraph .41 of AT-C section 205 states that, prior to doing so, the practitioner should obtain written acknowledgment from management that internal auditors providing direct assistance to the practitioner will be allowed to follow the practitioner's instructions and that management will not interfere in the performance of the internal auditors' work. The practitioner may decide to document that acknowledgment in the engagement letter.

2.80 If management is the engaging party and refuses to sign the engagement letter, the practitioner should decline to accept or perform the cybersecurity risk management examination, unless withdrawal is not allowed by applicable law or regulation.

Accepting a Change in the Terms of the Engagement

2.81 After the engagement agreement is executed but prior to the completion of the engagement, management may communicate a desire to change the scope of the engagement. When management requests a change in the scope of the engagement, paragraph .29 of AT-C section 105 states that the practitioner should not agree to the change in the terms of the engagement unless there is reasonable justification for the change. Reasonable justification may exist for changes to the terms of the engagement requested as a result of the following:

- Misunderstanding concerning the nature of the engagement originally requested
- Change in the needs of users of the cybersecurity risk management examination report
- Change in the intended users of the report

2.82 As an example, there may be reasonable justification for management's request to change the scope of an engagement, which was originally the entity-wide cybersecurity risk management program, by excluding from that scope the controls designed and operated at a division of the entity in the process of being sold, when the report is intended only for the use of board members.

2.83 Other changes to the scope of the engagement, however, may not be considered reasonable if they relate to information that is incorrect, incomplete, or otherwise unsatisfactory. An example of such a situation is a request to change the scope of the cybersecurity risk management examination from the entity-wide cybersecurity risk management program to only a portion of the entity-wide program to avoid a modified opinion on the effectiveness of controls, in a situation in which the practitioner has obtained evidence that controls were not effective to achieve the entity's cybersecurity objectives based on one or more of the control criteria.

2.84 If, after using professional judgment, the practitioner believes there is reasonable justification to change the terms of the engagement from those originally contemplated, the practitioner would issue an appropriate report on the portion of the entity's cybersecurity risk management program included within the scope of the engagement. The attestation standards do not require the practitioner's report to include a reference to (*a*) the original engagement, (*b*) any procedures that may have been performed, or (*c*) scope limitations that resulted in the changed engagement. The practitioner may also decide to document the change in the engagement in an addendum to the engagement agreement to evidence agreement to the change among the parties.

2.85 However, if the practitioner and the engaging party are unable to agree to a change of the terms of the cybersecurity risk management examination, the practitioner and management may agree to continue the engagement in accordance with the original terms or mutually agree to terminate the engagement. If management does not accept either of these alternatives, the practitioner should take appropriate action, which could include disclaiming an opinion on both the description and the effectiveness of controls or withdrawing from the engagement.

Establishing an Overall Examination Strategy and Planning the Examination

2.86 When planning the cybersecurity risk management examination, the engagement partner and other key members of the engagement team develop an overall strategy for the scope, timing, and conduct of the engagement and an engagement plan, consisting of a detailed approach for the nature, timing, and extent of procedures to be performed. Adequate planning helps the practitioner devote appropriate attention to important areas of the engagement, identify potential problems on a timely basis, and properly organize and manage the engagement to make sure it is performed in an effective and efficient manner. Adequate planning also assists the practitioner in properly assigning work to engagement team members and facilitates the direction, supervision, and review of their work. Furthermore, if the work of internal auditors, other practitioners, or specialists is used in the engagement, proper planning helps the practitioner coordinate their work.

2.87 Paragraph .11 of AT-C section 205 requires a practitioner to establish an overall engagement strategy that sets the scope, timing, and direction of the engagement and guides in the development of the engagement plan. In establishing the overall engagement strategy, the practitioner does the following:

a. Obtains an understanding of the entity's business, cybersecurity objectives, and cybersecurity risk management program that define the engagement

b. Ascertains the expected timing and nature of required communications

c. Should consider the factors that, in the practitioner's professional judgment, are significant in directing the engagement team's efforts

d. Should consider the results of preliminary engagement activities, such as client acceptance, and, when applicable, whether knowledge gained on other engagements performed by the engagement partner for the entity is relevant

e. Plans the engagement process, including possible sources of evidence and choices among alternative measurement or evaluation methods

f. Obtains an understanding of the influences and pressures on management and other appropriate party(ies) within the entity

g. Should consider intended users of the cybersecurity risk management examination report and their information needs

h. Should consider the risk of fraud relevant to the engagement

i. Ascertains the nature, timing, and extent of resources necessary to perform the engagement

j. Assesses the effect on the engagement of using the work of an internal audit function or obtaining direct assistance from internal audit function personnel

2.88 The nature and extent of planning activities will vary depending on the practitioner's previous experience with the entity and on whether security events were identified in prior periods. Planning activities also will vary based on the entity's organizational characteristics, including the following:

- The complexity of the entity's cybersecurity risk management program based on factors such as its size and structure (for instance, centralized versus decentralized, insourced versus outsourced)
- The industry in which the entity operates
- The entity's network topology
- Uncommon, unusual, or outdated technologies used by the entity
- Significant changes to IT architecture, applications, or IT and security staffing during the past 12 months
- Acquisitions or divestitures during the most recent period, the integration or segmentation strategy used for the IT systems, and the current state of those activities
- Countries in which the entity does business or has a significant data presence, including those countries deemed high risk by management
- Business units or divisions with IT systems administered under a separate management structure (for instance, outside of a centralized IT function)
- Third parties (customers, vendors, business partners, and others) with access to the entity's information and systems who could represent a material risk to the achievement of the entity's cybersecurity objectives

2.89 The nature and extent of planning activities also will vary with the engagement circumstances. Based on paragraph .A9 of AT-C section 205, other matters the practitioner may consider when planning the cybersecurity risk management examination include the following:

- The characteristics of the specific cybersecurity risk management examination, including factors such as
  - — whether the engagement will be performed on the entity-wide cybersecurity risk management program or on only a portion of that program;
  - — whether management is the engaging party; and
  - — the time frame for the engagement
- The expected timing and the nature of any required communications
- The results of preliminary engagement activities, such as client acceptance, and whether knowledge gained on other engagements for the entity is relevant to the cybersecurity risk management examination, including possible sources of evidence about
  - — the presentation of the description;
  - — the design, implementation, and operation of controls; and
  - — management's selection of description criteria and control criteria against which the description and effectiveness of controls will be evaluated
- The practitioner's understanding of the entity and its environment, including the risk that

  - — the description of the entity's cybersecurity risk management program may not be presented in accordance with the description criteria and
  - — controls may not be effective to achieve the entity's cybersecurity objectives
- Identification of intended users of the cybersecurity risk management examination report and their information needs, consideration of materiality, and the components of attestation risk
- The risk of fraud relevant to the engagement
- Use of the internal audit function, other practitioners, or specialists in the cybersecurity risk management examination

2.90 Paragraph .13 of AT-C section 205 includes more detailed requirements and additional explanatory guidance that the practitioner should consider when developing the engagement plan.

2.91 When establishing the overall engagement strategy and engagement plan, it is important to remember that the cybersecurity risk management examination is ordinarily performed using a top-down approach, similar to the approach used by management during its assessment. As in other internal control engagements, the top-down approach in a cybersecurity risk management examination ordinarily involves consideration of the matters discussed in the preceding paragraphs of this section, followed by consideration of entity-level processes and controls as well as management's assessment and monitoring activities.

2.92 In a cybersecurity risk management examination, entity-level controls usually refer to the trust services criteria for

a. control environment (CC1.1–1.5),[10]
b. communication and information (CC2.1–2.3),
c. risk assessment (CC3.1–3.4), and
d. monitoring (CC4.1–4.2).

2.93 Planning is a cumulative and iterative process that occurs throughout the engagement. Accordingly, the practitioner may need to revise the overall strategy and engagement plan based on unexpected events, changes in conditions, or evidence obtained that contradicts information considered during planning.

Considering Materiality During Planning

2.94 When establishing the overall engagement strategy, paragraph .16 of AT-C section 205 also requires the practitioner to consider both qualitative and quantitative materiality factors. Due to the vast number of information and other assets and the number of related processes and controls within even a small entity, or a business unit or segment of a larger entity, practitioners need to consider materiality to determine the nature, timing, and extent of procedures and to perform the cybersecurity risk management examination. Adoption of an appropriate materiality allows the practitioner to prioritize testing efforts and supports an effective and efficient engagement.

[10] These references are to the trust services criteria for security, availability, and confidentiality (control criteria) presented in appendix D, "Trust Services Criteria for Security, Availability, and Confidentiality for Use as Control Criteria in the Cybersecurity Risk Management Examination."

2.95 In the cybersecurity risk management examination, materiality relates to the likelihood and magnitude of the risks that threaten the achievement of the entity's cybersecurity objectives and whether the processes and controls the entity has designed, implemented, and operated were effective in mitigating those risks to an acceptable level.

2.96 Accordingly, the practitioner should consider the nature of threats and the likelihood and magnitude of the risks arising from those threats to specific information and other assets. In addition, the practitioner should consider the technical environment and whether the realization of threats or exploitation of vulnerabilities related to specific information assets, which appear inconsequential, could expose (either directly or indirectly) information assets and thereby result in failure to achieve the entity's cybersecurity objectives. For example, if access to the information assets of a financially immaterial business unit could provide access to the entity's strategic business systems, and the practitioner determines there is a high likelihood that such a vulnerability might be exploited, the practitioner is likely to consider access to the information assets of the financially immaterial business unit material in the cybersecurity risk management examination.

2.97 The practitioner's consideration of materiality is a matter of professional judgment and is affected by the practitioner's perception of the common information needs of report users as a group. In this context, it is reasonable for the practitioner to assume that report users

a. have a reasonable knowledge of cybersecurity, including the nature of cybersecurity risks and vulnerabilities and the processes and controls typically used to manage such risks, and are willing to study the topic with reasonable diligence.

b. understand that the description of an entity's cybersecurity risk management program and the controls within that program are measured or evaluated and examined to appropriate levels of materiality and understand any materiality concepts included in the description and control criteria.

c. understand any inherent uncertainties involved in describing a cybersecurity risk management program and inherent limitations in the design and operation of controls. (To make sure that report users understand such uncertainties, both management's assertion and the practitioner's report disclose inherent limitations of a cybersecurity risk management engagement.)

d. make reasonable decisions on the basis of the description and the effectiveness of controls, taken as a whole.

2.98 Unless the engagement has been designed to meet the particular information needs of specific users of the cybersecurity risk management examination report (and the report is restricted to those specific users), the possible effect of misstatements regarding the description of the entity's cybersecurity risk management program or the effectiveness of controls on specific users, whose information needs may vary widely, is not ordinarily considered.

2.99 If the practitioner becomes aware, during the conduct of the engagement, of information that would have caused him or her to have initially determined a different materiality, paragraph .17 of AT-C section 205 requires the practitioner to reconsider materiality. Chapter 3 of this guide discusses

materiality considerations during the performance of the cybersecurity risk management examination in further detail.

Performing Risk Assessment Procedures

Obtaining an Understanding of the Entity's Cybersecurity Risk Management Program and Controls Within That Program

2.100 Paragraph .14 of AT-C section 205 requires the practitioner to obtain a sufficient understanding of the subject matter of the engagement. As previously discussed, there are two subject matters in the cybersecurity risk management examination:

1. A description of the entity's cybersecurity risk management program in accordance with the description criteria
2. The effectiveness of the controls within that program to achieve the entity's cybersecurity objectives based on the control criteria

2.101 The practitioner's risk assessment procedures to obtain the understanding may include the following, usually in some combination:

- Inquiring of management, those charged with governance, and others within the entity who, in the practitioner's judgment, may have relevant information
- Observing operations and inspecting documents, reports, and printed and electronic records of transaction processing
- Inspecting a selection of agreements between the entity and its customers and vendors and business partners (VBPs)
- Reperforming the application of a control

2.102 One or more of the procedures discussed in the preceding paragraph may be accomplished through the performance of a walkthrough. In addition, the practitioner may perform such procedures concurrently with procedures to obtain evidence about whether the description is presented in accordance with the description criteria and whether the controls within the program were effective in achieving the entity's cybersecurity objectives based on the control criteria.

2.103 When obtaining the understanding of the entity's program and controls, the practitioner needs to understand certain controls at a detailed level to enable him or her to perform procedures designed to obtain evidence about whether such controls were effective in achieving the entity's cybersecurity objectives. Chapter 3 discusses the practitioner's procedures in a cybersecurity risk management examination in more detail.

Assessing the Risk of Material Misstatement

2.104 In the cybersecurity risk management examination, the practitioner's understanding of the entity's cybersecurity risk management program and controls within that program should be sufficient to enable the practitioner to do the following:

- Identify and assess the risks that

- — the description of the entity's cybersecurity risk management program is not presented in accordance with the description criteria and
- — controls were not effective in achieving the entity's cybersecurity objectives based on the control criteria, because of deficiencies in the design or operations of controls

- Provide a basis for designing and performing further procedures that are responsive to the assessed risks and for obtaining reasonable assurance to support the practitioner's opinion on the description and the effectiveness of controls

2.105 When assessing the risks of material misstatement, paragraph .15 of AT-C section 205 states that the practitioner should obtain an understanding of internal control, which, in the case of a cybersecurity risk management examination, focuses on evaluating the design of controls over the preparation of the description and determining whether they have been implemented by making inquiries of the personnel responsible for the description and by performing other procedures. In addition, the practitioner should consider controls, including monitoring activities, that the entity has designed and implemented to provide reasonable assurance that the entity's cybersecurity objectives are achieved.

2.106 The practitioner should consider whether any risk assessment procedures and other procedures performed to obtain the understanding indicate a risk of material misstatement due to fraud or noncompliance with laws or regulations. For example, fraud risks might include the risk of management override of entity controls, misappropriation of information and other assets, and the creation, by entity personnel, of false or misleading documents or records. Chapter 3 discusses the practitioner's responsibilities for responding to known or suspected fraud or noncompliance in further detail.

2.107 As previously discussed, the risk of material misstatement relates to the likelihood and magnitude of the risks that threaten the achievement of the entity's cybersecurity objectives and whether the processes and controls the entity has designed, implemented, and operated were effective in mitigating those risks. In the cybersecurity risk management examination, risk assessment often begins with identifying and assessing the types, likelihood, and impact of risks that affect the preparation of the description and the effectiveness of controls within the entity's cybersecurity risk management program. Risks to the entity's information assets, including manufacturing and industrial control systems, may arise from any of the following:

- Intentional (for example, fraud) and unintentional internal and external acts
- Identified threats, vulnerabilities, and deficiencies
- The use of external parties that store, process, or transmit sensitive information on the entity's behalf (for example, suppliers, customers, vendors, business partners, "fourth parties")
- The type of employee personnel (finance, administrative, operations, IT, sales and marketing, and so on) and others (contractors, vendor employees, business partners, and so on) with access to information and systems

2.108 Accordingly, when understanding the inherent risks that may affect the entity's ability to achieve its cybersecurity objectives, the practitioner should consider whether the entity

- maintains information in the IT environment that is critical to operating its business or maximizing its advantage in the marketplace.
- is dependent on internet connectivity to support its business operations.
- is a high-profile entity within the sector in which it operates.
- relies extensively on complex industrial controls systems.
- has an extensive number of third-party vendors or service providers with connections into its systems.
- operates within a regulated sector.
- operates in a sector that has a history of being a target of cyberattacks.
- operates in a sector that has been the target of attacks resulting in breaches that have had a material effect on the related entity.
- has a history of being subject to cyberattacks.

Some practitioners find it useful to use terms such as high, medium, or low to describe an entity's overall inherent risk assessment. However, use of such terminology is not required.

2.109 Once the practitioner has identified and assessed the risks, the practitioner should consider the processes and controls the entity has designed, implemented, and operated to mitigate those risks. As required by paragraph .18 of AT-C section 205, the practitioner should consider the assessed risk of material misstatement as the basis for designing and performing further procedures whose nature, timing, and extent (*a*) are responsive to assessed risks of material misstatement and (*b*) allow the practitioner to obtain reasonable assurance about whether the description is presented in accordance with the description criteria and whether the controls were effective to achieve the entity's cybersecurity objectives based on the control criteria.

2.110 Most of the practitioner's procedures in forming an opinion on the description and on the effectiveness of controls consist of obtaining and evaluating evidence. Procedures to obtain evidence include inspection, observation, reperformance, and analytical procedures, often in some combination, in addition to inquiry. Chapter 3 provides additional guidance on performing examination procedures in the cybersecurity risk management examination.

Understanding the Internal Audit Function

2.111 If the entity has an internal audit function, then as part of understanding the entity's cybersecurity risk management program, the practitioner also obtains an understanding of

a. the nature of the internal audit function's responsibilities and how the internal audit function fits into the entity's organizational structure and

b. the activities performed or to be performed by the internal audit function as it relates to the cybersecurity risk management program.

2.112 If the internal audit function does not perform activities related to the cybersecurity risk management program, or if the entity does not have a function that performs similar activities, the practitioner should consider the effect on his or her conclusions regarding the effectiveness of monitoring of controls.

2.113 An entity's internal audit function performs assurance and consulting activities designed to evaluate and improve the effectiveness of the entity's governance, risk management, and internal control processes. Activities similar to those performed by an internal audit function may be conducted by functions with other titles within an entity. Some or all of the activities of an internal audit function may also be outsourced to a third-party service provider. For example, an entity may engage a service provider to perform (*a*) penetration testing; (*b*) responsibilities of the internal audit function that the function itself does not have the competency or qualifications to perform (for example, performing the IT internal audit function); or (*c*) a one-time special assessment at the request of the board of directors. Neither the title of the function nor whether it is performed by the entity or a third-party service provider are sole determinants of whether the practitioner can use the work of internal auditors. Rather, it is the nature of the activities, the extent to which the internal audit function's organizational status and relevant policies and procedures support the objectivity of the internal auditors, the competence of internal auditors, and the systematic and disciplined approach of the function that are relevant. References in this guide to the work of the internal audit function include relevant activities of other functions or third-party providers that have these characteristics.

2.114 Activities of the internal audit function that may be relevant to the cybersecurity risk management examination include those that provide information or evidence about whether the description is presented in accordance with the description criteria or whether controls within the cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives.

2.115 When obtaining an understanding of the internal audit function's responsibilities and activities, the practitioner makes inquiries of internal audit personnel and reads information about the internal audit function included in the description of the entity's cybersecurity risk management program. Ordinarily, the practitioner also requests and reads any relevant internal audit reports related to the period covered by the engagement. For example, reading the internal audit plan and reports issued by the internal audit function enables the practitioner to understand the nature of the internal audit function's responsibilities and how the internal audit function fits into the entity's organizational structure. Additionally, any findings in internal audit reports that relate to the presentation of the description of the entity's cybersecurity risk management program or the effectiveness of controls within that program should be taken into consideration as part of the risk assessment and in determining the nature, timing, and extent of the practitioner's planned procedures.

Planning to Use the Work of Internal Auditors

2.116 If, after obtaining an understanding of the internal audit function, the practitioner concludes that (*a*) the activities of the internal audit function are not relevant to the cybersecurity risk management examination or (*b*) it may not be efficient to consider the work of the internal audit function, the practitioner does not need to give further consideration to the work of the internal audit function.

2.117 The practitioner may determine, however, that the engagement can be performed more effectively or efficiently by using the work of the internal audit function or obtaining direct assistance from internal audit function personnel. The phrase "using the work of the internal audit function" usually refers to using work designed and performed by the internal audit function, in accordance with an internal audit plan, to obtain evidence to support the various entity objectives. This differs from work the internal audit function performs to provide direct assistance to the practitioner, including assistance in performing tests of controls that are designed by the practitioner and performed by members of the internal audit function under the practitioner's direction, supervision, and review. When members of the internal audit function provide direct assistance, the procedures they perform are similar to work performed by the engagement team.[11]

Evaluating the Competence, Objectivity, and Systematic Approach Used by Internal Auditors

2.118 If the practitioner determines that the work of the internal audit function is relevant to the cybersecurity risk management examination, and the practitioner intends to use the work of the internal audit function in obtaining evidence, or plans to use internal auditors to provide direct assistance during the examination, the practitioner should determine whether the work can be used for purposes of the examination by evaluating several factors. The factors the practitioner should evaluate include

a. the level of competence of the internal audit function or the individual internal auditors providing direct assistance;

b. the extent to which the internal audit function's organizational status and relevant policies and procedures support the objectivity of the internal audit function as a whole or, for internal auditors providing direct assistance, the existence of threats to the objectivity of those internal auditors and the related safeguards applied to reduce or eliminate those threats; and

c. the application by the internal audit function of a systematic and disciplined approach, including quality control.

2.119 When evaluating competence, the practitioner should consider the attainment and maintenance of knowledge and skills of the internal audit function at the level required to enable assigned tasks to be performed diligently and with the appropriate level of quality, particularly as it relates to the work

[11] Regardless of whether the practitioner plans to use the internal audit's work or to use the internal audit function in a direct assistance capacity, the term *engagement team*, as used throughout this guide, does not include individuals within the entity's internal audit function.

of the internal audit function that is to be used or, when using individuals for direct assistance, the individual. Consideration of factors such as the following may assist the practitioner with that evaluation: (*a*) hiring policies; (*b*) the adequacy of resources relative to the size of the entity; (*c*) technical training and proficiency of individuals; (*d*) knowledge of the areas being examined, including industry-specific or technical knowledge required to perform the work; and (*e*) whether internal auditors are members of relevant professional bodies or have certifications that oblige them to comply with the relevant professional standards, including continuing professional education requirements.

2.120 When evaluating objectivity, the practitioner should consider whether the internal audit function as a whole or, when using individuals for direct assistance, the individual performs tasks without allowing bias, conflict of interest, or undue influence of others to override professional judgments. Factors that may impact objectivity include whether there are (*a*) any conflicts of interest or undue influence of others to override professional judgments, (*b*) conflicting responsibilities, and (*c*) constraints or restrictions on the internal audit function (or, when using direct assistance, the individual).

2.121 When evaluating the application by the internal audit function of a systematic and disciplined approach, including quality control, the practitioner may consider the function's approach to planning, performing, supervising, reviewing, and documenting its activities. Relevant factors to consider may include, among others, (*a*) the existence, adequacy, and use of documented internal audit procedures or guidance covering such areas as risk assessments, work programs, documentation, and reporting; or (*b*) whether the internal audit function has appropriate quality control policies and procedures.

2.122 The objectivity and competence of internal auditors are important considerations when determining whether to use their work and, if so, the nature and extent to which their work should be used. However, as noted in paragraph .A46 of AT-C section 205, a high degree of objectivity cannot compensate for a low degree of competence, nor can a high degree of competence compensate for a low degree of objectivity. Additionally, when the practitioner is considering whether to use the work of the internal audit function, neither a high level of competence nor strong support for the objectivity of the internal auditors compensates for the lack of a systematic and disciplined approach by the internal audit function.

2.123 Based on an evaluation of the preceding factors, it is up to the practitioner to determine whether the risks to the quality of the work of the internal audit function or the individual, when using direct assistance, are too significant and whether it is appropriate to use any of the work of the function or individual as examination evidence.

Deterining the Extent to Which to Use the Work of Internal Auditors

2.124 The extent to which the practitioner plans to use the work of the internal audit function is a matter of professional judgment. Because the practitioner has sole responsibility for expressing an opinion on the description and on the effectiveness of controls, the practitioner makes all significant judgments in the examination, including when to use the work of the internal audit function in obtaining evidence.

2.125 To prevent undue use of the internal audit function in obtaining evidence, the practitioner should use less of the work of the internal audit function and perform more of the work directly in situations when

- more judgment is involved to plan and perform the procedures or to evaluate the evidence obtained.
- the assessed risk of material misstatement is high.
- the internal audit function's organizational status and relevant policies and procedures raise concerns about the objectivity of the internal auditors.
- the level of competence of the internal audit function is low.

Coordinating Procedures With the Internal Auditors

2.126 When the practitioner plans to use the work of the internal audit function, the practitioner may find it helpful to review the internal audit function's audit plan and discuss with management the planned use of the work of the internal audit function as a basis for coordinating the work of internal auditors with the practitioner's procedures. The audit plan provides information about the nature, timing, extent, and scope of the work performed by the internal audit function, as well as the work that is planned to be performed.

2.127 As a basis for coordinating the respective activities between the practitioner and the internal auditors, it may be useful to address the following when planning to use the work of the internal audit function:

- The nature of the work performed
- The timing of such work
- The extent of coverage
- Proposed methods of item selection and sample sizes
- Documentation of the work performed
- Review and reporting procedures

2.128 Coordination between the practitioner and the internal audit function is effective when discussions take place at appropriate intervals throughout the period to which management's assertion pertains. It is important that the practitioner informs the internal audit function of significant matters as they arise during the engagement. Equally important is that the practitioner has access to relevant reports of the internal audit function and is advised of any significant matters that come to the attention of the internal auditors, when such matters may affect the scope of the examination and the potential nature, timing, or extent of the examination procedures. Communication throughout the engagement provides opportunities for internal auditors to bring up matters that may affect the practitioner's work. The practitioner is then able to take such information into account (for example, when assessing the risks that the description is not presented in accordance with the description criteria or that controls were not effective in achieving the entity's cybersecurity objectives based on the control criteria).

2.129 Although the practitioner is not precluded from using work that the internal audit function has already performed, coordination of activities between the practitioner and the internal audit function is likely to be most effective when appropriate interaction occurs before the internal audit function performs the work.

2.130 When planning to use internal auditors to provide direct assistance, paragraph .41 of AT-C section 205 requires the practitioner to obtain written acknowledgment from management that internal auditors providing direct assistance will be allowed to follow the practitioner's instructions without management's interference.

Evaluating Whether the Work of Internal Auditors is Adequate for the Practitioners' Purposes

2.131 When using the work of the internal audit function, the practitioner should perform sufficient procedures, including reperformance, on the body of work of the internal audit function that the practitioner plans to use to evaluate whether such work is adequate for the practitioner's purposes. Chapter 3 provides guidance on the practitioner's considerations when performing procedures on that work.

Planning to Use the Work of an Other Practitioner

2.132 In certain situations, the practitioner might plan to use the work of an other practitioner. For example, if the entity operates divisions or business units in other geographic locations, the practitioner might plan to use the work of a practitioner located in the same geographic region as the entity to obtain sufficient appropriate evidence to enable the practitioner to express an opinion on the description and on the effectiveness of controls in the cybersecurity risk management engagement.

2.133 For those reasons, the practitioner who decides to use the work of an other practitioner is required by paragraph .31 of AT-C section 105 to

a. obtain an understanding of whether the other practitioner understands, and will comply with, the ethical requirements that are relevant to the engagement and, in particular, is independent. (The discussion beginning in paragraph 2.66 of this guide also applies to the other practitioner.)

b. obtain an understanding of the other practitioner's professional competence. (See paragraph 2.135)

c. communicate clearly with the other practitioner about the scope and timing of the other practitioner's work and findings. (See paragraph 2.136)

d. be involved in the work of the other practitioner, if assuming responsibility for the work of the other practitioner.

e. evaluate whether the other practitioner's work is adequate for the practitioner's purposes. (See paragraph 2.137)

f. determine whether to make reference to the other practitioner in the practitioner's report. (See paragraph 2.138)

2.134 When using the work of an other practitioner, paragraph .A57 of AT-C section 205 clarifies that the practitioner is responsible for directing, supervising, and performing the engagement in compliance with professional standards, applicable regulatory and legal requirements, and the firm's policies and procedures. The practitioner is also responsible for determining whether the report issued is appropriate in the circumstances.

2.135 When evaluating the professional competence of the other practitioner, the practitioner may make inquiries of the professional reputation of the other practitioner, consider whether the other practitioner is subject to regulatory oversight, and read any publicly available regulatory reports.

2.136 Once the practitioner has decided to use the work of an other practitioner, he or she should communicate with the other practitioner about the scope and timing of the other practitioner's work. Through this communication, the practitioner can better plan the nature, timing, and extent of any procedures that relate to the work of the other practitioner, including the practitioner's involvement in directing, supervising, and reviewing the work of the other practitioner. Due to complexities involved in planning a cybersecurity risk management engagement, using the work of other practitioners is most likely to be successful when these matters are addressed early in engagement planning.

2.137 When using the work of an other practitioner, the practitioner is also required to evaluate whether the other practitioner's work is adequate for the purposes of the engagement. The nature, timing, and extent of this involvement are affected by the practitioner's understanding of the other practitioner, such as previous experience with, or knowledge of, the other practitioner and the degree to which the engagement team and the other practitioner are subject to common quality control policies and procedures.

2.138 The practitioner also determines whether to take responsibility for the work of the other practitioner or to make reference to the other practitioner in the practitioner's report. Chapter 4 provides a more detailed discussion about reporting when the work of an other practitioner is used.

Planning to Use the Work of a Practitioner's Specialist

2.139 When planning a cybersecurity risk management examination, a practitioner may decide that engaging or assigning a specialist with specific skills and knowledge is necessary to execute the planned examination. If a practitioner's specialist will be used in the cybersecurity risk management examination, paragraph .36 of AT-C section 205 requires the practitioner to

a. evaluate the specialist's competence, capabilities, and objectivity;

b. obtain an understanding of the specialist's field of expertise to enable the practitioner to determine the nature, scope, and objectives of the specialist's work and to evaluate the adequacy of that work; and

c. agree with the specialist regarding the

  i. nature, scope, and objectives of the specialist's work;

  ii. the respective roles and responsibilities of the practitioner and the specialist;

  iii. the nature, timing, and extent of communication between the practitioner and the specialist, including the form of any report or documentation to be provided by the specialist; and

  iv. the need for the practitioner's specialist to observe confidentiality requirements.

2.140 By communicating with the practitioner's specialist about these matters early in the engagement, the practitioner will be in a better position to plan the scope and timing of the specialist's work on the engagement. In addition, he or she will be better able to plan the nature, timing, and extent of any procedures that relate to the work of the specialist, including the direction, supervision, and review of the specialist's work, particularly if that work will be used during initial engagement planning and risk assessment. Though not required, the practitioner should consider documenting, in an engagement letter or other appropriate form of written communication, the understanding reached with the practitioner's specialist about the matters discussed. When evaluating the practitioner specialist's competence and capabilities, the practitioner may obtain information from a variety of sources, including discussions with the specialist, personal experience with the specialist's work, discussions with others who are familiar with the specialist's work, or published papers or books written by the specialist, among other things. In addition, the practitioner needs to determine that the practitioner's specialist has a sufficient understanding of the attestation standards relevant to the cybersecurity risk management examination and this guide to enable the practitioner's specialist to understand how his or her work will help achieve the objectives of the engagement.

2.141 When evaluating the objectivity of the practitioner's external specialist, the practitioner may inquire of management (or the engaging party, if different) about any known interests or relationships (such as financial interests, business and personal relationships, and provision of other services by the practitioner's external specialist) that management has with the specialist that may affect the objectivity of the practitioner's external specialist. In certain cases, the practitioner may decide to request written representations from the practitioner's external specialist about any interests or relationships with management (or the engaging party, if different) of which the specialist is aware.

2.142 The practitioner may also discuss with the practitioner's specialist any safeguards applicable to the specialist and evaluate whether the safeguards are adequate to reduce known threats to independence to an acceptable level. There may be some circumstances in which safeguards cannot reduce such threats to an acceptable level. For example, if the practitioner's specialist has played a significant role in implementing or operating significant aspects of the entity's cybersecurity risk management program, he or she is likely not objective (independent) when measuring or evaluating the effectiveness of controls within that program.

2.143 When considering the relevance of the practitioner's specialist's field of expertise to the engagement, the practitioner should consider (*a*) whether that specialist's field includes areas of specialty relevant to the engagement; (*b*) whether professional or other standards and regulatory or legal requirements apply; (*c*) assumptions and methods used by the specialist and whether they are generally accepted within the specialist's field and appropriate in the engagement circumstances; and (*d*) the nature of internal and external data or information used by the practitioner's specialist.

2.144 The nature, timing, and extent of the practitioner's procedures to evaluate the matters discussed in this section vary depending on the particular circumstances of the engagement. When determining the nature, timing, and

extent of those procedures, paragraph .38 of AT-C section 205 states that the practitioner should consider the following:

a. The significance of that practitioner's specialist's work in the context of the engagement

b. The nature of the matter to which the practitioner's specialist's work relates

c. The risks of material misstatement in the matter to which the practitioner's specialist's work relates

d. The practitioner's knowledge of and experience with previous work performed by the practitioner's specialist

e. Whether the practitioner's specialist is subject to the practitioner's firm's quality control policies and procedures, such as involvement in the firm's recruitment and training programs

2.145 In addition to the matters discussed in this section, paragraph .36 of AT-C section 205 also requires the practitioner to evaluate the adequacy of the work of the practitioners' specialist for the practitioner's purposes. That evaluation is discussed further beginning in paragraph 3.115 of this guide.

Chapter 3

Performing the Cybersecurity Risk Management Examination

This chapter discusses responding to the assessed risks, materiality considerations, and other matters affecting the nature, timing, and extent of the practitioner's procedures to obtain sufficient appropriate evidence about whether (*a*) management's description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and (*b*) the controls within that program were effective for the specified period of time to achieve the entity's cybersecurity objectives.

Responding to Assessed Risks and Obtaining Evidence

3.01 Paragraphs .20–.21 of AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*), require the practitioner to respond to the assessed risks when designing and performing examination procedures. Specifically, they require the practitioner to

a. design and implement overall responses to address the assessed risks of material misstatement and

b. design and perform further procedures whose nature, timing, and extent are based on, and responsive to, the assessed risks of material misstatement.

3.02 Paragraph .10 of AT-C section 105, *Concepts Common to All Attestation Engagements* (AIPCA, *Professional Standards*), defines a *misstatement* as follows:

> A difference between the measurement or evaluation of the subject matter by the responsible party and the proper measurement or evaluation of the subject matter based on the criteria. Misstatements can be intentional or unintentional, qualitative or quantitative, and include omissions. In certain engagements, a misstatement may be referred to as a deviation, exception, or instance of noncompliance.

3.03 In this guide, the following terms are used when discussing misstatements related to different aspects of the entity's cybersecurity risk management program and the effectiveness of controls within that program:

- The term *description misstatement* is used when describing differences between (or omissions in) the presentation of the description of the cybersecurity risk management program and the description criteria.
- The term *deficiency* is used to identify misstatements in which controls were not suitably designed or did not operate effectively.
- The term *deviation* is used to identify misstatements in which the operation of a control was not effective in a specific instance. A deviation may, individually or in combination with other deviations, result in a deficiency.

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

Description misstatements and deficiencies that are immaterial do not result in a modification of the practitioner's opinion.

Considering Materiality in Responding to the Assessed Risks and Planning Procedures

3.04 As discussed in chapter 2, "Accepting and Planning a Cybersecurity Risk Management Examination," paragraph .16 of AT-C section 205 requires the practitioner to consider materiality when establishing the engagement strategy. Paragraph .A15 states that materiality in an attestation engagement is considered in the context of qualitative factors and, when applicable, quantitative factors. The relative importance of each of those factors when considering materiality in a particular engagement is a matter of professional judgment, and those judgments are made in light of the surrounding circumstances. Furthermore, due to the nature of a cybersecurity examination, the application of materiality to different aspects of the entity will result in differences in planned procedures due to underlying differences in threats and vulnerabilities.

3.05 Due to the vast number of information and other assets and the number of related processes and controls within even a small entity, or a business unit or segment of a larger entity, practitioners need to consider materiality during risk assessment and when determining the nature, timing, and extent of procedures to perform during the cybersecurity risk management examination. Adoption of an appropriate materiality allows the practitioner to prioritize testing efforts and supports an effective and efficient engagement.

3.06 As discussed throughout this guide, there are two distinct but complementary subject matters in a cybersecurity risk management examination: (1) the description of the entity's cybersecurity risk management program and (2) the effectiveness of the controls within that program to achieve the entity's cybersecurity objectives; consequently, consideration of materiality is different as it relates to each.

3.07 When considering materiality regarding the description, the practitioner should consider whether description misstatements (including omissions) in the presentation, individually or in the aggregate, could reasonably be expected to influence relevant decisions of report users. For instance, a material omission may result from the entity's failure to describe a cybersecurity objective related to compliance with the European Union's General Data Protection Regulation, when significant operations of the entity are subject to that regulation. Paragraph 3.19 discusses materiality considerations when evaluating whether the description is presented in accordance with the description criteria.

3.08 When considering materiality regarding the effectiveness of controls to achieve the entity's cybersecurity objectives, the practitioner should consider both qualitative and quantitative factors, as discussed in paragraph 3.38.

Designing Overall Responses to the Risk Assessment

3.09 The assessment of the risks of material misstatement is affected by many factors, including materiality considerations and the practitioner's understanding of the effectiveness of entity-level controls. Effective entity-level controls, particularly the control environment and monitoring activities, may allow the practitioner to have more confidence in the processes and controls

the entity has designed, implemented, and operated to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented. Thus, effective entity-level controls may reduce the nature and extent of the practitioner's procedures to obtain evidence about control effectiveness; they may also impact decisions related to when such procedures may be performed.

3.10 In contrast, deficiencies in entity-level controls may have the opposite effect. For that reason, it is important that the practitioner understand the root cause of the deficiencies and the impact they may have on the operating effectiveness of the related controls. Ways in which a practitioner may respond to ineffective entity-level controls include

- selecting different types of procedures, or changing the timing of those procedures, to obtain evidence about the operating effectiveness of controls and
- obtaining more extensive evidence about the operating effectiveness of controls.

3.11 Paragraph .A24 of AT-C section 205 states that other overall responses to address the assessed risks of material misstatement may include the following:

- Emphasizing to the engagement team the need to maintain professional skepticism
- Assigning more experienced staff or using specialists
- Providing more supervision
- Incorporating additional elements of unpredictability in the selection of procedures to be performed
- Making changes to the nature, timing, or extent of procedures

3.12 However, the importance of effective entity-level controls in a cybersecurity risk management examination go beyond providing the practitioner with more confidence in the processes and controls at the entity. For an entity with complex IT networks and architectures, effective entity-level controls may be necessary in order to establish effective internal control to achieve the entity's cybersecurity objectives.

3.13 The remainder of this chapter discusses the nature, timing, and extent of further procedures the practitioner performs to obtain sufficient appropriate evidence in the cybersecurity risk management examination.

Obtaining Evidence About Whether the Description of the Entity's Cybersecurity Risk Management Program Is Presented in Accordance With the Description Criteria

3.14 As previously discussed, the description of the entity's cybersecurity risk management program is intended to provide report users with information that will enable them to better understand the entity's cybersecurity risk management program. For example, disclosures about the environment in which the entity operates, the process used to develop its cybersecurity objectives, commitments made to customers and others, responsibilities involved in operating and maintaining a cybersecurity risk management program, and the nature

of the IT components used, allow users to better understand the context in which the processes and controls operate within the entity's cybersecurity risk management program. Management is responsible for preparing the description and for making an assertion about whether the description is presented in accordance with the description criteria. Appendix A, "Information for Entity Management," provides guidance to management on preparing the presentation. This section discusses the procedures the practitioner performs to obtain evidence about whether the description is presented in accordance with the description criteria.

3.15 The practitioner should obtain and read management's description of the entity's cybersecurity risk management program and perform procedures to determine whether the description is presented in accordance with the description criteria. The description is presented in accordance with the description criteria when it

- describes the cybersecurity risk management program the entity has implemented (that is, placed in operation);
- includes information about each description criterion presented in appendix C, "Description Criteria for Use in the Cybersecurity Risk Management Examination" of this guide; and
- does not omit or distort information that is likely to be relevant to users' decisions. (See paragraph 3.22)

3.16 When evaluating whether the description is presented in accordance with the description criteria, the practitioner gives consideration to the implementation guidance for each criterion. The implementation guidance presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. Because the implementation guidance does not address all possible situations, the practitioner should consider the facts and circumstances of the entity and its environment when applying the description criteria.

3.17 When considering whether the description reflects the cybersecurity risk management program and controls the entity has implemented, the practitioner should consider the understanding of the entity's cybersecurity risk management program and controls obtained during planning, as discussed in chapter 2. The practitioner then supplements this understanding by obtaining information about the program and controls through inquiry, inspection of relevant documents, walkthroughs, and other procedures. The description is not presented in accordance with the description criteria if it (*a*) states or implies that aspects of the program, or controls within that program, exist when they do not or (*b*) inadvertently or intentionally omits information about aspects of the program or related controls that result in a presentation that could be misleading.

3.18 Management may organize its description in the manner it deems most effective, as long as each criterion is addressed within the description. Management may use various formats, such as narratives, flowcharts, tables, or graphics, or a combination thereof, to prepare the description. In addition, the degree of detail to be included in the description is generally a matter of judgment. In other words, the description is intended to be prepared at a level of sufficient detail to provide the context that users need to understand the entity's cybersecurity risk management program; however, it is not intended to include disclosures at such a detailed level that the likelihood of a hostile party

exploiting a security vulnerability is increased. Furthermore, unless specifically required by a criterion, disclosures need not be quantified.

Materiality Considerations When Evaluating Whether the Description is Presented in Accordance With the Description Criteria

3.19 Paragraph .A15 of AT-C section 205 indicates that the practitioner should consider the concept of materiality in the context of qualitative factors (as discussed in the next paragraph) and quantitative factors (for example, when management elects to disclose the percentage of time that its internet-based systems were available during the period). Accordingly, the practitioner should consider materiality when evaluating whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria.

3.20 As previously discussed, applying the description criteria requires judgment. One of those judgments involves the level of materiality that applies when evaluating the description of the entity's cybersecurity risk management program in accordance with the description criteria. Because the description criteria call for disclosure of primarily nonfinancial information, most descriptions will be presented in narrative form. Thus, materiality considerations are mainly qualitative in nature and center around whether there are misstatements in, or omissions of, the information disclosed (description misstatements) that could, individually or in the aggregate, reasonably be expected to influence the decisions of intended users. For that reason, an understanding of the perspectives and information needs of intended users of the report is necessary to the assessment of materiality.

3.21 Examples of qualitative factors ordinarily considered when determining whether the description is presented in accordance with the description criteria include whether

- the description is prepared at a level of detail likely to be meaningful to report users.
- each description criterion in appendix C of this guide has been addressed without using language that omits or distorts the information related to any of the description criteria.
- the characteristics of the presentation are appropriate, since the description criteria allow for variations in presentation.
- an identified description misstatement
  - is unintentional or the result of an intentional act, particularly when the person perpetrating that act is a member of management.
  - is significant with regard to the practitioner's understanding of known previous communications to report users.
  - relates to the relationship between management and, if different, the engaging party or the engaging party's relationship with other parties.

Considering Whether the Description is Misstated or Otherwise Misleading

3.22 Paragraph .60 of AT-C section 205 requires the practitioner to evaluate, based on the evidence obtained, whether the description of the entity's cybersecurity risk management program is misleading within the context of the engagement.

3.23 When making this evaluation, paragraph .A73 of AT-C section 205 states that the practitioner may consider whether additional disclosures are necessary to supplement the description of the entity's cybersecurity risk management program. Additional disclosures may include, for example,

- significant interpretations made in applying the criteria in the engagement circumstances (for example, what constitutes a security event or a security incident);
- subsequent events,[1] depending on their nature and significance; and
- when reporting on only a portion of the entity-wide cybersecurity risk management program, a significant security incident that occurred in another portion of that program not covered by the examination.

Such additional disclosures may be presented in the description (in which case it would be subject to the practitioner's examination procedures) or as other information.

3.24 Although the description should be presented in accordance with the description criteria, paragraph .60 of AT-C section 205 does not require the practitioner to determine whether the description discloses every matter related to the entity's cybersecurity risk management program that every user might consider useful when making decisions. For example, a description presented in accordance with the description criteria may omit certain information related to the entity's cybersecurity risk management program when it is unlikely to be significant (in other words, it is immaterial) to report users' decisions.

3.25 As part of the practitioner's evaluation of whether the description is misleading within the context of the engagement, the practitioner may consider whether the description

- omits information involving one or more significant business units or segments, when the examination addresses the entity-wide cybersecurity risk management program.
- contains statements that cannot be objectively evaluated. For example, describing an entity as being the "world's best" or "most respected in the industry" is subjective and, therefore, could be misleading to report users.
- contains or implies certain facts that are not true (for example, that certain IT components exist when they do not or that certain processes and controls have been implemented when they are not being performed).

---

[1] Subsequent events are discussed beginning in paragraph 3.139 of this guide.

- inadvertently or intentionally omits or distorts material information about any of the description criteria that might affect the decisions of report users.

3.26 If the practitioner believes that the description is misstated or otherwise misleading, the practitioner ordinarily would ask management to amend the description by including the omitted information or revising the misstated information. If management refuses to amend the description, the practitioner should consider the effect on his or her opinion about whether the presentation of the description is in accordance with the description criteria.

Evaluating the Description When the Cybersecurity Risk Management Examination Addresses Only a Portion of the Entity's Cybersecurity Risk Management Program

3.27 As discussed in chapter 1, "Introduction and Background," the cybersecurity risk management examination usually addresses an entity-wide cybersecurity risk management program. However, there may be circumstances in which management engages the practitioner to examine and report on only a portion of that program. In other words, the cybersecurity risk management examination may be limited to any of the following:

- One or more specific business units or segments of an entity, when those units or segments operate under an entity-wide cybersecurity risk management program
- One or more specific business units or segments of an entity, when those units or segments operate under an independent cybersecurity risk management program
- One or more specific sets of systems or particular sets of information used by the entity

3.28 In those situations, the description is tailored to disclose only information about the portion of the cybersecurity risk management program (that is, the particular business unit, segment, or type of information) within the scope of the engagement. Likewise, when evaluating whether the description is presented in accordance with the description criteria, consideration is given to whether the description addresses all relevant aspects of the portion of the cybersecurity risk management program within the scope of the engagement. For example, if the engagement addresses only one specific business unit, and that unit's cybersecurity risk management program relies on aspects of the entity-wide program, the description would also include disclosure of those aspects of the entity-wide program relevant to that business unit.

Procedures to Obtain Evidence About the Description

3.29 Procedures the practitioner performs to obtain evidence about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria include a combination of the following:

- Discussing with management and other entity personnel the content of management's assertion and the description of the entity's cybersecurity risk management program.
- Reading the entity's annual report to understand

  - the nature of the entity's operations and the goods or services offered to its customers,
  - the entity's network environment and the information and systems the entity uses when interacting with customers, and
  - other matters related to cybersecurity affecting financial reporting.

- Reading the entity's cybersecurity objectives to determine whether they are suitable and complete in the specific engagement circumstances. Paragraphs 2.42 and 3.34 further discuss the suitability of an entity's cybersecurity objectives.
- Inspecting documentation supporting the entity's risk assessment and risk management processes, including the determination of the entity's risk appetite and the identification and mitigation of risk.
- Reading customer contracts, performance or service-level agreements, marketing materials distributed to customers or posted on the entity's website, and other available documentation to
  - better understand the specific goods or services provided to customers and
  - evaluate whether the controls the entity has implemented are suitably designed to achieve the entity's cybersecurity objectives related to commitments to customers and others. (For example, reading service-level agreements may help the practitioner understand the specific processing commitments made, including commitments related to the timeliness of processing, expected rates of error, or persons accessing confidential information.)
- Observing control procedures or other activities performed by entity personnel.
- Reading documents (such as board minutes, organization charts, and cybersecurity communications) to understand the entity's cybersecurity risk governance structure and processes, including
  - the involvement of board members,
  - the organizational structure to support the entity's cybersecurity risk management program,
  - the types of threat and vulnerability assessments the entity performs (both internal and external), and
  - the types and frequency of cybersecurity communications made to executive management and others.
- Reading documents about the entity's cybersecurity awareness and training programs, communication of code of conduct, employee handbooks, information security policies, incident notification procedures, and other available documentation to understand the entity's processes for communicating responsibilities for cybersecurity and other related matters to entity personnel.

- Reading policy and procedure manuals, cybersecurity program documentation, flowcharts, narratives, hardware asset management records, and other system documentation to understand
  - — the entity's use of technology, including its applications, infrastructure, network architecture, use of mobile devices, use of cloud technologies, and the types of external party access or connectivity to the entity;
  - — information technology policies and procedures; and
  - — controls over data loss prevention, access provisioning and de-provisioning, user identification and authentication, data destruction, security event monitoring and detection, and backup procedures.
- Reading internal audit reports, third-party assessments, audit committee presentations, and other documentation related to the entity's cybersecurity monitoring activities, security events, or investigative activities.
- Reading example contracts with vendors and business partners (for example, contract templates or a selection of contracts) and associated performance or service-level agreements and other documentation to understand
  - — how the entity's contracting process addresses cybersecurity-related matters;
  - — the interrelationship between the entity and its vendors and business partners, including the entity's process for assessing and managing cybersecurity risks associated with vendors or business partners; and
  - — the procedures the entity performs to monitor the effectiveness of controls performed by such vendors or business partners, when such controls are material to the achievement of the entity's cybersecurity objectives.
- Reading incident response and recovery plan documentation to understand the entity's processes to recover from identified security events, including its incident response procedures, incident communication protocols, recovery procedures, alternate processing plans, and procedures for the periodic testing of recovery procedures.
- Reading documents describing laws, regulations, or industry standards relevant to the entity's cybersecurity risk management program.

3.30 Performing walkthroughs provides evidence about whether the processes and controls within the program have been implemented. Performing a walkthrough involves making inquiries of management and other personnel and requesting that they describe and demonstrate their actions in performing a procedure. Walkthrough procedures include following a transaction, event, or activity from origination until final disposition through the entity's processes, including its information systems, using the same documents and IT systems that entity personnel use. Walkthrough procedures usually include a combination of inquiry, observation, inspection of relevant documentation, and

reperformance of procedures. It may be helpful for the practitioner to use flowcharts, questionnaires, or decision tables to facilitate understanding the design of the controls. An appropriately performed walkthrough provides an opportunity to verify the practitioner's understanding of the flow of information throughout the entity's cybersecurity risk management program and the design of the processes and controls within that program. If properly performed, walkthroughs may provide evidence about whether controls that, individually or in combination with other controls, support the key security policies and processes included in the description were implemented and operated effectively.

3.31 Inquiry, combined with other walkthrough procedures, enables the practitioner to gain a sufficient understanding of the processes and controls to determine whether they have been implemented as stated in the description of the entity's cybersecurity risk management program. During a walkthrough, the practitioner may inquire about instances during the period in which processes and controls did not operate as described or designed. In addition, the practitioner may inquire about variations in the process for different types of information. For example, the entity's processing may take different forms depending on how information is collected from customers or others.

3.32 In assessing whether the description is presented in accordance with the description criteria, the practitioner should consider whether there is alignment between the key security policies and processes described in the description and the controls the entity has designed and implemented to achieve the entity's cybersecurity objectives. Although management's description includes only information about the key security policies and processes, such key security policies and processes should be supported by controls designed and implemented to achieve the entity's cybersecurity objectives. The lack of comprehensive alignment between the key security policies and processes included in the description and the underlying controls necessary to achieve the entity's cybersecurity objectives would be an indicator of a description misstatement.

3.33 When performing a cybersecurity risk management examination, the practitioner should obtain an understanding of changes in the entity's cybersecurity risk management program implemented during the period covered by the examination. If the practitioner believes that the changes would be considered significant by report users, the practitioner should determine whether those changes have been included in the description of the entity's cybersecurity risk management program. The narrative discussing the change would be expected to contain an appropriate level of detail, including the date the change occurred and how the affected aspects of the program differed before and after the change. If such changes have not been included in the description, the practitioner may ask management to amend the description to include this information. If management refuses to include this information in the description, the practitioner should consider the effect of such changes on his or her conclusions regarding the presentation of the description of the entity's cybersecurity risk management program and the practitioner's opinion.

Considering the Suitability of the Entity's Cybersecurity Objectives

3.34 As discussed in chapter 2, during the engagement acceptance process, the practitioner should consider whether management has established suitable objectives. The practitioner does not have a responsibility to express an opinion on the suitability of the entity's cybersecurity objectives.

3.35 If, however, while performing risk assessment or further procedures, the practitioner becomes aware of information that causes him or her to believe that the cybersecurity objectives developed by management are not, in fact, suitable and complete, the practitioner should discuss the matter with management. If management is unwilling to revise the cybersecurity objectives to address the practitioner's concerns, the practitioner should consider the effect on his or her opinion.

3.36 Assume, for example, that the client is a hospital that dispenses medication to patients through infusion pumps that are controlled through the entity's medication system, but the client failed to establish a cybersecurity objective related to guarding against the improper use, modification, or destruction of the medication system to safeguard the life and health of its patients. Because the entity did not establish such an objective, it did not identify and assess the risks that such objective would not be achieved, nor did it design, implement, and operate controls to mitigate such risks. Accordingly, its cybersecurity objectives are incomplete and thus not suitable in the circumstances. In that situation, the practitioner may conclude that a modification of the opinion is appropriate because of the following:

- The cybersecurity objectives identified in the description in accordance with description criterion number 3 (DC3), *The entity's principal cybersecurity risk management program objectives (cybersecurity objectives) related to availability, confidentiality, integrity of data, and integrity of processing*,[2] are not suitable; therefore, the description is not presented in accordance with the description criteria; or
- The controls were not effective to achieve the entity's cybersecurity objectives because controls over the objective-setting process are ineffective based on the entity's failure to meet control criterion 3.1 (CC3.1), *The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.*

3.37 Because the entity's cybersecurity objectives need to be suitable to enable both management and the practitioner to evaluate whether internal control over cybersecurity is effective, the lack of suitable cybersecurity objectives is likely to have a pervasive effect on the effectiveness of the entity's cybersecurity risk management program. Accordingly, it is likely that the practitioner would express an adverse opinion on both subject matters.

Materiality Considerations When Evaluating the Effectiveness of Controls to Achieve the Entity's Cybersecurity Objectives

3.38 Paragraph 3.19 discusses materiality considerations related to the description, whereas this section discusses materiality considerations that can affect the practitioner's conclusion about the suitability of design and operating effectiveness of controls to achieve the entity's cybersecurity objectives.

---

[2] The quoted description criterion is presented in appendix C, "Description Criteria for Use in the Cybersecurity Risk Management Examination" of this guide. Other description criteria cited in this guide (indicated with the naming convention "DC") are also drawn from appendix C.

3.39 When considering whether controls within the program were effective to achieve the entity's cybersecurity objectives, the practitioner should consider a number of factors, including

- the nature of threats, and the likelihood and magnitude of the risks arising from those threats, to specific information assets.
- the technical environment, including whether the realization of those threats or the exploitation of vulnerabilities related to specific information assets that appear inconsequential could expose (either directly or indirectly) the information assets and result in controls that were not effective to achieve the entity's cybersecurity objectives. For example, if access to the information assets of a financially immaterial business unit could provide access to the entity's strategic business systems, and the practitioner determines there is a high likelihood that such a vulnerability might be exploited, the practitioner is likely to consider access to the information assets of the financially immaterial business unit to be material in the cybersecurity risk management examination.
- the nature of threats arising from error or fraud, and the likelihood and magnitude of the risks arising from such threats, to the operation of processes and controls that support the achievement of the entity's cybersecurity objectives, and the vulnerabilities of those processes and controls to those threats. For instance, the security operation center staff's lack of knowledge regarding new types of cyberattacks may result in the failure to detect, in a timely manner, a security incident that could significantly affect the entity's achievement of its cybersecurity objectives; consequently, this deficiency could result in a material failure to achieve a cybersecurity objective.

3.40 The practitioner should consider both qualitative and quantitative factors when evaluating control effectiveness. Qualitative factors the practitioner considers include the following:

- *Relevance of a control to achieve a particular cybersecurity objective based on the control criteria.* Not all controls that have been implemented need to be considered if the control criteria are met through the application of other controls. As an example, assume an entity mirrors data to a data center located in another city and creates tapes of the data as a secondary backup. These tapes are stored at a third location. Data written to the backup tapes is encrypted. The entity has identified the encryption of the tape as a control; however, the entity has not identified physical security controls over the tape storage location in its description because management concluded that
  - — the risk that both the primary data center and the mirror site are destroyed simultaneously is remote and
  - — encryption of the data on the tapes is sufficient to achieve the entity's cybersecurity objectives with regard to

protecting the confidentiality of the information based on the control criteria.

In this example, physical access controls over the tape storage location are unlikely to be material or relevant because controls over the encryption of the tapes prevent unauthorized access.

- *Alignment between the key security policies and processes included in management's description and the underlying controls within the entity's cybersecurity risk management program.* If management's description includes a particular system in the entity operations summary or in the listing of information assets, it is likely that report users would presume that system is material for the purposes of the cybersecurity risk management examination. Similarly, report users are likely to expect that controls that, individually or in combination with other controls, support the key security policies and processes described in management's description would ordinarily be tested and evaluated as part of the evaluation of control effectiveness.
- *Practitioner's understanding of previous communications made to report users regarding cybersecurity.* If the practitioner becomes aware that the entity has made representations to report users regarding cybersecurity (for instance, through a presentation on the entity's website that indicates that all client data is kept encrypted at all times), the practitioner is likely to consider those representations important to such users.
- *Relevance to compliance with laws and regulations.* If the entity is subject to requirements specified by laws or regulations related to cybersecurity, identified deficiencies and deviations related to compliance are likely to be significant since they may have additional consequences to the organization. Requirements established by laws and regulations may therefore need to be included in the consideration of materiality and the related engagement strategy. For laws and regulations that have a direct effect (for example, laws protecting sensitive personal health information), the entity may establish cybersecurity objectives regarding compliance with such laws. Other laws and regulations may be less directly linked to the cybersecurity objectives but may still be relevant to the examination (for example, regulations over the physical storage of biohazard materials, when the materials are stored in a warehouse with access secured by an electronic badging system).
- *Interactions with third parties.* Materiality considerations are based on factors such as the likelihood and magnitude of cybersecurity risks arising from interactions with third parties (customers, vendors, business partners, or others) with access to the entity's system, the degree to which those risks are relevant to the entity's cybersecurity risk management program, and the extent to which the entity monitors controls performed by those third parties.
- *Indicators of the operating effectiveness of cybersecurity performance activities.* Indicators of the operating effectiveness of

control activities, such as the number and nature of security events resulting in a loss, the mean time from first occurrence to detection, and the mean time from detection to remediation, may be indicative of challenges in the design or operating effectiveness of cybersecurity controls; accordingly, such factors may affect materiality judgments.

- *Degree to which controls are designed to identify and address threats and vulnerabilities that are currently unknown*. Certain controls may have the ability to detect and address unknown threats. An example of this is a data loss prevention (DLP) control that monitors and restricts outbound information, regardless of what caused the attempt to send the information externally.
- *Threats related to prior periods.* An identified threat or vulnerability in a prior period may affect the assessment of the entity's cybersecurity risk management program or the effectiveness of controls for the current period.
- *Effect of deviations.* Identified deviations may affect the entity's ability to mitigate threats or vulnerabilities to information and other assets and achieve the related cybersecurity objectives. For example, the practitioner may question management's assertion that a control is effective when considering the nature and extent of observed deviations in the operation of the control.
- *Intentional acts*. A deficiency or deviation may be the result of an unintentional act or may be intentional. An intentional act perpetrated by management or senior management would be particularly relevant to materiality considerations.
- *Relationship to other parties.* A deficiency in controls may relate to the relationship between the entity and other parties. For example, a deficiency in controls at the entity that could also result in a deficiency in controls at a customer is more likely to be considered material.

3.41 Quantitative factors to be considered in a cybersecurity risk management examination relate to matters such as the tolerable rate of deviation and the observed rate of deviation. (In this guide, the tolerable rate of deviation is the maximum rate of deviation in the operation of the control that the practitioner is willing to accept without modifying the opinion relating to one or more of the control criteria.) Quantitative factors are less likely to apply when evaluating the design of controls but would be considered when evaluating the operating effectiveness of the controls. Note, however, that the practitioner should carefully consider the effect of identified deviations, either individually or in combination with other identified deviations, on the controls' ability to mitigate assessed risks because such deviations could result in the failure to achieve one or more of the entity's cybersecurity objectives.

3.42 Paragraph .17 of AT-C section 205 indicates the practitioner should reconsider materiality if the practitioner becomes aware of information during the engagement that would have caused him or her to have initially determined a different materiality.

Obtaining and Evaluating Evidence About the Suitability of the Design of Controls to Achieve the Entity's Cybersecurity Objectives

3.43 As discussed in chapter 1, the practitioner's opinion on the effectiveness of controls encompasses both the suitability of the design of controls and their operating effectiveness. Because there are specific considerations when evaluating each, this chapter contains separate discussions of suitability of design and operating effectiveness to support the overall opinion on the effectiveness of controls to achieve the entity's cybersecurity objectives. This section discusses evaluating the suitability of design, whereas the section beginning in paragraph 3.57 discusses evaluating the operating effectiveness of controls.

3.44 Paragraph .15 of AT-C section 205 states that the practitioner's understanding of the controls within an entity's cybersecurity risk management program includes an evaluation of the design of controls within that program and whether they have been implemented. Suitably designed controls, if complied with satisfactorily, provide reasonable assurance of achieving the entity's cybersecurity objectives based on the control criteria. Suitably designed controls operate as designed by persons who have the necessary authority and competence to perform the controls.

3.45 Matters that are relevant in determining whether controls are suitably designed include the following:

- Whether the applicable control or set of controls adequately addresses the risks that threaten the achievement of the entity's cybersecurity objectives based on the control criteria
- Whether the applicable control or set of controls, if operated effectively, would protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented
- Whether the information used in the operation of the controls is reliable. For example, the operation of a control may rely on configuration parameters of the comparison of the data to another set of data that is expected to be complete and accurate.
- Whether the applicable control or set of controls is adequately changing, adapting, and evolving, from a cyber-threat monitoring perspective, as new threats and exploits are identified and become able to be defended against by entities.

3.46 Management is responsible for designing and implementing controls to achieve the entity's cybersecurity objectives, identifying the risks that threaten the achievement of the objectives, modifying the controls as necessary based on new and evolving risks, and evaluating the linkage between the controls and the evolving risks and threats that threaten the achievement of the objectives. In many cases, the practitioner is able to obtain management's documentation of its identification of risks and evaluation of the linkage of controls to those risks. In these instances, the practitioner may evaluate the completeness, accuracy, relevance, and timeliness of management's identification of risks and the design of the controls in mitigating those risks. The practitioner may also contemplate whether the controls designed and implemented

by management achieve the cybersecurity objectives based on the current operating environment, the known risks and threats as of a given point in time, and the exploitation of evolving vulnerabilities.

3.47 When considering the suitability of design, the practitioner should also consider (*a*) management's process for assessing risks and for designing and implementing controls to address those risks, (*b*) the results of walkthroughs, and (*c*) evidence about the operating effectiveness of controls that indicated a deficiency in the design of the controls, in light of the practitioner's knowledge and experience and the particular circumstances. Controls are intended to mitigate the risks that the entity's cybersecurity objectives will not be achieved. For example, the risk that a server will not be able to support availability in the event of a distributed denial of service attack can be addressed by a control that provides redundant load balanced infrastructure protected by mechanisms for detecting and dropping access attempts.

3.48 Identified risks that may impact the achievement of the entity's cybersecurity objectives also encompass fraud such as management's override of identified controls at the entity, misappropriation of assets by entity personnel, creation by entity personnel of false or misleading documents or records, and inappropriate physical and logical access controls to information and the underlying infrastructure through social engineering attacks or similar measures. The practitioner should consider both the risk of fraud and errors in evaluating the suitability of the design of controls.

3.49 The practitioner's evaluation of management's risk assessment process (that is, the assessment of potential events and circumstances that could threaten the achievement of the entity's cybersecurity objectives) includes consideration of items such as the following:

- The process management uses to
  - — identify its cybersecurity objectives,
  - — identify information and other assets,
  - — determine the threats to information and other assets,
  - — design and implement controls to address identified risks, and
  - — incorporate information from its monitoring activities that identify previously unconsidered potential events and circumstances
- The frequency with which management updates the risk assessment and supporting risk management processes and controls
- Whether management uses an appropriate management framework for managing its processes and controls (for example, the National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity" [NIST cybersecurity framework] or International Standardization Organization/International Electrotechnical Commission [ISO/IEC] Standards 27001 and 27002) as part of its assessment and management process

3.50 Factors such as the size and complexity of the entity, the goods or services provided, and commitments made to customers and others are important considerations when evaluating the suitability of the design of controls.

A smaller, less complex entity may be able to address risks that threaten the achievement of the entity's cybersecurity objectives using a different set of controls than a larger, more complex entity. For example, a smaller, less complex entity may

- have policies and procedures that are less formal and detailed but sufficient for the practitioner to evaluate;
- have fewer levels of management, which may result in more direct oversight of the operation of key controls; and
- make greater use of manual controls versus automated controls.

3.51 When considering suitability of design, the practitioner may determine that some information assets (such as network access points, databases, or transactions) are subject to greater threats or have vulnerabilities that are more likely to be exploited. In such instances, control activities designed and implemented to prevent or detect security events associated with these threats and vulnerabilities may require greater precision and reliability in order to be suitably designed.

3.52 The practitioner evaluates the suitability of the design of controls by using evidence and other information obtained when

- obtaining an understanding of the cybersecurity risk management program and the controls within that program;
- determining whether the description of the entity's cybersecurity risk management program was presented in accordance with the description criteria (including evidence obtained from performing walkthroughs); and
- performing a combination of the following procedures:
  - Inquiry of entity personnel regarding the design and operation of applicable controls and the types of security events that have occurred or that may occur
  - Inspection of documents produced by the entity
  - Performing additional walkthroughs of control-activity-related policies and procedures
  - Reading applicable and supporting program documentation
  - Determining whether attacks and vulnerability exploitations, including those that are well established in the hacker community as well as emerging risks and threats, are addressed to achieve the entity's cybersecurity objectives

3.53 To evaluate the suitability of the design of the controls within the entity's cybersecurity risk management program, the practitioner should consider the following information about the controls:

- The frequency or timing of the occurrence or performance of the control
- The authority and competence of the individual responsible for conducting the activity (for example, details regarding the appropriateness of the level of the individual performing the control, their role in the organization, and conflicting duties).

- The tasks within the activity being performed and the precision and sensitivity of those tasks (for example, the results of reviews and related follow-up activities)
- Contrary evidence that the control is not functioning as designed, such as the rate of security incidents identified related to the control

3.54 After performing the procedures and considering the guidance in paragraphs 3.38–3.42, the practitioner should consider whether the controls have the ability, as designed, to provide reasonable assurance of achieving the entity's cybersecurity objectives based on the control criteria. Further, the practitioner should consider whether the appropriate controls are in fact in place given the circumstances.

Identifying and Evaluating Deficiencies in the Suitability of Control Design

3.55 In determining whether there is a deficiency in the design of a control, the practitioner determines whether

- a control necessary to meet the one or more control criteria is missing or
- an existing control is not properly designed, meaning that, even if the control operates as designed, one or more control criteria would not be met.

3.56 When evaluating the suitability of the design of controls, the practitioner determines whether the controls are appropriate and whether they have been implemented. If a necessary control does not exist, this would be considered a design deficiency. If deficiencies exist in the design of a control, the practitioner often would not test the operating effectiveness of that control. Rather, the practitioner generally would consider the design of other controls that address the same risks.

Obtaining Evidence About the Operating Effectiveness of Controls to Achieve the Entity's Cybersecurity Objectives

3.57 Controls are suitably designed if they have the potential to achieve the entity's cybersecurity objectives based on the control criteria. Suitably designed controls are operated as designed by persons who have the necessary authority and competence to perform the control. Controls that operated effectively provide reasonable assurance of achieving the entity's cybersecurity objectives based on the control criteria.

3.58 A control may be designed to address an identified risk on its own or may function in combination with other controls. For example, when a supervisor, prior to approving user credentials, is reviewing the list of authorized users to determine whether a new user has been authorized by the entity to access one or more of its systems, the review control (reviewing and approving the user's credentials) may be complemented by an application control requiring that the supervisor acknowledge his or her review and approval by entering a sign-off in the system. In this instance, both the manual and automated controls would be tested by the practitioner because the two controls are dependent on each other.

3.59 The practitioner should obtain information from management regarding changes made to controls during the period covered by the practitioner's report. In addition, during the performance of his or her procedures, the practitioner is alert for any changes that may not have been identified by management. If the practitioner believes the control changes could be significant to users of the report and could be relevant to meeting one or more of the control criteria, both the superseded controls and the updated controls would be included in the controls the practitioner would test.

Designing and Performing Procedures to Evaluate the Operating Effectiveness of Controls

3.60 Paragraph .24 of AT-C section 205 requires the practitioner to design and perform tests of controls to obtain sufficient appropriate evidence about the operating effectiveness of controls. The practitioner is responsible for determining the nature (how the controls are tested), timing (when the controls are tested and the frequency of the testing), and extent (the number of testing procedures performed or size of the sample) of testing necessary to provide sufficient and appropriate evidence that the controls operated effectively throughout the specified period of time.[3]

3.61 When determining the nature, timing, and extent of procedures to be performed to obtain sufficient appropriate evidence of the operating effectiveness of controls, the practitioner should consider the type of evidence that can be obtained from the performance of the control and how long that evidence will be available.

3.62 If the practitioner determines that certain entity-level controls (control environment, communication and information, risk assessment, and monitoring controls) did not operate effectively, the practitioner may be able to adjust the nature, timing, and extent of procedures performed to obtain evidence about whether the entity's controls were effective to achieve the entity's cybersecurity objectives. In some situations, deficiencies in the operation of entity-level controls may lead the practitioner to conclude that controls are not operating effectively to achieve certain cybersecurity objectives. For example, consider an entity whose ability to retain knowledgeable employees has been impaired. The practitioner may decide to increase the testing of controls that prevent and detect security incidents (for example, inspection of security configurations and event management scan logs) to determine whether controls operated effectively to achieve the cybersecurity objectives based on the control criteria.

Nature of Procedures to Evaluate the Effectiveness of Controls

3.63 When designing and performing tests of controls, the practitioner

a. makes inquiries and performs other procedures to obtain evidence about the following:
   i. How the control was implemented (For example, was the control performed as designed?)
   ii. The level of consistency with which the control was applied throughout the period

[3] If the cybersecurity risk management examination is as of a *point in time*, the practitioner's responsibility is the same. However, the practitioner's considerations related to the nature, timing, and extent of procedures to perform to obtain sufficient appropriate evidence will differ from those performed when the examination is for a *specified period of time.*

iii. By whom or by what means the control was applied (For example, is the control automated or manual? Has there been high turnover of personnel in the position that performs the control? Is the control being performed by an inexperienced person?)

b. determines whether the controls to be tested depend on other controls and, if so, whether it is necessary to obtain evidence supporting the operating effectiveness of those other controls.

c. determines an effective method for selecting the items to be tested to meet the objectives of the procedure.

3.64 Other procedures that the practitioner performs, in combination with inquiry, to obtain evidence about the operating effectiveness of controls include one or more of the following:

- Observation of the application of the control
- Inspection of documents, reports, or electronic files that contain evidence of the performance of the control, such as system log files
- Reperformance of certain controls performed by management, such as access recertification and security event log reviews

3.65 Because of the nature and methods of information storage used in the operation of cybersecurity control activities, the practitioner may find the use of analytics to be a highly effective technique in performing his or her procedures, such as in the following examples:

- Documentation of authorization of approvals of management may be stored in an online workflow system permitting the records from the system to be extracted and analyzed.
- System logs may be scanned for unusual activity.
- Server security configuration parameters may be scanned and analyzed for consistency with policy.
- Access control lists can be analyzed for appropriateness of access rules.

When using analytics, the practitioner would perform procedures to validate the completeness and accuracy of the information received from the entity.

3.66 Inquiry alone does not provide sufficient appropriate evidence of the operating effectiveness of controls. Some procedures provide more convincing evidence of the operating effectiveness of controls than others (for example, inquiry combined with inspection or reperformance ordinarily provides more convincing evidence than inquiry and observation alone).

3.67 The type of control being tested may affect the nature, timing, and extent of the testing performed by the practitioner. For example, for some controls, operating effectiveness is evidenced by documentation. In such circumstances, the practitioner may inspect the documentation. Other controls may not leave evidence of their operation that can be tested at a later date, and accordingly, the practitioner may need to test the operating effectiveness of such controls at various times throughout the specified period via observation.

3.68 Evidence of the operating effectiveness of a control may be lost, misplaced, or inadvertently deleted by the entity. In such instances, the practitioner determines whether other evidence of the operating effectiveness of the control

exists and whether the results of tests would provide sufficient appropriate evidence. If not, the practitioner should consider whether there are other effective controls in place to achieve the entity's cybersecurity objectives based on the control criteria. If certain limitations exist in the ability to retain evidence (such as security logs), the practitioner may plan to obtain such evidence at multiple intervals throughout the examination period.

3.69 In addition to procedures to directly test the operation of a control, the practitioner may also perform procedures to obtain evidence about whether the control functioned to prevent or detect errors and fraud. For example, when testing the effectiveness of an entity's vulnerability scanning controls, the practitioner may use his or her own vulnerability scanning tool to detect unidentified vulnerabilities in order to assess the effectiveness of the entity's controls. As another example, the practitioner might obtain a listing of the security incidents identified during the period and compare the vulnerabilities exploited to the controls implemented to protect information and other assets in order to identify deficiencies in the design or operation of the related control activities.

Evaluating the Reliability of Information Produced by the Entity

3.70 When using information produced by the entity, paragraph .35 of AT-C section 205 requires the practitioner to evaluate whether the information is sufficiently reliable for the practitioner's purposes, including, as necessary, the following:

a. Obtaining evidence about the accuracy and completeness of the information

b. Evaluating whether the information is sufficiently precise and detailed for the practitioner's purposes

3.71 Examples of information produced by the entity's information system include the following:

- Population lists the practitioner uses to select a sample of items for testing
- Manually prepared or system-generated reports
- Exception reports generated by the system
- Ad hoc request reports
- Documentation that provides evidence of the operating effectiveness of controls, such as user access lists
- Logs from security tools (for instance, data loss prevention, network activity, vulnerability scans)

3.72 The results of the practitioner's tests will not be reliable if the population from which the items have been selected for testing is incomplete. As an example, the effectiveness of a control, such as the periodic review of user access, is affected by the completeness and accuracy of the information used to prepare the user access reports. In this situation, the practitioner would inspect the scripts used to create user access reports for accuracy of logic.

3.73 The practitioner identifies the information produced by the entity while performing procedures to assess the design, implementation, and operating effectiveness of controls within the entity's cybersecurity risk management program. When assessing the information produced, the practitioner should consider the reliability of the information, specifically the completeness and

accuracy of the information. For example, if the practitioner intends to test a population of user terminations during the period under examination, the practitioner would perform procedures to determine that the lists of terminated users generated from human resource management systems are complete and accurate.

3.74 The information may be produced only once or on a recurring basis for use in the execution of a control. The information may be produced manually by management or generated from a system. When the information produced by the entity is provided to the practitioner, the practitioner assesses how the information is used, the source of the information, and the impact the information could have on the engagement.

3.75 Depending on the means by which the practitioner obtains the information, the practitioner would develop a plan to assess the completeness and accuracy of the data. The information may also provide evidence of the operating effectiveness of a control. When assessing information used in the execution of controls, the practitioner should consider the following factors:

- The level of assurance being sought from the control
- The degree to which the effectiveness of the control depends on the completeness and accuracy of the information
- The precision with which the control is performed (for example, precision of review controls)
- The degree to which the control depends on other controls

3.76 Additional items to be considered by the practitioner when assessing the completeness and accuracy of information may include the following:

- Where is the information produced or generated from—the entity's applications or systems, other sources, or third parties?
- Is the information located in a controlled information technology environment or an ad hoc reporting database or data warehouse?
- Is the information highly structured and complex or relatively straightforward?
- What is the basis for the entity's comfort regarding the completeness and accuracy of the data or information?

3.77 Determining the nature and extent of evidence needed to assess the completeness and accuracy of data is a matter of professional judgment. When obtaining evidence about the completeness and accuracy of the information, the practitioner may perform this as part of his or her tests of the effectiveness of controls or may develop specific procedures to be applied to the information received. The more important the control or information, the more persuasive the evidence needed about the completeness and accuracy of the information. In addition, the practitioner should considers the need to ascertain the completeness and accuracy of the information throughout the period covered by the cybersecurity risk management examination.

3.78 The following are examples of procedures the practitioner may perform when the information being tested has been produced by the entity:

- *Example 1 (Population of incidents)*. The incident management recordkeeping application generates a report of all incidents during a period. Before testing a sample of such incidents, the

practitioner may inspect the query logic used to generate the report and perform a walkthrough of the process used to record incidents in the application. The practitioner may also inspect the report for anomalous gaps in sequence or timing to determine completeness.

- *Example 2 (Population of changes)*. The change management system is used to communicate changes ready for implementation. Before testing a sample of changes to application software, the practitioner may perform a walkthrough of the process used to communicate changes ready for implementation in order to understand whether any alternate paths of communication exist. The practitioner would also assess the segregation of duties between those responsible for the development and testing of the changes and those responsible for migration of changes to the production environment. The practitioner would also consider the enforcement of the segregation of these duties through logical access controls.
- *Example 3 (Population of servers)*. All servers are included in vulnerability scans. Before testing the results of a sample of vulnerability scans, the practitioner would ascertain the process for performing the vulnerability scans (for example, subnet scanning, manually adding server names) and the configurations used to include the entity's relevant environments. The practitioner would need to understand and consider how the server build-out process is conducted and how servers are migrated to the relevant environments to be included in the scanning.

Timing of Procedures

When the Examination is for a Specified Period of Time

3.79 When the examination is for a period of time specified by management, the practitioner should obtain evidence about the operating effectiveness of controls over the period of time covered by the examination to support the opinion. Based on consideration of a number of factors, the practitioner may decide to perform procedures at interim dates, at the end of the examination period, or after the examination period, when evidence of the operation of controls during the period is available after the end of the period. The following are some relevant factors to consider when determining the timing of procedures:

- The nature of the controls
- The period of time during which the information will be available (for example, electronic files may be overwritten after a period of time or hard copy records may not be retained)
- Whether testing requires direct observation of a procedure that is only performed at certain times during the examination period
- Whether the control leaves evidence of its operation and, if not, whether the control must be tested through observation

3.80 Performing procedures at an interim date and communicating deviations and deficiencies to management at an early stage in the examination may provide management with an opportunity to make changes in the design

or operation of controls to correct the deviations for the remaining portion of the examination period.

3.81 When the practitioner performs tests of the operating effectiveness of controls at an interim period, the practitioner should determine what additional testing is necessary for the remaining period.

When the Examination is as of a Point in Time

3.82 When the practitioner is reporting as of a point in time, the practitioner should obtain sufficient appropriate evidence about the operating effectiveness of controls. Because not all controls will operate on a daily basis, the practitioner should consider the timing of his or her procedures over an appropriate interval prior to the point in time at which effectiveness is evaluated. Furthermore, a single instance of the operation of a control may not provide sufficient appropriate evidence that a control is operating effectively. In establishing the nature, timing, and extent of procedures to be performed when reporting as of a point in time, the practitioner determines the timeframe over which the operation of a control can be tested to support his or her conclusion as of the specified point in time, as well as the number of instances of the operation of the control necessary to conclude on the effective operation of the control. All such decisions are a matter of professional judgment.

Extent of Procedures

3.83 The practitioner should design and perform tests of controls and other procedures to obtain sufficient appropriate evidence that controls operated effectively throughout the period to achieve the entity's cybersecurity objectives based on the control criteria. Relevant factors in determining the extent of tests of controls include the following:

- The nature of the controls
- The frequency of the performance of the control during the period (for example, daily management review of open incidents versus monthly review of closed incidents to identify ongoing problems)
- The relevance and reliability of the evidence that can be obtained to support the conclusion that the controls operated effectively to meet the control criteria
- The extent to which evidence is obtained from tests of other controls designed to meet the same criterion

3.84 The practitioner should obtain evidence about the operating effectiveness of controls throughout the examination period. In some cases, however, a control may not operate frequently enough to be assessed as operating effectively. For example, if a control operates only annually in December, and the examination covers the six-month period from January 1, 20XX, to June 30, 20XX, the practitioner is unable to test the operating effectiveness of that control throughout the period. In other instances, a control may not operate because the circumstances that trigger its operation do not occur during the period covered by the examination. The latter situation is discussed further beginning in paragraph 3.99.

3.85 The shorter the test period, the greater the risk that controls may not have operated effectively throughout the period or that the practitioner will be unable to obtain sufficient evidence to express an opinion on the operating effectiveness of those controls. For example, testing the operation of a monitoring

activity for only a limited portion of the examination period may not be indicative of the associated control's effectiveness throughout the period. Depending on the significance of the controls to the achievement of the entity's cybersecurity objectives based on the control criteria, the practitioner may decide to express a qualified opinion or disclaim an opinion because of the limitation on the scope of the engagement.

3.86 When evaluating the operating effectiveness of controls, the practitioner may consider the results of tests performed while providing other services to the entity. Furthermore, deviations in the operation of a control identified during the prior year's examination may impact the practitioner's risk assessment for that control, which may cause the practitioner to increase the extent of testing in the current period. For example, if the practitioner's opinion in the prior year was qualified because of deficiencies in controls over the authorization of user access due to the inexperience of the person performing the controls, the practitioner may decide to increase the number of items tested in the current examination period to determine if the deficiency has been effectively corrected.

3.87 An automated control usually functions consistently unless the program, including the tables, files, or other permanent data used by the program, is changed. Once the practitioner determines that an automated control is functioning as intended, which could be determined at the time the control is initially implemented or at some other date, the practitioner should perform tests to determine that the control continues to function effectively. Such tests ordinarily would include determining that changes to the program are not made without being subject to the appropriate program change controls, that the authorized version of the program is used for processing transactions, and that other relevant controls are effective.

3.88 If a control operates frequently, the practitioner may consider whether to use audit sampling when testing the operating effectiveness of the control. When determining the extent of tests of controls and whether sampling is appropriate, the practitioner should consider (*a*) the characteristics of the population of the controls to be tested, including the nature of the controls, (*b*) whether the population is made up of homogenous items, (*c*) the frequency of their application, and (*d*) the expected deviation rate. The AICPA Audit Guide *Audit Sampling* may be useful to the practitioner when performing sampling.

3.89 Before deciding to use sampling in a cybersecurity risk management engagement, the practitioner should consider whether sampling is an appropriate strategy for testing the control. For example,

a. due to the design of one or more systems, it may not be possible to give every item in the population a chance of being selected for the sample.

b. the practitioner may determine that a 100 percent test of the control using data analytics is necessary because even a one-time failure of the control could result in failure to achieve the entity's cybersecurity objectives.

c. the practitioner may conclude that it is more efficient and more effective to perform a 100 percent test of the data evidencing the effective operation of the control than selecting and testing a sample.

In such circumstances, sampling may not be an appropriate approach to obtaining sufficient appropriate evidence to evaluate the effectiveness of the control. Consequently, in applying professional judgment regarding the extent of testing, the practitioner needs to consider whether the assumptions for sample-based testing have been met.

Selecting Items to Be Tested

3.90 For tests of controls using sampling, the practitioner determines the tolerable rate of deviation and uses that rate to determine the number of items to be selected for a particular sample.

3.91 The practitioner's selection of sample items should be reasonably expected to be representative of the population, resulting in a sample that is representative of the population covering the reporting period. Random-based selection of items represents one means of obtaining such samples.

Testing Changes to Controls

3.92 If, during the examination period, the entity makes changes to controls that are relevant to achieving the entity's cybersecurity objectives based on the control criteria, the practitioner should test, if possible, the superseded controls before the change and test the new controls after the change for the period they were in effect and consider whether the change in control was appropriately addressed in the description of the system. For example, assume that during the examination period June 1, 20X0, to May 31, 20X1, the entity automated a control that was previously performed manually. If the entity automated the control on December 15, 20X0, the practitioner would test the manual control for the period from June 1, 20X0, to December 14, 20X0, and test the automated control for the period from December 15, 20X0, to May 31, 20X1. If the practitioner cannot test the superseded controls (for example, because the controls did not leave evidence of operation after a period of time or the practitioner was engaged after the controls were superseded), the practitioner should determine the effect on the practitioner's report.

Risk Mitigation and Control Considerations Related to Third Parties

3.93 Given the prevalence and ease with which information, operations, and processes are shared and exchanged across traditional organizational boundaries, an entity needs to carefully consider the cybersecurity risks posed by interactions with third parties.

3.94 As discussed in chapter 2, third parties include customers, vendors, business partners, and others with access to one or more of the entity's information systems who store confidential entity information on their systems, or who otherwise transmit information back and forth between themselves and the entity, or on behalf of the entity. Consider the following:

- *Vendor performs cybersecurity processes and controls*. An entity may engage a service provider to perform cybersecurity processes and controls. Examples of such processes and controls include the following:
  - The performance of periodic vulnerability scans, penetration tests, and other critical monitoring activities;

- The deployment of proprietary cybersecurity breach detection sensors throughout the entity's IT network and the monitoring and investigation of security events detected by those sensors; and
- The preparation of and reporting of customer analytics related to the entity's system

- *Vendor accesses entity's information assets.* An entity may permit a vendor to access its raw materials inventory system and production schedules in order to time the delivery of shipments of production inputs.

This access to the entity's systems by a third party gives rise to additional vulnerabilities to the entity's IT systems that could be exploited and result in controls that are not suitably designed to achieve one or more of the entity's cybersecurity objectives.

3.95 In response to such risks from third parties, management needs to understand the nature of the cybersecurity risks posed by the third parties, assess the likelihood and magnitude of such risks, and design and implement monitoring controls to address those risks. Management also needs to recognize and acknowledge that, even after implementing its strategy, management will be dependent on the cybersecurity risk management and control activities of the third party. For this reason, among others, it is important that management participate in ongoing communications with third parties to discuss changes to the third parties' processes and controls as the need arises.

3.96 The entity's cybersecurity risk management program ordinarily includes procedures to properly identify and assess the cybersecurity risks posed by third parties and to implement monitoring controls to address those risks. Such procedures and controls are commonly included in a third-party risk management program. Among other things, a third-party risk management program often includes procedures to obtain evidence about the effectiveness of the third party's processes and controls.

3.97 When determining the nature, timing and extent of procedures to obtain evidence about whether the entity's monitoring controls over the third party's processes and controls were effective in the circumstances, the practitioner's procedures ordinarily will depend upon the nature and extent of the entity's monitoring controls. For example, if the entity has obtained a type 2 SOC 2 report on aspects of a third party's operations that relate to the processing integrity of its services, as well as its security, availability, and confidentiality controls, the practitioner might review the report to determine whether management has adequately evaluated it by assessing (*a*) the relevance of the system description and complementary user entity controls to its own cybersecurity risk management program and (*b*) any deviations requiring further evaluation and response by management. If the third party does not provide management with a type 2 SOC 2 report, management may perform direct testing of the third party's controls by obtaining evidence from that party of the effectiveness of its controls. However, unless the practitioner is reperforming management's tests of the third party's controls, the practitioner's performance of tests directly on the third party's controls would not provide evidence about the effectiveness of the entity's cybersecurity controls. In any event, the practitioner should obtain sufficient appropriate evidence of the effectiveness of the third party's controls. In addition, the practitioner needs to consider whether the third party's use of

its own IT system and connections to the entity's IT network and assets represents new vulnerabilities that need to be assessed and addressed as part of the entity's third-party risk management program.

3.98 When evaluating the effectiveness of the controls within the entity's cybersecurity risk management program, the practitioner needs to conclude on whether the entity's monitoring controls over the processes and controls performed by third parties are effective to achieve the entity's cybersecurity objectives. When the practitioner is unable to reach such a conclusion, or when the practitioner determines that such activities were ineffective to achieve the entity's cybersecurity objectives, the practitioner's report should be modified accordingly.

Controls Did Not Need to Operate During the Period Covered by the Practitioner's Report

3.99 Management's description of the entity's cybersecurity risk management program includes, among other things, a description of the key security policies and processes that ordinarily operate during the period covered by the cybersecurity risk management examination report. In some cases, however, the circumstances that trigger the operation of certain of those processes do not occur; therefore, some or all of the related controls do not operate during the period covered by the cybersecurity risk management examination report. For example, if no identified security incidents required the recovery of systems, data, or other information assets, the recovery controls (such as restoring systems and data from clean backups and replacing compromised files) would not operate. When management informs the practitioner that the events requiring the operation of a control did not occur, the practitioner should obtain sufficient appropriate evidence to corroborate management's statement. Reporting in this situation is discussed in chapter 4, "Forming the Opinion and Preparing the Practitioner's Report."

Revising the Risk Assessment

3.100 Paragraph .34 of AT-C section 205 clarifies that the practitioner's assessment of the risks of material misstatement may change during the course of the engagement as additional evidence is obtained. In circumstances in which the practitioner obtains evidence from performing further procedures or when new information is obtained, either of which is inconsistent with the evidence on which the practitioner originally based the assessment, the practitioner should revise the risk assessment and modify the planned procedures accordingly. This may require the performance of additional procedures as necessary.

Using the Work of Internal Auditors

3.101 Chapter 2 of this guide discusses a practitioner's considerations with respect to understanding the nature of the internal audit function's responsibilities, and the activities it performs, to determine whether to use the work of internal audit during the cybersecurity risk management examination. For situations in which the practitioner decides to use the work of the internal audit function in the cybersecurity risk management examination, chapter 2 also addresses the need to obtain written acknowledgment from management that internal auditors providing direct assistance will be allowed to follow the

practitioner's instructions without management's interference, the evaluation of the objectivity and technical competence of members of the internal audit function, and the coordination of procedures with them, among other matters. This section discusses the practitioner's responsibility to test the work of the internal audit function to determine whether it is adequate for the examination.

3.102 When using the work of the internal audit function, paragraph .40 of AT-C section 205 requires the practitioner to perform sufficient procedures, including reperformance, on the body of work of the internal audit function that the practitioner plans to use in order to evaluate whether such work is adequate for the practitioner's purposes.

3.103 The nature, timing, and extent of procedures the practitioner performs in evaluating the adequacy of that work depends on the practitioner's assessment of the significance of that work to the practitioner's conclusions (for example, the significance of the risks that the controls are intended to mitigate). Such procedures usually consist of one or more of the following:

- Independent testing of items tested by the internal audit function (reperformance)
- Independent selection of items from the population tested by internal audit and the performance of testing of items of a similar nature that were performed by internal audit to independently evaluate internal audit's conclusion

3.104 Some relevant factors in determining whether to use the work of the internal audit function to obtain evidence about the operating effectiveness of controls include the pervasiveness of the control, the potential for management override of the control, and the degree of judgment and subjectivity required to evaluate the effectiveness of the control. As the significance of these factors increases, so does the need for the practitioner, rather than the internal audit function, to perform the procedures, and conversely, as these factors decrease in significance, the need for the practitioner to perform the tests decreases.

3.105 To prevent undue use of the internal audit function in obtaining evidence, the practitioner uses less of the work of the internal audit function and performs more of the work directly when more judgment is involved in planning and performing relevant procedures or in evaluating the evidence obtained. Such situations are likely to occur when

- the assessed risk of material misstatement is higher;
- the internal audit function's organizational status and relevant policies and procedures that adequately support the objectivity of the internal auditors are lower; and
- the level of competence of the internal audit function is lower.

3.106 The practitioner uses professional judgment in performing procedures to evaluate the work performed by the members of the entity's internal audit function. As discussed in chapter 2, the practitioner is responsible for determining the work to be performed and obtaining sufficient appropriate evidence for the opinion. The practitioner has sole responsibility for the opinion expressed in the practitioner's report, and that responsibility is not reduced by the practitioner's use of the work of the internal audit function.

3.107 If the practitioner finds that the quality and extent of the work performed by the members of the entity's internal audit function are not equivalent to the quality and extent of work the practitioner would have performed, the practitioner generally will perform additional procedures and consider the extent to which the work of the internal audit function may be used to obtain evidence.

3.108 In reviewing internal audit reports, the practitioner evaluates exceptions[4] identified by the members of the entity's internal audit function to determine whether those exceptions require the practitioner to alter the nature, timing, and extent of the practitioner's procedures. The practitioner ordinarily corroborates exceptions identified by the members of the internal audit function and considers the extent of the exceptions, their nature and underlying causes, and whether additional procedures by the practitioner are necessary.

3.109 Another relevant factor in evaluating the adequacy of the work of the internal audit function is the adequacy of the sampling procedures used and whether the sampling procedures were appropriate and free from bias (that is, whether all items in the population have the same opportunity to be selected). The AICPA Audit Guide *Audit Sampling* provides additional guidance that may be useful to a practitioner who has decided to use audit sampling in performing procedures.

3.110 If the size of the sample used by the members of the entity's internal audit function is less than the sample size the practitioner would have used, the practitioner generally would select additional items to achieve the required sample size. For example, if internal audit has selected a sample of 25 items for testing, the practitioner may determine that an additional 15 items need to be tested.

3.111 The responsibility to report on management's description of the entity's cybersecurity risk management program and the effectiveness of controls rests solely with the practitioner and cannot be shared with the internal audit function. Therefore, the judgments about the significance of deviations in the effectiveness of controls, the sufficiency of procedures performed, the evaluation of identified deficiencies, and other matters that affect the practitioner's opinion are those of the practitioner. In making judgments about the extent of the effect of the work of the internal audit function on the practitioner's procedures, the practitioner may determine, based on the risk associated with the controls and the significance of the judgments relating to them, that the practitioner will perform the work relating to some or all of the controls, rather than using the work performed by the internal audit function.

3.112 When using internal auditors to provide direct assistance to the practitioner, paragraph .42 of AT-C section 205 requires the practitioner to direct, supervise, and review the work of the internal auditors. The practitioner fulfills that responsibility by (*a*) informing the internal auditors of their responsibilities, the objectives of the procedures they are to perform, and matters that may affect the nature, timing, and extent of their procedures and by

---

[4] As discussed in paragraph 3.03, the term *deviation* is used throughout this guide when discussing a misstatement, identified by the practitioner, in which the operation of a control was not effective in a specific instance. To distinguish deviations identified by the practitioner from those identified by the internal audit function, the term *exception* is used when referring to misstatements identified by the internal audit function.

(*b*) supervising and reviewing the work performed by internal auditors in a manner similar to the review of work performed by the firm's own staff.

3.113 Paragraph .44 of AT-C section 205 requires the practitioner, before the completion of the engagement, to evaluate whether the use of the work of the internal audit function or the use of internal auditors to provide direct assistance results in the practitioner still being sufficiently involved in the examination, given the practitioner's sole responsibility for the opinion expressed.

Using the Work of a Practitioner's Specialist

3.114 Chapter 2 discusses the practitioner's responsibilities when a practitioner's specialist will be used in the cybersecurity risk management engagement. Those responsibilities include (*a*) evaluating the specialist's competence, capabilities, and objectivity; (*b*) obtaining an understanding of the specialist's field of expertise to enable the practitioner to determine the nature, scope, and objectives of the specialist's work and to evaluate the adequacy of that work; and (*c*) agreeing with the specialist on the terms of the engagement and other matters. In addition to those responsibilities, paragraph .36 of AT-C section 205 requires the practitioner to evaluate the adequacy of the work of the practitioner's specialist for the practitioner's purposes.

3.115 According to paragraph .36 of AT-C section 205, evaluating the adequacy of the work of the practitioner's specialist involves consideration of the following:

a. The relevance and reasonableness of the findings and conclusions of the specialist and their consistency with other evidence

b. If the work of the practitioner's specialist involves the use of significant assumptions and methods,

  i. obtaining an understanding of those assumptions and methods and

  ii. evaluating the relevance and reasonableness of those assumptions and methods in the circumstances, giving consideration to the rationale and support provided by the practitioner's specialist, and in relation to the practitioner's other findings and conclusions

c. If the work of the practitioner's specialist involves the use of source data that are significant to the work of the practitioner's specialist, the relevance, completeness, and accuracy of that source data

3.116 If the practitioner determines that the work of the practitioner's specialist is not adequate, paragraph .37 of AT-C section 205 requires the practitioner to

a. agree with the practitioner's specialist on the nature and extent of further work to be performed by the practitioner's specialist or

b. perform additional procedures considered appropriate in the circumstances.

Evaluating the Results of Procedures

3.117 The practitioner should evaluate the sufficiency and appropriateness of the evidence obtained and consider whether it is necessary to obtain

further evidence to support his or her opinion on the description and the effectiveness of controls for the specified period of time.[5] When making this evaluation, the practitioner should consider all relevant evidence, regardless of whether it appears to corroborate or to contradict the conclusion that the description is presented in accordance with the description criteria and the controls were effective to achieve the entity's cybersecurity objectives based on the control criteria. Paragraphs .A49–.A53 of AT-C section 205 provide application guidance that might be helpful to the practitioner when making this evaluation.

3.118 The practitioner evaluates the results of all procedures performed and conducts both a quantitative (for example, rates of deviations in testing a control using a sample-based testing strategy) and qualitative analysis of whether identified description misstatements and deficiencies in the effectiveness of controls result in the description not being presented in accordance with the description criteria or in the controls not being effective to achieve one or more of the entity's cybersecurity objectives. As an example, assume that, when investigating the follow-up and resolution of two identified security incidents, the practitioner determined that the resolution took longer than the management-prescribed resolution requirement to complete, but that difference was not material (for example, final resolution took two days longer than prescribed). In such an instance, the practitioner may conclude that the deficiencies were not material. However, if the practitioner's testing determined that entity personnel failed to follow up at all for the two instances, he or she might conclude that the controls were not effective in achieving one or more criteria.

3.119 When evaluating the results of procedures, the practitioner investigates the nature and cause of any identified description misstatements and deficiencies or deviations in the effectiveness of controls and determines

- whether the identified description misstatements result in either the failure to meet one or more of the description criteria or in a presentation that could be misunderstood by users if the practitioner's opinion were not modified to reflect the identified description misstatements.
- whether identified deviations are within the expected rate of deviation and are acceptable or whether they constitute a deficiency. If deviations are within the expected rate of deviation, the procedures that have been performed provide an appropriate basis for concluding that the control operated effectively throughout the specified period.
- whether identified deficiencies are likely to have, in the practitioner's judgment, a pervasive effect on the achievement of the entity's cybersecurity objectives (for example, whether more than one criterion would be affected).
- whether

[5] The evaluation of test results may differ when the cybersecurity risk management examination is as of a point in time rather than a period of time. For example, assume the practitioner was engaged to conduct the examination as of December 31, 20X2. While performing the procedures, the practitioner identified, in June 20X1, a deficiency in a control; the deficiency was remediated in November 20X1. In this example, because the practitioner was engaged to conduct the examination as of December 31, 20X2, the deficiency would not cause the practitioner to modify the report because it had already been remediated by December 31, 20X2.

- a previously tested control (or combination of controls) provides sufficient appropriate evidence about whether controls operated effectively or
- whether additional testing of the control or other controls is necessary to determine whether the controls were effective throughout the period to meet the control criterion. (If the practitioner is unable to apply additional procedures to the selected items, the practitioner should consider the reasons for this limitation and concludes on whether those selected items are deviations from the prescribed policy or result in a limitation of the scope of the engagement for the purpose of evaluating the sample. If the practitioner concludes that further evidence is needed, but the practitioner is unable to obtain it, paragraph .47 of AT-C section 205 states that the practitioner should consider the need to modify the opinion.)

- the magnitude of the effect of such deficiencies on the achievement of the entity's cybersecurity objectives based on the control criteria.
- whether users could be misled if the practitioner's opinion were not modified to reflect the identified deficiencies.

3.120 According to paragraph .A105 of AT-C section 205, the term *pervasive* describes "the effects on the subject matter of misstatements or the possible effects on the subject matter of misstatements, if any, that are undetected due to an inability to obtain sufficient appropriate evidence." Based on that guidance, pervasive effects in the cybersecurity risk management examination might be those that are, in the practitioner's professional judgment,

a. not confined to only specific aspects of the conclusion about control effectiveness or,

b. if so confined, represent or could represent a substantial proportion of the conclusion about control effectiveness.

3.121 Factors that may be considered when determining whether the identified deviations may have a pervasive effect on other controls include

- the effect that entity-level controls have on the operation of other controls. Deviations in entity-level controls often have a pervasive effect on other controls.
- the extent of the use of segmentation across the entity's networks and systems. The greater the use of segmentation, the less likely it is that deviations in the operation of controls will have an effect on the operation of other controls.
- the extent to which deficiencies in certain key controls have a pervasive effect on other controls. For example, an entity that does not have effective controls over the detection of security events is unlikely to have an effective cybersecurity risk management program.

3.122 Paragraph .45 of AT-C section 205 also requires the practitioner to accumulate description misstatements or deficiencies identified during the engagement, other than those that are clearly trivial. In addition, the practitioner should accumulate deviations that have not been determined to rise to

the level of a deficiency and consider whether, in the aggregate, they result in a deficiency.

3.123 If the practitioner identifies material description misstatements or material deficiencies in control effectiveness, the practitioner should modify the opinion. When modifying the opinion, the practitioner's understanding of the nature and cause of the description misstatements and deficiencies enables the practitioner to determine how to appropriately modify the opinion. Chapter 4 of this guide discusses modifications of the practitioner's report.

Responding to and Communicating Known or Suspected Fraud, Noncompliance With Laws or Regulations, Uncorrected Misstatements, or Internal Control Deficiencies

Known or Suspected Fraud or Noncompliance With Laws or Regulations

3.124 As discussed in chapter 2, the practitioner has a responsibility to consider known or suspected incidents of fraud and noncompliance with laws or regulations. The practitioner determines the effect of such incidents on management's description of the entity's cybersecurity risk management program, on the effectiveness of controls to achieve the entity's cybersecurity objectives based on the control criteria, and on the practitioner's report. Additionally, the practitioner communicates such information to appropriate parties.

3.125 When incidents of fraud or suspected fraud are identified during the engagement, the practitioner is expected to respond appropriately. For example, unless prohibited by law, regulation, or ethics standards, appropriate responses may include the following:

- Discussing the matter with senior management (and the engaging party, if different) and other appropriate party(ies), unless senior management is suspected to have committed the fraud. If the practitioner suspects fraud involving senior management, the practitioner should communicate these suspicions to those charged with governance and discuss with them the nature, timing, and extent of procedures necessary to complete the examination.
- Requesting that senior management (and the engaging party, if different) consult with an appropriately qualified third party, such as the entity's legal counsel or a regulator
- Considering the implications of the matter in relation to other aspects of the engagement, including the practitioner's risk assessment and the reliability of written representations from management (and the engaging party, if different)
- Obtaining legal advice about the consequences of different courses of action
- Communicating with third parties (such as a regulator)
- Withdrawing from the engagement

3.126 The actions noted in the preceding paragraph may also be appropriate in response to noncompliance or suspected noncompliance with laws or regulations identified during the engagement. In addition, the practitioner may decide to describe the matter in a separate paragraph in the practitioner's report, unless the practitioner

a. is precluded by management (or the engaging party, if different) from obtaining sufficient appropriate evidence to evaluate whether noncompliance that may be material to the conclusion about the effectiveness of controls to achieve the entity's cybersecurity objectives has, or is likely to have, occurred. In this situation, there is a scope limitation which precludes the practitioner from expressing an opinion on the effectiveness of controls to achieve the entity's cybersecurity objectives; accordingly, the practitioner would disclaim an opinion.

b. concludes that the noncompliance results in the entity's failure to achieve the entity's cybersecurity objectives based on the control criteria. In this situation, the practitioner expresses a modified opinion.

Communicating Incidents of Known or Suspected Fraud, Noncompliance With Laws or Regulations, Uncorrected Misstatements, or Internal Control Deficiencies

3.127 In addition to responding to known and suspected fraud and noncompliance with laws or regulations, the practitioner should communicate information regarding those matters, along with information regarding any uncorrected description misstatements or material deficiencies, to the appropriate levels of management (and to the engaging party, if different). The practitioner may also consider whether to communicate other matters.

3.128 If the practitioner identifies or suspects noncompliance with laws or regulations that are not relevant to the subject matters of the cybersecurity risk management examination, the practitioner should determine whether he or she has a responsibility to report the identified or suspected noncompliance to parties other than management (and the engaging party, if different).

3.129 The practitioner may be precluded from reporting such incidents to parties outside the entity because of the practitioner's professional duty to maintain the confidentiality of client information. However, the practitioner's legal responsibilities may vary by jurisdiction and, in certain circumstances, the duty of confidentiality may be overridden by statute, law, or courts of law. A duty to notify parties outside the entity may exist

- in response to a court order or
- in compliance with requirements for examinations of entities that receive financial assistance from a government agency.

3.130 Because potential conflicts with the practitioner's ethical and legal confidentiality obligations may be complex, the practitioner may decide to consult with legal counsel before discussing noncompliance with parties outside the entity.

Obtaining Written Representations From Management

3.131 During the cybersecurity risk management examination, management makes many oral and written representations to the practitioner in response to specific inquiries or through the presentation of the description of the entity's cybersecurity risk management program and management's assertion. Such representations from management are part of the evidence the practitioner obtains. However, they cannot replace other evidence the practitioner could reasonably expect to be available, nor do they provide sufficient appropriate evidence on their own about any of the matters with which they deal. Furthermore, the fact that the practitioner has received reliable written representations does not affect the nature or extent of other evidence that the practitioner obtains.

3.132 Written representations from management ordinarily confirm representations explicitly or implicitly given to the practitioner, indicate and document the continuing appropriateness of such representations, and reduce the possibility of a misunderstanding concerning the matters that are the subject of the representations.

3.133 Paragraph .50 of AT-C section 205 indicates that, in an examination engagement, a practitioner should request written representations in the form of a letter from the responsible party. The representations in the cybersecurity risk management examination should

a. include management's assertion about the subject matters[6] based on the criteria.[7]

b. state that

  i. all relevant matters are reflected in the measurement or evaluation of the subject matters or assertion,

  ii. all known matters contradicting the subject matters or assertion and any communication from regulatory agencies or others affecting the subject matters or assertion have been disclosed to the practitioner, including communications received between the end of the period addressed in the written assertion and the date of the practitioner's report.

c. acknowledge responsibility for

  i. the subject matters and the assertion,

  ii. selecting the criteria, and

  iii. determining that such criteria are appropriate for management's purposes.

d. state that any known events subsequent to the period (or point in time) of the subject matters being reported on that would have a material effect on the subject matters or assertion have been disclosed to the practitioner.

---

[6] Within this section of the guide, the term *subject matters* refers to the two subject matters in the cybersecurity risk management examination: (1) the description of the entity's cybersecurity risk management program and (2) the effectiveness of controls within that program to achieve the entity's cybersecurity objectives based on the control criteria.

[7] Within this section of the guide, the term *criteria* refers to both the description criteria and the control criteria.

e. state that management has provided the practitioner with all relevant information and access.

f. state that management believes the effects of uncorrected misstatements (description misstatements and deficiencies) are immaterial, individually and in the aggregate, to the subject matters.

g. state that management has disclosed to the practitioner

i. all deficiencies in internal control relevant to the cybersecurity risk management examination of which it is aware;

ii. its knowledge of any actual, suspected, or alleged fraud or noncompliance with laws or regulations affecting the subject matters;

iii. identified security incidents that affected the entity's achievement of its cybersecurity objectives; and

iv. other matters the practitioner deems appropriate (for instance, discussion of matters considered material).

3.134 When written representations are directly related to matters that are material to the subject matter, the practitioner should

a. evaluate their reasonableness and consistency with other evidence obtained, including other representations (oral or written) made by management, and

b. consider whether those making the representations can be expected to be well informed on the particular matters.

3.135 The written representations required are separate from, and in addition to, management's written assertions. They are usually made in the form of a representation letter addressed to the practitioner, dated as of the date of the practitioner's report, and they should address the subject matters and periods referred to in the practitioner's opinion.

Requested Written Representations Not Provided or Not Reliable

3.136 Paragraph .55 of AT-C section 205 provides guidance to the practitioner when

- management has not provided one or more of the requested representations;
- the practitioner concludes that there is sufficient doubt about the competence, integrity, ethical values, or diligence of those providing the written representations; or
- the practitioner concludes that the written representations are otherwise not reliable.

3.137 In such circumstances, the guidance in that paragraph states that the practitioner should

- discuss the matter with the appropriate party(ies);
- reevaluate the integrity of those from whom the representations were requested or received and evaluate the effect that this may have on the reliability of representations and evidence in general; and
- if any of the matters are not resolved to the practitioner's satisfaction, take appropriate action.

3.138 Ordinarily, in the cybersecurity risk management examination, management's refusal to furnish evidence in the form of written representations constitutes a limitation on the scope of the examination sufficient to preclude an unmodified opinion on either the description or the effectiveness of controls. Usually, the scope limitation is sufficient to cause the practitioner to disclaim an opinion on both or to withdraw from the engagement.

Subsequent Events and Subsequently Discovered Facts

3.139 Events or transactions may occur after the specified period of time covered by the examination engagement, but prior to the date of the practitioner's report, that could have a significant effect on the description of the entity's cybersecurity risk management program or the effectiveness of controls within that program. In such circumstances, disclosure in the description or in management's assertion may be necessary to prevent users of the cybersecurity risk management examination report from being misled.

3.140 The following are examples of events that could affect the description of the entity's cybersecurity risk management program or management's assertion:

- After the period covered by the examination engagement, management discovered that, during the last quarter of that period, the IT security director provided all the programmers with access to the production data files, enabling them to modify data.
- After the period covered by the examination engagement, management discovered that a confidentiality breach occurred at the entity during the period covered by the practitioner's report.

3.141 Paragraph .48 of AT-C section 205 requires the practitioner to inquire of management (and if different, the engaging party) about whether it is aware of any such events. If such events exist, the practitioner should apply appropriate procedures to obtain evidence regarding the events. For example, the practitioner may obtain evidence by inquiring about and considering information regarding the effectiveness of controls within the entity's cybersecurity risk management program by inspecting

- relevant internal auditors' reports issued during the subsequent period.
- other practitioners' reports issued during the subsequent period.
- relevant regulatory agencies' reports issued during the subsequent period.
- reports on other professional engagements for that entity.

3.142 Paragraph .48 of AT-C section 205 does not require the practitioner to perform any procedures regarding the description of the entity's cybersecurity risk management program, the effectiveness of controls within that program, or management's assertion, after the date of the practitioner's report. However, paragraph .49 of AT-C section 205 clarifies that the practitioner is responsible for responding appropriately to facts that become known after the date of the report that, had they been known as of the report date, may have caused the practitioner to revise the report.

3.143 After obtaining information about an event, the practitioner determines whether the facts existed at the date of the report and, if so, whether persons who would attach importance to these facts are currently using, or

likely to use, the cybersecurity risk management examination report (which includes management's description and assertion and the practitioner's report). The practitioner may do this through discussions with management and other appropriate parties and through the performance of additional procedures that the practitioner considers necessary to determine whether the description, assertion, and practitioner's report need revision or whether the previously issued report continues to be appropriate.

3.144 Specific actions to be taken at that point depend on a number of factors, including the time elapsed since the date of the practitioner's report and whether issuance of a subsequent report is imminent. Depending on the circumstances, the practitioner may determine that notification of persons currently using or likely to use the practitioner's report is necessary. This may be the case, for example, when

- the cybersecurity risk management examination report is not to be relied upon because
  - — the description, management's assertion, or the practitioner's report needs revision or
  - — the practitioner is unable to determine whether revision is necessary and
- issuance of a subsequent practitioner's report is not imminent.

3.145 If the practitioner believes the event is of such a nature and significance that its disclosure is necessary to prevent users of the cybersecurity risk management examination report from being misled, the practitioner should determine whether information about the event is adequately disclosed in the description or management's assertion. For example, assume that, after the period covered by the examination but prior to the date of the practitioner's report, management learns of a security incident involving the loss of customers' personal information. After investigation, management determines that the incident stemmed from an otherwise unknown vulnerability in its system; furthermore, that vulnerability existed during the examination period. In this example, the practitioner ordinarily would conclude that the matter should be disclosed in the description and assertion. If it is not, the practitioner's course of action depends on the practitioner's legal and ethical rights and obligations. Therefore, the practitioner may consider seeking legal advice before deciding on a course of action. Appropriate actions may include

a. disclosing the event (including a description of the nature of the event and its effect on the description, assertion, or report) in the practitioner's report and modifying the related practitioner's opinion, and

b. withdrawing from the engagement.

Subsequent Events Unlikely to Have an Effect on the Practitioner's Opinion

3.146 The practitioner may have determined that the event discovered subsequent to the period covered by the examination engagement would likely have had no effect on either the presentation of the description in accordance with description criteria or the effectiveness of controls because the underlying situation did not exist until after the period covered by the cybersecurity risk management examination report. However, the matter may be sufficiently

important to warrant disclosure by management in its description and, potentially, emphasis by the practitioner in the practitioner's report. The following are examples of such events:

- The entity was acquired by another entity.
- The entity experienced a significant operating disruption.
- A data center-hosting entity that provides applications and technology that enable user entities to perform essential business functions made significant changes to its information systems, including a system conversion or significant outsourcing of operations.

Documentation

3.147 Paragraphs .34–.41 of AT-C section 105 provide requirements regarding the documentation that should be prepared for an attestation engagement. Those paragraphs address matters such as the timeliness of the documentation, how to make necessary changes to the documentation after the original preparation date, retention of engagement documentation, confidentiality of documentation, and the need to document situations in which the practitioner judges it necessary to depart from a relevant presumptively mandatory requirement.

3.148 Additionally, paragraphs .87–.89 of AT-C section 205 discuss the practitioner's responsibilities for preparing and maintaining documentation that is appropriate to an examination engagement. The practitioner's documentation in a cybersecurity risk management examination is the principal record of attestation procedures applied, information obtained, and conclusions or findings reached by the practitioner. The quantity, type, and content of documentation are matters of the practitioner's professional judgment. However, the documentation should be sufficient to determine

a. the nature, timing, and extent of the procedures performed to comply with AT-C sections 105 and 205 and applicable legal and regulatory requirements, including
    i. the identifying characteristics of the specific items or matters tested;
    ii. who performed the engagement work and the date such work was completed;
    iii. the discussions with management or others about findings or issues that, in the practitioner's professional judgment, are significant, including the nature of the significant findings or issues discussed, and when and with whom the discussions took place;
    iv. when management will not provide one or more of the requested written representations or the practitioner concludes that there is sufficient doubt about the competence, integrity, ethical values, or diligence of those providing the written representations or that the written representations are otherwise not reliable, the matters in paragraph .55 of AT-C section 205 (see paragraphs 3.136–.137 of this guide); and

vi. who reviewed the engagement work performed and the date and extent of such review.

b. the results of the procedures performed and the evidence obtained.

3.149 In addition to the items in the preceding paragraphs, documentation in the cybersecurity risk management examination should include the following:

- If the practitioner has identified information that is inconsistent with the practitioner's final conclusions, how the practitioner addressed the inconsistency
- If, after the date of the report, the practitioner becomes aware of facts that may have caused the practitioner to revise the report had they been known at the time of the report,
  - — the circumstances encountered;
  - — any new or additional procedures performed, evidence obtained, and conclusions reached and their effect on the report; and
  - — when and by whom the resulting changes to the documentation were made and reviewed

3.150 As in other attestation engagements, documentation in the cybersecurity risk management examination would ordinarily also include a record of

- issues identified with respect to compliance with relevant ethical requirements and how they were resolved.
- conclusions on compliance with independence requirements that apply to the engagement and any relevant discussions with the firm that support these conclusions.
- conclusions reached regarding the acceptance and continuance of client relationships and attestation engagements.
- the nature and scope of, and conclusions resulting from, consultations undertaken during the course of the engagement.
- if the practitioner uses the work of the internal audit function, other practitioners, or specialists, documentation of conclusions reached by the practitioner regarding the evaluation of the adequacy of the work and the procedures performed on that work.

3.151 Paragraphs .A117–.A119 of AT-C section 205 provide additional application guidance that might be helpful to a practitioner when deciding what to document in the cybersecurity risk management examination.

Management's Responsibilities at or Near Engagement Completion

3.152 Management's responsibilities at or near completion of the cybersecurity risk management examination include

- modifying the description, if appropriate (chapter 4 describes a number of situations in which the practitioner would recommend that management modify the description);

- modifying management's written assertion, if appropriate;
- providing written representations (as discussed beginning in paragraph 3.131);
- informing the practitioner of subsequent events; and
- distributing the report to appropriate parties.

Modifying Management's Assertion

3.153 As discussed in chapter 2, management provides the practitioner with a written assertion about whether the description is presented in accordance with the description criteria and whether the controls within the program were effective to achieve the entity's cybersecurity objectives. Management's written assertion is generally expected to align with the practitioner's opinion by reflecting the same modifications.

3.154 The following is an example of modifications (indicated with bold text) that might be made to management's assertion when the description is not presented in accordance with the description criteria and the practitioner has modified the opinion in his or her report:

> [*Assertion paragraph*]
>
> **Except for the matter described in the following paragraph**, we assert that the description throughout the period [*date*] to [*date*] is presented in accordance with the description criteria. We have performed an evaluation of the effectiveness of the controls within the cybersecurity risk management program throughout the period [*date*] to [*date*] using the [*name of the control criteria, e.g., the criteria for security, availability, and confidentiality set forth in TSP section 100,* 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy *(AICPA,* Trust Services Criteria*) or other suitable criteria*] (control criteria). Based on this evaluation, we assert that the controls were effective to achieve the entity's cybersecurity objectives throughout the period [*date*] to [*date*] based on the control criteria.
>
> **The description of our cybersecurity risk management program states that the entity has physical access controls that incorporate biometric devices and individual PINs. Although such controls have been implemented throughout ABC's main facility, they have not been consistently implemented in our other three facilities.**

3.155 The following is an example of modifications (indicated with bold text) that might be made to management's assertion when controls were not effective to achieve the entity's cybersecurity objectives and the practitioner has modified that component in his or her report:

> [*Assertion paragraph*]
>
> We assert that the description throughout the period [*date*] to [*date*] is presented in accordance with the description criteria. We have performed an evaluation of the effectiveness of the controls within the cybersecurity risk management program throughout the period [*date*] to [*date*] using the [*name of the control criteria, e.g., the criteria for security, availability, and confidentiality set forth in TSP section 100,* 2017 Trust Services Criteria for Security, Availability, Processing

Integrity, Confidentiality, and Privacy *(AICPA,* Trust Services Criteria*) or other suitable criteria*] (control criteria). Based on this evaluation, we assert that, **with the exception of the matter described in the following paragraph**, the controls were effective to achieve the entity's cybersecurity objectives throughout the period [*date*] to [*date*] based on the control criteria.

The description of our cybersecurity risk management program states on page 8 that application changes are tested prior to their implementation. The procedures, however, do not include a requirement for scanning application code for known vulnerabilities prior to placing the change into operation. As a result, the controls were not effective to meet criterion CC8.1, ***The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.***

3.156 If management is unwilling to modify its assertion to align with the practitioner's opinion, the practitioner should consider the implications on the practitioner's report. For example, the practitioner should consider whether report users are likely to misunderstand a cybersecurity risk management examination report that includes management's assertion and the practitioner's report, when management and the practitioner have reached and expressed different conclusions with respect to either the description or the effectiveness of controls in the same document. If the practitioner believes it is likely that such a report will be misunderstood by users, the practitioner may decide to withdraw from the engagement.

Chapter 4

Forming the Opinion and Preparing the Practitioner's Report

This chapter describes the practitioner's responsibilities when forming his or her opinion and preparing the report in the cybersecurity risk management examination. This chapter focuses on the required elements of the practitioner's report and the practitioner's considerations when determining the type of opinion and other modifications to the report that might be necessary.

Responsibilities of the Practitioner

4.01 In the cybersecurity risk management examination, the practitioner is responsible for directly expressing an opinion, in a written report, on the following matters:

a. Whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and

b. Whether the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria

4.02 Because there are two distinct but complementary subject matters, the practitioner expresses an opinion on each in his or her report. Therefore, unless otherwise stated, a reference to the practitioner's report in this chapter includes the practitioner's responsibility to express an opinion on both the (1) description and (2) effectiveness of controls within the cybersecurity risk management program.

4.03 In some circumstances, management may engage the practitioner to perform an examination on the design of the controls rather than on their effectiveness. In that case, the practitioner reports on whether the (1) description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and (2) controls implemented within that program were suitably designed[1] to achieve the entity's cybersecurity objectives. Paragraph 4.14 discusses how the elements of the practitioner's report in paragraph 4.12 would be tailored in that situation.

Forming the Practitioner's Opinion

4.04 When forming his or her opinion, paragraph .59 of AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*), requires the practitioner to evaluate

[1] As used here, the concept of the suitability of design relates to controls that have been *designed and implemented* within the entity's cybersecurity risk management program.

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

a. the practitioner's conclusion about the *sufficiency and appropriateness of evidence* obtained during the cybersecurity risk management examination and

b. whether uncorrected misstatements are material, individually or in the aggregate.

Considering the Sufficiency and Appropriateness of Evidence

4.05 When forming his or her conclusion with respect to the sufficiency and appropriateness of evidence obtained during the examination, the practitioner exercises professional judgment, which is influenced by factors such as the following:

- The significance of a potential description misstatement or deficiency and the likelihood that it will have a material effect, individually or aggregated with other potential description misstatements and deficiencies, on the presentation of the description of the entity's cybersecurity risk management program or on the effectiveness of controls to achieve the entity's cybersecurity objectives based on the control criteria
- The effectiveness of management's responses to address the known risks
- The experience gained during previous consulting or examination engagements with respect to similar potential description misstatements and deficiencies
- The results of procedures performed, including whether such procedures identified specific description misstatements and deficiencies
- The source and reliability of the available information
- The persuasiveness of the evidence
- The practitioner's understanding of the entity and its environment

Considering Material Uncorrected Description Misstatements and Deficiencies

4.06 The cybersecurity risk management examination is a cumulative and iterative process. As the practitioner performs planned procedures, evidence obtained may cause the practitioner to alter the nature, timing, or extent of other planned procedures. For example, information such as the following—which differs significantly from the information on which the risk assessment and planned procedures were based—may come to the practitioner's attention:

- The nature and number of identified description misstatements and deficiencies. (This may change the practitioner's professional judgment about the reliability of particular sources of information.) For example, the practitioner may discover that management was unaware that detection tools were not implemented over a portion of the entity's network. In response, the practitioner may determine that additional testing is needed to evaluate the effectiveness of other controls over that portion of the network.
- Identified discrepancies in relevant information or conflicting or missing evidence.

- Procedures performed toward the end of the engagement that indicate a previously unrecognized risk of material misstatement. As an example, assume that, while testing management's procedures to mitigate security incidents, a practitioner becomes aware of a deficiency in the design of a control that prevents unauthorized access. The practitioner may determine that additional testing is needed to evaluate whether there are other suitably designed controls that operated effectively to mitigate the risk of unauthorized access addressed by the deficient control.

In such circumstances, the practitioner may need to reevaluate the planned procedures.

4.07 The practitioner also evaluates the effect of such uncorrected description misstatements or deficiencies on the engagement and on the opinion. The practitioner may conclude that additional appropriate evidence is required in order to form a conclusion about the description or control effectiveness. In such a case, the practitioner should design and perform additional procedures to obtain sufficient appropriate evidence.

4.08 If the practitioner concludes, based on the evidence obtained, that the description is not presented in accordance with the description criteria or that the controls were not effective to achieve the cybersecurity objectives based on the control criteria, he or she should modify the opinion to express a qualified or adverse opinion. Reporting in a cybersecurity risk management examination when the practitioner decides to modify the opinion is discussed beginning in paragraph 4.16.

Expressing an Opinion on the Subject Matters in the Cybersecurity Risk Management Examination

4.09 As discussed in paragraph 4.01, the practitioner expresses an opinion on two distinct but complementary subject matters in the cybersecurity risk management examination: (1) description of the entity's cybersecurity risk management program and (2) the effectiveness of controls within the program to achieve the entity's cybersecurity objectives. Depending on the circumstances, the practitioner's opinion may be different for each subject matter.

4.10 When the practitioner concludes that an opinion modification on one of the subject matters is appropriate, the practitioner should also consider the effect on the opinion on the other subject matter. Consider the following examples:

- A practitioner expresses a qualified opinion on the effectiveness of the controls because certain controls did not operate consistently throughout the period under examination. The practitioner may conclude that the qualified opinion has no effect on his or her unmodified opinion on whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria. Accordingly, the practitioner would issue an unmodified opinion on the description.
- A practitioner expresses a qualified opinion on the description because management failed to disclose a significant subsequent event. The practitioner may conclude that, because the subsequent event did not affect the effectiveness of controls during the

period covered by the examination, a qualification of the opinion on control effectiveness is not necessary.

- A practitioner disclaims an opinion on the description because of a lack of sufficient appropriate evidence about whether key security policies and processes have been implemented during the specific period of time covered by the examination. In this situation, the lack of evidence also leads the practitioner to disclaim an opinion about the effectiveness of controls associated with such key security policies and processes.

4.11 If the practitioner's report is intended for use by parties within the entity as well as users external to the entity, and the practitioner has decided to express different opinions on each of the subject matters, the practitioner should consider whether it is likely that external users will misunderstand the practitioner's opinion. If the practitioner believes there is a high risk of misunderstanding, he or she may consider adding an alert restricting the use of the report to board members, management, and others within the entity or to those third parties (specified parties) that are likely to understand it.

Preparing the Practitioner's Report

Elements of the Practitioner's Report

4.12 When a practitioner issues an unmodified opinion in the cybersecurity risk management examination, the practitioner's report should include the following elements:

a. A title that includes the word *independent*

b. An appropriate addressee as required by the circumstances of the engagement (The report would ordinarily be addressed to management of the entity or to those charged with governance, such as board members.)

c. Identification of the following:

i. A description of the entity's cybersecurity risk management program and the effectiveness of controls within that program,[2] as well as the specified period of time[3] to which they relate

ii. The criteria used to evaluate the description of the entity's cybersecurity risk management program (description criteria) and the criteria used to evaluate whether controls within that program were effective to achieve the entity's cybersecurity objectives (control criteria)

---

[2] If the subject matter of the engagement is less than entity-wide, the practitioner should modify the language used to identify the subject matter of the engagement.

[3] As discussed in chapter 1, "Introduction and Background," management is responsible for determining whether the engagement will be performed for a specified period of time or as of a point in time to be used in the cybersecurity risk management examination report. However, because most users are likely to find a conclusion about control effectiveness more valuable if it is over a period of time, this guide uses a period of time. If management elects to report as of a point in time, the practitioner would modify the language in the report to refer to the point in time.

d. A statement that an entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that were not prevented

e. A statement that identifies management as the responsible party and indicates management's responsibilities, including matters such as the following:

i. Establishing the entity's cybersecurity objectives, which are presented on page XX of the description

ii. Designing, implementing, and operating the cybersecurity risk management program, including the controls within that program, to achieve the entity's cybersecurity objectives

iii. Preparing the description of the entity's cybersecurity risk management program

iv. Providing an assertion about whether

(1) the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and

(2) the controls within the cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives

v. Selecting, and identifying in its assertion, the description criteria and the control criteria

vi. Having a reasonable basis for its assertion about whether the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives by performing an assessment of the effectiveness of those controls based on the control criteria

f. A statement indicating that the practitioner's responsibility is to express an opinion, based on the examination, about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria

g. A statement indicating that the examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants

h. A statement indicating that those standards require the practitioner to plan and perform the cybersecurity risk management examination to obtain reasonable assurance about whether, in all material respects,

i. the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and

ii. the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria

i. A statement describing the nature of a cybersecurity risk management examination, using language such as the following, indicating that the examination includes

i. obtaining an understanding of the entity's cybersecurity objectives and its cybersecurity risk management program,

ii. assessing the risks that the description is not presented in accordance with the description criteria and that the controls within that program were not effective, and

iii. performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria and whether the controls were effective

j. A statement asserting that the practitioner's examination also included performing such other procedures as considered necessary in the circumstances and that the practitioner believes the evidence obtained is sufficient and appropriate to provide a reasonable basis for the opinion

k. A statement about the inherent limitations of an entity's cybersecurity risk management program, which may include statements such as the following:

i. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

ii. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

iii. Examples of inherent limitations in a cybersecurity risk management program include

(1) vulnerabilities in information technology components as a result of design by their manufacturer or developer,

(2) ineffective controls at a vendor or business partner, and

(3) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

iv. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

l. The practitioner's opinion about whether, in all material respects,

i. the description of the entity's cybersecurity risk management program throughout the period [*date*] to [*date*] is presented in accordance with the description criteria and

ii. the controls within that program were effective throughout the period [*date*] to [*date*] to achieve the entity's cybersecurity objectives based on the control criteria

m. The manual or printed signature of the practitioner's firm

n. The city and state where the practitioner practices

o. The date of the report

4.13 Appendix F-1 presents an illustrative practitioner's report with an unmodified opinion. Headings in that illustrative report are optional.

Tailoring the Practitioner's Report in a Design-Only Examination

4.14 When the practitioner has been engaged to perform a design-only examination, certain of the elements in paragraph 4.12 would be tailored to refer specifically to the matters addressed by the design-only report. For instance, among other things, all references to management's assertion and the practitioner's opinion would be revised to refer to the following:

i. the description throughout the period [*date*] to [*date*] is presented in accordance with the description criteria and

ii. the controls within that program were suitably designed throughout the period [*date*] to [*date*] to achieve the entity's cybersecurity objectives based on the control criteria

4.15 Appendix F-2, *Illustrative Accountant's Report in a Cybersecurity Risk Management Examination that Addresses Only the Suitability of the Design of Controls Implemented Within the Entity's Cybersecurity Risk Management Program (Design-Only Report) as of a Point in Time*, presents an illustrative practitioner's design-only report with an unmodified opinion. Headings in that illustrative report are optional.

Modifications to the Practitioner's Opinion

4.16 Paragraph .68 of AT-C section 205 requires the practitioner to modify the opinion when either of the following circumstances exists and, in the practitioner's professional judgment, the effect of the matter is or may be material:

a. The practitioner is unable to obtain sufficient appropriate evidence to conclude that the subject matter is in accordance with (or based on) the criteria, in all material respects. A limitation on the scope of the engagement ordinarily results in the practitioner either expressing a qualified opinion or disclaiming an opinion, depending on the circumstances that caused it. Scope limitations are discussed beginning in paragraph 4.42 of this guide.

b. The practitioner concludes that, based on the evidence obtained,

i. management's description of the entity's cybersecurity risk management program is not presented in accordance with the description criteria or

ii. the controls within that program were not effective to achieve the entity's cybersecurity objectives based on the control criteria.

4.17 When determining whether to modify the practitioner's opinion, the practitioner should consider the individual and aggregate effect of identified misstatements on the description of the entity's cybersecurity risk management program or the effect of deficiencies on the effectiveness of the controls to achieve the entity's cybersecurity objectives throughout the specified period.

4.18 A security incident may have a significant impact on the achievement of an entity's cybersecurity objectives. For example, if an entity's controls do not provide reasonable assurance that unauthorized access by an outside party to a critical system is detected in a timely manner, the entity's ability to protect information in accordance with its cybersecurity objectives is significantly impaired. As a result, when controls are not effective in meeting one or more control criteria, there is a higher likelihood that the effect of the deficiency would be pervasive, causing the practitioner to express an adverse opinion.

4.19 In certain circumstances, a deficiency in controls may relate to only a limited portion of the entity's information assets. For example, this might be the case if the practitioner identifies a deficiency at one subsidiary that affects the achievement of only one of the entity's cybersecurity objectives, and that subsidiary's information systems are isolated from the entity's other information systems. In such circumstances, the practitioner may conclude that a qualified opinion is appropriate.

4.20 As illustrated in the following table, the practitioner's professional judgment about the nature of the matter giving rise to the modification and the pervasiveness of its effects (or possible effects) on the description and the effectiveness of controls affects the type of opinion to be issued.

Nature of Matter Giving Rise to the Modification	**Practitioner's Professional Judgment About the Pervasiveness of the Effects or Possible Effects on the Description or on the Effectiveness of Controls**	
	Material but Not Pervasive	***Material and Pervasive***
Scope limitation • The practitioner is unable to obtain sufficient appropriate evidence.	Qualified opinion	Disclaimer of opinion
Material misstatements • The description is materially misstated. Or • The controls were not effective to achieve the entity's cybersecurity objectives.	Qualified opinion	Adverse opinion

4.21 If the practitioner believes a modified opinion is appropriate, he or she determines whether to issue a qualified or adverse opinion or whether to disclaim an opinion. When a modified opinion will be issued, paragraph .69 of AT-C section 205 states that the practitioner should include a separate paragraph in the report that provides a description of the matter(s) giving rise to the modification.

Emphasis of Certain Matters

4.22 When the practitioner believes there are certain matters that are particularly relevant for report users to understand the subject matter or the practitioner's report, the practitioner may include additional paragraphs to emphasize those matters in his or her report. For example, a practitioner might decide to highlight a certain matter in the report when

- the description is appropriately presented but specific circumstances of the entity's operating environment are, in the practitioner's professional judgment, of such importance that they are necessary for users' understanding of the entity's cybersecurity risk management program and the effectiveness of controls within that program.
- changes to the entity's controls occurred after the end of the examination period but, in the practitioner's judgment, could affect the usefulness of the information presented in the report to intended users' decision making.

4.23 The following is an example of a paragraph emphasizing a situation in which the entity experienced a significant operating disruption after the examination period but before issuance of the practitioner's report:

> As described on page X of the description, subsequent to the period covered by the cybersecurity risk management examination report, ABC Entity's data center was flooded and rendered inoperable for a period of two weeks by a severe storm that occurred in January, 20XX.

Controls Did Not Operate During the Period Covered by the Report

4.24 In certain circumstances, management's description of the entity's cybersecurity risk management program may include key processes that ordinarily operate during the period covered by the examination but did not operate during that period because the circumstances that warrant the operation of those processes and associated controls did not occur. For example, an identified security event involving the unauthorized access of confidential information by an entity employee would not always trigger the operation of all recovery processes and controls (such as restoring systems and data from clean backups and replacing compromised files), particularly if the event did not result in a data loss. In these circumstances,

- management would continue to include the processes in its description.
- management would modify its assertion to identify which key processes did not operate during the period and indicate that they did not operate because the circumstances that warranted the operation of those processes and associated controls did not occur during the period.

- the practitioner would include in the report a paragraph emphasizing that the key processes and associated controls did not operate, including a statement that no tests of those controls were performed.

4.25 The following is an example of an additional paragraph that might be added to the practitioner's report in this situation:

> ABC Entity's description of its cybersecurity risk management program includes its cybersecurity incident response and recovery plan (CIRP), which discusses the key security policies and processes implemented and operated to respond to and recover from security incidents. To meet control criteria CC7.4, *The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate*, and CC7.5, *The entity identifies, develops, and implements activities to recover from identified security incidents,* ABC Entity's CIRP includes procedures to help understand, contain, monitor, or eradicate a security incident; restore normal business operations in a timely manner with minimal, or no, business interruption or loss of data; and communicate with affected parties. However, during the period [*date*] through [*date*], ABC Entity did not experience a security incident that would warrant the operation of the response and recovery processes and controls within its CIRP. Because those controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls to meet control criteria CC7.4 and CC7.5.

Material Misstatements

4.26 When the practitioner has obtained sufficient appropriate evidence but has identified description misstatements or deficiencies that, individually or in the aggregate, are believed to be material or material and pervasive to the description or control effectiveness, the practitioner should determine whether to issue a qualified opinion or an adverse opinion. Chapter 3, "Performing the Cybersecurity Risk Management Examination," of this guide discusses materiality considerations related to identified description misstatements or deficiencies that, individually or in the aggregate, are believed to be material or material and pervasive to the description or control effectiveness.

Qualified Opinion

4.27 According to paragraph .70 of AT-C section 205, the practitioner should express a qualified opinion when he or she, after having obtained sufficient appropriate evidence, concludes

- the description misstatements, either individually or in the aggregate, are material but not pervasive or
- deficiencies in the design or operation of controls are material but not pervasive.

4.28 In that case, paragraph .69 of AT-C section 205 states that the practitioner should add a separate paragraph to the practitioner's report that provides an explanation of the matter(s) giving rise to the modification.

4.29 In addition, the illustrative practitioner's report in appendix F-1 of this guide would be modified by

- stating in the opinion paragraph that, *except for the effects of the matter(s) giving rise to the modification,* the description is presented in accordance with the description criteria or the controls were effective to achieve the entity's cybersecurity objectives based on the control criteria, in all material respects, and
- amending the practitioner's responsibility paragraph to state that the practitioner believes that the evidence the practitioner has obtained is sufficient and appropriate to provide a basis for the practitioner's *qualified* opinion.

Adverse Opinion

4.30 Paragraph .72 of AT-C section 205 states that the practitioner should issue an adverse opinion when he or she concludes that

- the description misstatements, either individually or in the aggregate, are material and pervasive or
- deficiencies in the design or operation of controls are material and pervasive.

4.31 When the practitioner expresses an adverse opinion, the illustrative practitioner's report in appendix F-1 should be modified by

- including, in a separate paragraph, a clear explanation of the matter(s) giving rise to the modification;
- stating, in the opinion paragraph, that because of the significance of the matter(s) giving rise to the modification, the description is not presented in accordance with the description criteria, or the controls were not effective to achieve the entity's cybersecurity objectives based on the control criteria, in all material respects, or both; and
- amending the practitioner's responsibility paragraph to state that the practitioner believes that the evidence the practitioner has obtained is sufficient and appropriate to provide a basis for the practitioner's *adverse* opinion.

Separate Paragraphs Because of Material Misstatements in the Description

4.32 If the practitioner has identified misstatements in the description that, individually or in the aggregate, are material, and management is unwilling to amend the description, the practitioner should modify the opinion about whether the description was prepared in accordance with the description criteria.

4.33 Beginning in paragraph 4.34, this guide presents examples of separate paragraphs that might be appropriate when misstatements in the description have caused the practitioner to conclude that the opinion on the description should be modified. Ordinarily, the same paragraphs may be used regardless of whether the practitioner intends to express a qualified or adverse opinion on the description.

Description Includes Information That Is Considered Misleading

4.34 The following is an example of a separate paragraph that might be appropriate when the description of the entity's cybersecurity risk management program includes information that is considered misleading to report users:

> On page XX of the accompanying description, ABC Entity states that changes to software other than those classified as minor are subject to vulnerability scanning prior to implementation. However, during the period [*date*] to [*date*] only one out of 15,000 changes were classified as other than minor.

4.35 The following is an example of a separate paragraph that might be appropriate when the description of the entity's cybersecurity risk management program includes subjective information that is not objectively measurable:

> On page XX of the accompanying description, ABC Entity states that its information security function is the industry's best and is staffed by the most talented IT personnel. Because there are no criteria against which these attributes can be measured, these statements are not measurable and cannot be objectively evaluated within the scope of this examination.

Description Omits Relevant Changes to Controls

4.36 The following is an example of a separate paragraph that might be appropriate when the description does not address relevant changes to the entity's cybersecurity controls:

> The accompanying description on page XX states that the information security group monitors and reviews user access on a monthly basis. However, our procedures indicated that this control was first implemented on July 1, 20XX, three months after the beginning of the period addressed by this report.

Description Omits Information Relevant to One or More Description Criteria

4.37 If management refuses to include information about one or more description criteria in its description, the practitioner ordinarily would express either a qualified or an adverse opinion on the description. Management may refuse to disclose such information, for example, if it believes the disclosures may expose the entity's information assets to additional cybersecurity risks. The following paragraph might be appropriate if management refuses to disclose information in accordance with description criterion 6 about identified security incidents during the examination period.

> The accompanying description of ABC Entity's cybersecurity risk management program omits information necessary to meet description criterion 6, *For security incidents that (1) were identified during the 12-month period preceding the period end date of management's description and (2) resulted in a significant impairment of the entity's achievement of its cybersecurity objectives, disclosure of the following: (*a*) nature of the incident; (*b*) timing surrounding the incident; and (*c*) extent (or effect) of those incidents and their disposition.* Disclosure of such information is necessary for the description to be presented in accordance with the description criteria.

Separate Paragraphs Because of Material Deficiencies in the Effectiveness of Controls to Achieve the Entity's Cybersecurity Objectives

4.38 If the practitioner has identified deficiencies in the effectiveness of controls that, individually or in the aggregate, are material, the practitioner should modify the opinion (with either a qualified or adverse opinion) about whether the controls were effective to achieve the entity's cybersecurity objectives.

4.39 Paragraph 4.41 presents an example of a separate paragraph that might be appropriate when deficiencies in the effectiveness of controls have caused the practitioner to conclude that the opinion on control effectiveness should be modified. Ordinarily, the same paragraph may be used regardless of whether the practitioner intends to express a qualified or adverse opinion on control effectiveness.

Deficiencies in the Design of Controls to Achieve the Entity's Cybersecurity Objectives

4.40 The following is an example of a separate paragraph that might be appropriate if the practitioner has identified deficiencies in the suitability of the design of controls that affect the entity's ability to achieve its cybersecurity objectives and, accordingly, affect the opinion on control effectiveness:

> The accompanying description of ABC Entity's cybersecurity risk management program states on page 8 that ABC Entity makes changes to systems only if the changes are authorized, tested, and documented. ABC Entity's procedures, however, do not include a requirement to approve changes before placing the changes into operation. As a result, controls were not suitably designed to meet criterion CC8.1, *The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.*

Deficiencies in the Effectiveness of Controls During a Portion of the Period

4.41 If the practitioner has identified deficiencies in the effectiveness of controls but the factors that led to the deficiencies are corrected by management during the period under examination, the practitioner should modify the opinion and provide an explanation of the matter(s) giving rise to the modification and the period of time for which those matters existed. The following is an example of such a separate paragraph:

> The accompanying description of ABC Entity's cybersecurity risk management program states on page 8 that ABC Entity makes changes to systems only if the changes are authorized, tested, and documented. However, during the period January 1, 20XX, to March 31, 20XX, ABC Entity's procedures did not include a requirement to approve changes before placing the changes into operation. On April 1, 20XX, ABC Entity implemented a procedure requiring that all changes be approved by the director of application development before being placed into operation. As a result, during the period January 1, 20XX, to March 31, 20XX, controls were not suitably designed to meet criterion CC8.1, *The entity authorizes, designs, develops or acquires, configures, documents,*

tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Scope Limitation

4.42 As previously mentioned, a practitioner may express an unmodified opinion only when he or she has conducted the engagement in accordance with the attestation standards. If the practitioner has been unable to apply all the procedures considered necessary in the circumstances, the practitioner would not have complied with the attestation standards.

4.43 According to paragraph .A107 of AT-C section 205, a scope limitation may arise from any of the following:

a. *Circumstances beyond the control of management.* For example, documents that the practitioner considers necessary to inspect were in the custody of a vendor whose services are no longer in use and the documents no longer exist.

b. *Circumstances relating to the nature or timing of the practitioner's work.* For example, a physical process that the practitioner considers necessary to observe may have occurred before the practitioner's engagement or may not be performed regularly during the examination period. (However, an inability to perform a specific procedure does not constitute a scope limitation if the practitioner is able to obtain sufficient appropriate evidence by performing alternative procedures.)

c. *Limitations imposed by management (or the engaging party, if different).* For example, management may have imposed a limitation that prevents the practitioner from performing a procedure that the practitioner considers necessary in the circumstances. Limitations of this kind may have other implications for the engagement, such as for the practitioner's consideration of risks of material misstatement and for engagement acceptance and continuance.

4.44 When there is a scope limitation, the practitioner should determine the pervasiveness of the effects or possible effects on the description of the entity's cybersecurity risk management program and on control effectiveness. According to paragraph .70 of AT-C section 205, the practitioner should express a qualified opinion when the practitioner is unable to obtain sufficient appropriate evidence on which to base the opinion and the practitioner has concluded that the possible effects on the subject matter of undetected description misstatements or deficiencies, if any, could be material but not pervasive to the subject matter. Paragraph .74 of AT-C section 205 indicates that the practitioner should disclaim an opinion when the practitioner is unable to obtain sufficient appropriate evidence on which to base the opinion and the practitioner concludes that the possible effects on the subject matter of undetected description misstatements or deficiencies, if any, could be both material and pervasive.

Qualified Opinion

4.45 When expressing a qualified opinion, the illustrative practitioner's reports in appendix F-1 would be modified by

- including, in a separate paragraph before the opinion paragraph, a clear explanation of the matter(s) giving rise to the modification;

- stating, in the opinion paragraph, that except for the possible effects of the matter(s) giving rise to the modification, the description is presented in accordance with the description criteria and the controls were effective to achieve the entity's cybersecurity objectives based on the control criteria, in all material respects; and
- amending the practitioner's responsibility paragraph to state that the practitioner believes that the evidence the practitioner has obtained is sufficient and appropriate to provide a basis for the practitioner's *qualified* opinion.

4.46 If the practitioner expresses a qualified opinion because of a scope limitation, and also concludes there were material misstatements in the description or material deficiencies in the effectiveness of the controls to achieve the cybersecurity objectives, paragraph .78 of AT-C section 205 requires the practitioner to include, in the practitioner's report, a clear explanation of both the scope limitation and the matter(s) that cause the description or the effectiveness of controls to be materially misstated.

Separate Paragraph When a Scope Limitation Results in a Qualified Opinion

4.47 The following is an example of a separate paragraph that might be appropriate when the practitioner is unable to obtain sufficient appropriate evidence about whether controls were effective to achieve the entity's cybersecurity objectives based on the control criteria and the practitioner has decided to issue a qualified opinion.

> Page XX of the accompanying description of ABC Entity's cybersecurity risk management program states that a service provider researches and classifies events logged by the intrusion detection software for follow-up by ABC Entity personnel. On July 15, 20X0, ABC Entity replaced its existing service provider (original service provider) with a new service provider. However, all records of the research performed by the original service provider were destroyed by that organization upon termination of the service agreement. As a result, we were unable to inspect evidence that independent research was performed on events logged by the intrusion protection systems for the period January 1, 20X0, to July 15, 20X0. As a result, we were unable to determine whether controls were effective during the period January 1 to July 14, 20X0, to achieve the entity's cybersecurity objectives based on criterion CC6.1, *The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.*

Disclaimer of Opinion

4.48 When the practitioner decides to disclaim an opinion, paragraph .77 of AT-C section 205 provides guidance about modifications to the description of the practitioner's responsibility and the description of the examination in the practitioner's report. In addition to adding a separate paragraph to the practitioner's report, the practitioner's report should state that,

a. because of the significance of the matter(s) giving rise to the modification, the practitioner has not been able to obtain sufficient appropriate evidence to provide a basis for an examination opinion, and

b. accordingly, the practitioner does not express an opinion on the subject matter.

Restricting the Use of the Practitioner's Report

Restricting Use When Required by Professional Standards

4.49 In certain circumstances, a practitioner is required to include in his or her report an alert paragraph that restricts the use of the report to certain parties. Such an alert is designed to avoid misunderstandings related to the use of the report, particularly if the report is taken out of the context in which the report is intended to be used.

4.50 In the following circumstances, paragraph .64 of AT-C section 205 states that the practitioner's report should include an alert, in a separate paragraph, that restricts the use of the report:

a. The practitioner determines that the criteria used to evaluate the subject matter are appropriate only for a limited number of parties who either participated in their establishment or can be presumed to have an adequate understanding of the criteria.

b. The criteria used to evaluate the subject matter are available only to specified parties.

4.51 If an alert paragraph is required, paragraph .65 of AT-C section 205 states that the alert should

a. state that the practitioner's report is intended solely for the information and use of the specified parties;

b. identify the specified parties for whom use is intended; and

c. state that the practitioner's report is not intended to be and should not be used by anyone other than the specified parties.

4.52 The practitioner may identify the specified parties in his or her report by naming them, referring to a list of those parties, or identifying the class of parties, for example, "prospective buyers of XYZ Company's pharmaceutical division."

4.53 The following is an example of an alert paragraph that may be added to the practitioner's report to restrict the use of the report to specified parties:

> This report is intended solely for the information and use of [*identify the specified parties*] and is not intended to be and should not be used by anyone other than the specified parties.

Restricting Use in Other Situations

4.54 Although the practitioner is *required* to include an alert paragraph restricting the use of the practitioner's report when the circumstances discussed beginning in paragraph 4.49 exist, paragraph .A94 of AT-C section 205 clarifies that the practitioner is never precluded from restricting the use of his or her report. As discussed throughout this guide, there are circumstances in which the practitioner may choose to restrict the use of the report, even though standards do not require it. In some circumstances, the practitioner may determine that certain types of individuals are likely to misunderstand the report and may experience adverse consequences from their decisions that result from

the use of the information contained in the cybersecurity risk management examination report. As a result, the practitioner may decide to restrict the use of the report to persons who are unlikely to misunderstand it. Consider the following examples:

- When only a portion of an entity's cybersecurity risk management program is the subject matter of the engagement, the practitioner may become aware of information that causes him or her to believe management has limited the subject matter because of its belief that an examination of the entire entity's cybersecurity risk management program would result in a modified opinion. In that situation, the practitioner should consider whether
  - — an opinion on only a portion of an entity's cybersecurity risk management program is likely to meet the information needs of report users and
  - — the resulting cybersecurity risk management examination report is subject to the risk of misunderstanding by all but a limited number of report users.
- The practitioner's concerns may lead him or her to decide to restrict the use of the practitioner's report to those limited users.
- If the practitioner expects to express a different opinion on the description than on the effectiveness of controls, the practitioner may consider whether report users are likely to misunderstand the two opinions and why they are different. If the practitioner believes the risk of misunderstanding is high, the practitioner may conclude that it is appropriate to restrict the use of the practitioner's report to board members, management, and others within the entity.
- In an initial cybersecurity risk management examination, the practitioner may conclude that potential report users external to the entity, if any, may misunderstand the nature of the engagement, the practitioner's procedures, the inherent limitations of the engagement, or other elements of the engagement. These concerns may lead the practitioner to conclude that an alert to restrict the use of the report to board members, management, and others within the entity is appropriate.

4.55 If the practitioner decides to restrict the use of the report to specified parties, he or she should add a paragraph as described beginning in paragraph 4.51 of this guide.

Distribution of the Report

4.56 When engaged by management, the practitioner provides the report to management and those charged with governance; management distributes the report to intended users.

4.57 In most cases, the practitioner is engaged by management to perform the cybersecurity risk management examination. However, in some cases, the practitioner may be engaged by others. A practitioner ordinarily distributes his or her report only to the party that engaged the practitioner.

4.58 Paragraph .A100 of AT-C section 205 indicates that a practitioner may consider informing the responsible party and, if different, the engaging party or other specified parties that the report is not intended for distribution to parties other than those specified in the report. The practitioner may, in connection with establishing the terms of the engagement, reach an understanding with the responsible party or, if different, the engaging party that the intended use of the report will be restricted and may obtain the responsible party's agreement that the responsible party and specified parties will not distribute the report to parties other than those identified therein. A practitioner is not responsible for controlling, and cannot control, distribution of the report after its release.

Reporting When Using the Work of an Other Practitioner

4.59 If the practitioner assumes responsibility for the work of an other practitioner, the practitioner should not refer to the other practitioner in his or her report.

Reporting When a Specialist is Used for the Cybersecurity Risk Management Examination

4.60 As discussed in chapter 2, "Accepting and Planning a Cybersecurity Risk Management Examination," the practitioner has sole responsibility for the opinion expressed in the cybersecurity risk management examination; that responsibility is not reduced by the use of the work of a specialist. For this reason, as discussed in paragraph .67 of AT-C section 205, the practitioner should not refer to the work of a practitioner's specialist when the practitioner is expressing an unmodified opinion in the cybersecurity risk management examination. However, when the practitioner is expressing a modified opinion, paragraph .81 of AT-C section 205 permits the practitioner to make reference to the work of the specialist, when such reference is relevant to users' understanding of the modification to the practitioner's opinion. If the practitioner decides to make reference to the specialist in the report, the practitioner should indicate that such reference does not reduce the practitioner's responsibility for that opinion.

Report Date

4.61 The practitioner dates his or her report no earlier than the date on which the practitioner has obtained sufficient appropriate evidence to support his or her opinion. According to paragraph .63 of AT-C section 205, that includes evidence that

- the examination documentation has been reviewed;
- the description of the entity's cybersecurity risk management program and management's assertion have been prepared; and
- management has provided a written assertion.

Other Information

4.62 When the practitioner is willing to permit the cybersecurity risk management examination report to be included in a document that contains other information or permit other information to be attached to the cybersecurity

risk management examination report, that other information is not covered by the practitioner's report. Paragraph .57 of AT-C section 205 requires the practitioner to read the other information to identify material inconsistencies between the other information and the description of the entity's cybersecurity risk management program, management's assertion, or the practitioner's report or material misstatements of facts between the other information and information in the cybersecurity risk management examination report. If the practitioner identifies a material inconsistency or becomes aware of a material misstatement of fact in the other information, the description of the entity's cybersecurity risk management program or the effectiveness of controls within that program, management's assertion, or the practitioner's report, the practitioner should discuss the matter with management of the entity.

4.63 If management refuses to correct or delete the other information containing a material inconsistency or a material misstatement of fact, paragraph .A67 of AT-C section 205 identifies the following examples of further actions the practitioner may take:

- Requesting the appropriate party or parties consult with a qualified third party, such as the appropriate party's legal counsel
- Obtaining legal advice about the consequences of different courses of action
- If required or permissible, communicating with third parties (for example, a regulator)
- Describing the material inconsistency in the practitioner's report
- Withdrawing from the engagement, when withdrawal is possible under applicable laws and regulations

4.64 If other information accompanies the description, or if the description of the entity's cybersecurity risk management program and the practitioner's report is included in a document containing other information, the other information should be differentiated from the information covered by the practitioner's report.

4.65 Because of the nature of the other information or its presentation, the practitioner may decide to add a separate other-matter paragraph to the practitioner's report, indicating that the other information is not covered by that report.

Appendix A

Information for Entity Management

The purpose of this appendix is to assist management with understanding the cybersecurity risk management examination that can be performed by a CPA (practitioner) in connection with certain entity-prepared cybersecurity information. It is also intended to help management understand and discharge its responsibilities in connection with that engagement. This appendix is nonauthoritative and is included for informational purposes only.

Introduction

In response to requests for information about the effectiveness of an entity's cybersecurity risk management program, the AICPA has developed the *cybersecurity risk management examination.* In conjunction with that examination, the AICPA has also developed description criteria for use when preparing and evaluating the description of the entity's cybersecurity risk management program and control criteria for use when evaluating the effectiveness of controls within the entity's cybersecurity risk management program.

Overview of the AICPA Cybersecurity Risk Management Examination

A CPA (referred to as a *practitioner* in an attestation engagement) performs and reports in the cybersecurity risk management examination in accordance with the Statements on Standards for Attestation Engagements, commonly known as the attestation standards. Under those standards, an attestation engagement is predicated on the concept that a party other than the practitioner (that is, the responsible party) makes an assertion about whether the subject matter is measured or evaluated in accordance with suitable criteria. In the cybersecurity risk management examination, management is ordinarily the responsible party. As the responsible party, management prepares the description and makes an assertion about the subject matters. Specifically, management's assertion addresses whether the description was prepared in accordance with the description criteria and whether the controls within the program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

The practitioner designs and performs procedures to obtain sufficient appropriate evidence about whether the description is presented in accordance with the description criteria and whether the controls were effective to achieve the entity's cybersecurity objectives based on the control criteria.[1] The practitioner reports on that information in accordance with the attestation standards.

---

[1] In certain circumstances, the practitioner may be engaged to report on the description and on the suitability of the design of the controls within the entity's cybersecurity risk management program. Such an examination, which is referred to as a design-only examination, is discussed further

(continued)

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

In the cybersecurity risk management examination, there are two distinct but complementary subject matters: (1) the description of the entity's cybersecurity risk management program and (2) the effectiveness of controls within that program to achieve the entity's cybersecurity objectives. The cybersecurity risk management examination results in the issuance of a *cybersecurity risk management examination report*, which includes three key sets of information that, taken together, are intended to provide stakeholders with information about the entity's cybersecurity risk management efforts. The three key sets of information are the following:

- *Management's description of the entity's cybersecurity risk management program*. The first component is a management-prepared narrative description of the entity's cybersecurity risk management program. This description is designed to provide information about how the entity identifies its information assets,[2] the ways in which the entity manages the cybersecurity risks that threaten it, and the key security policies and processes implemented and operated to protect the entity's information assets against those risks. *The description, which is prepared in accordance with a specified set of suitable description criteria, provides the context needed for intended users to understand the entity's cybersecurity risk management program*.
- *Management's assertion*. The second component is an assertion provided by management about whether
  - — the description was presented in accordance with the description criteria and
  - — the controls implemented as part of the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on a specified set of suitable control criteria.
- *CPA's opinion*. The third component is a CPA's opinion about whether
  - — the description was presented in accordance with the description criteria and
  - — the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

According to the attestation standards, *criteria* are "the benchmarks used to measure or evaluate the subject matter." Among other things, management is responsible for selecting the criteria to be used in the cybersecurity risk management examination. To enable the preparation and evaluation of the

---

(footnote continued)

in the section titled "Cybersecurity Risk Management Examination Addresses Only the Suitability of the Design of Controls Within the Entity's Cybersecurity Risk Management Program (Design-Only Examination)."

[2] The term *information assets* refers to data and associated software and infrastructure used to process, transmit, and store information. Examples of information assets include employees' personally identifiable information, protected health information, customers' credit card information, and the systems that process, transmit, and store such information.

cybersecurity information in the examination, two distinct yet complementary sets of criteria are used:

- *Description criteria* are used to prepare and evaluate the description of the entity's cybersecurity risk management program.
- *Control criteria* are used to evaluate the effectiveness of controls to achieve the entity's cybersecurity objectives.

Management is responsible for selecting the criteria to be used and may select any criteria they want, as long as the criteria are suitable and available, in accordance with the attestation standards. Suitability of the criteria is discussed further in the section titled "Selecting the Description Criteria and the Control Criteria to Be Used in the Cybersecurity Risk Management Examination."

Description of the Entity's Cybersecurity Risk Management Program

The description of the entity's cybersecurity risk management program is designed to provide report users with information about the environment in which the entity operates and the process used to develop its cybersecurity objectives, identify its information assets and the threats against them, and design, implement, and operate controls to mitigate the risks of such threats. The description is also intended to provide report users with information about the processes within the cybersecurity risk management program that have been designed and implemented to respond to those risks. As such, the description is intended to enable users to understand the cybersecurity risk management program and the conclusions expressed by management in its assertion and by the practitioner in his or her report. It does not, however, provide a detailed narrative of the entity's controls nor a listing of tests of controls performed by the practitioner and the results thereof.

In the cybersecurity risk management examination, an *entity's cybersecurity risk management program* is defined as

> the set of policies, processes, and controls designed to protect *information and systems* from *security events* that could *compromise* the achievement of the entity's *cybersecurity objectives* and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented.

Italicized terms are defined as follows:

- *Information and systems* refers to information in electronic form during its use, processing, transmission, and storage and the systems that use such information to process, transmit or transfer, and store information. A *system* refers to infrastructure, software, people, processes, and data that are designed, implemented, and operated to work together to achieve one or more specific business objectives (for example, delivery of services or production of goods) in accordance with management-specified requirements. As used in this document, systems include manual, automated, and partially automated systems that are used for information processing, manufacturing and production, inventory management and distribution, information storage, and support functions within an

organization. Systems that have cybersecurity risks include, for example,

  - — manufacturing and production systems that are automated or partially automated (including the industrial control systems components);
  - — inventory management or distribution systems; and
  - — treasury and funds management and other types of back office systems.

- A *security event* is an occurrence, arising from actual or attempted unauthorized access or use by internal or external parties, that impairs or could impair the availability, integrity, or confidentiality of information or systems, result in unauthorized disclosure or theft of information or other assets, or cause damage to systems. A security incident is a security event that requires action on the part of an entity in order to protect information assets and resources.
- A *compromise* refers to a loss of confidentiality, integrity, or availability of information, including any resultant impairment of
  - — processing integrity or availability of systems or
  - — the integrity or availability of system inputs or outputs.
- An entity's *cybersecurity objectives* are those objectives that address cybersecurity risks that could affect the achievement of the entity's overall business objectives (including compliance, reporting, and operational objectives). Understanding the entity's cybersecurity objectives is integral to the assessment and evaluation of whether controls are effective. Cybersecurity objectives are discussed in more detail in the section titled "Establishing the Entity's Cybersecurity Objectives."

The definition of the entity's cybersecurity risk management program acknowledges a fundamental tenet of cybersecurity: *an entity that operates in cyberspace is likely to experience one or more security events or breaches at some point in time, regardless of the effectiveness of the entity's cybersecurity controls*. Understanding this tenet is essential to dispelling user misconceptions that an effective cybersecurity risk management program will prevent all security events from occurring. In fact, because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that security events are prevented and, for those not prevented, that they are detected, responded to, mitigated against, and recovered from on a timely basis. In other words, an effective cybersecurity risk management program is one that enables the entity to detect security events on a timely basis and to respond to and recover from such events with minimal disruption to the entity's operations.

Establishing the Entity's Cybersecurity Objectives

According to the Committee of Sponsoring Organizations of the Treadway Commission (COSO), in their 2013 *Internal Control—Integrated Framework* (COSO framework), internal control is a process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable

assurance regarding the achievement of the entity's business objectives.[3] Because of this relationship between internal control and objectives, the COSO framework states that management specifies suitable objectives so that the risks that threaten the achievement of the entity's overall business objectives can be identified, assessed, and managed.

According to the COSO framework, there are three categories of objectives:

- *Operations objectives*. These pertain to the effectiveness and efficiency of the entity's operations, including operational and financial performance goals and safeguarding assets against loss.
- *Reporting objectives*. These pertain to internal and external financial and nonfinancial reporting and may encompass reliability, timeliness, transparency, or other terms as set forth by regulators, recognized standard setters, or the entity's policies.
- *Compliance objectives*. These pertain to adherence to laws and regulations to which the entity is subject.

Cybersecurity risks are one of the types of risks that threaten the achievement of an entity's overall business objectives. Consequently, entities often establish cybersecurity objectives that address their specific cybersecurity risks. Generally, the nature of an entity's cybersecurity objectives varies depending on the environment in which the entity operates, the entity's mission and vision, the overall business objectives established by management, risk appetite, and other factors. For example, a telecommunications entity may have a cybersecurity objective related to the reliable functioning of those aspects of its operations that are deemed to be critical infrastructure, whereas an entity that promotes online dating is likely to regard the confidentiality of personal information collected from its customers as a critical factor toward the achievement of its operating objectives.

Management is responsible for establishing, and including in the description, the entity's cybersecurity objectives with sufficient clarity to enable users to understand what the entity is striving to achieve from a cybersecurity perspective and how the controls within the entity's cybersecurity risk management program were designed, implemented, and operated effectively to provide reasonable assurance of achieving those objectives. Because of the importance of the cybersecurity objectives to the cybersecurity risk management examination, the cybersecurity objectives established by management should be suitable for the engagement.

According to the COSO framework, suitable objectives are

- *specific*. The objectives provide a clear understanding of the cybersecurity risks that need to be mitigated.
- *measurable or observable*. The objectives permit an objective determination about whether each cybersecurity objective has been met.
- *attainable*. The objectives permit the implementation of controls that, if suitably designed and operated effectively, provide reasonable assurance of achieving each objective.

---

[3] ©2013, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used by permission. See www.coso.org.

- *relevant*. The achievement of each cybersecurity objective supports the entity's efforts to achieve its overall objectives.
- *time-bound*. The objectives reflect the desired operation of cybersecurity controls over time.

As discussed previously, cybersecurity objectives are established to address the cybersecurity risks that would threaten the achievement of the entity's overall objectives. Consequently, in establishing the entity's cybersecurity objectives, management also considers whether the cybersecurity objectives completely address those risks. Because the achievement of the entity's overall objectives depends on the achievement of the cybersecurity objectives, the cybersecurity objectives also need to meet one additional attribute: completeness. To be complete, the set of cybersecurity objectives established by management needs to address the significant cybersecurity risks that threaten the achievement of the entity's overall business objectives.

Management is likely to establish cybersecurity objectives that address several basic matters, regardless of the nature of the business and the industry in which the entity operates. Basic matters that management may consider when establishing the entity's cybersecurity objectives include the following:

- Commitments made to third parties (customers, vendors, business partners, and others) related to the security and availability of information and systems, including commitments related to critical infrastructure and extended supply chains
- Laws and regulations to which the entity is subject as a result of the types of information it possesses or uses (for instance, protected health information and personally identifiable information)
- Commitments made as part of a certification and authorization process for government agencies and other parties
- Industry standards to which the entity is subject as a result of the types of information it uses (for instance, Payment Card Industry Data Security Standards for entities that accept or process credit card transactions)
- Other business initiatives

To assist management with the development and disclosure of the entity's cybersecurity objectives, description criterion 3 (*The entity's principal cybersecurity risk management program objectives [cybersecurity objectives] related to availability, confidentiality, integrity of data, and integrity of processing*), presented in *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program*, includes as implementation guidance the following example of cybersecurity objectives an entity might establish:

Availability

Enabling timely, reliable, and continuous access to and use of information and systems to do the following:

- Comply with applicable laws and regulations
- Meet contractual obligations and other commitments
- Provide goods and services to customers without disruption

- Safeguard entity assets and assets held in custody for others
- Facilitate decision making in a timely manner

Confidentiality

Protecting information from unauthorized access and disclosure, including means for protecting proprietary information and personal information subject to privacy requirements, to do the following:

- Comply with applicable laws and regulations
- Meet contractual obligations and other commitments
- Safeguard the informational assets of an entity

Integrity of Data

Guarding against improper information modification or destruction of information to support the following:

- The preparation of reliable financial information for external reporting purposes
- The preparation of reliable information for internal use
- Information nonrepudiation and authenticity
- The completeness, accuracy, and timeliness of processing
- Management holding employees and users accountable for their actions
- The operation of processes addressing the privacy of personal information

Integrity of Processing

Guarding against improper use, modification, or destruction of systems to support the following:

- The accuracy, completeness, and reliability of information, goods, and services produced
- The safeguarding of entity assets
- The safeguarding of life and health

In the cybersecurity risk management examination, management would tailor those cybersecurity objectives to reflect the entity's business objectives based on the nature of the business and the industry in which it operates, the entity's mission and vision, and the entity's cybersecurity risk appetite.

Because of the close relationship among the entity's cybersecurity objectives, the practitioner's opinion on the effectiveness of controls, and report users' understanding of the practitioner's opinion, the practitioner also considers whether the cybersecurity objectives are suitable and complete. If the practitioner believes that the cybersecurity objectives established by management are not suitable and complete, the practitioner should discuss the matter with management. If management is unwilling to revise the cybersecurity objectives to address the practitioner's concerns, the practitioner may decide (*a*) to refuse to accept the engagement or (*b*) to restrict the use of the report to those users who are able to understand the risks not addressed by the entity's cybersecurity objectives.

Effectiveness of Controls Within the Entity's Cybersecurity Risk Management Program

In addition to providing a description of the entity's cybersecurity risk management program, the cybersecurity risk management examination report also provides information about whether the controls the entity has designed, implemented, and operated to mitigate cybersecurity risks were effective throughout the period of time covered by the engagement. For that reason, one of the subject matters of the cybersecurity risk management examination is the *effectiveness of controls within an entity's cybersecurity risk management program* to achieve the entity's cybersecurity objectives.

Management's assertion and the practitioner's opinion on the effectiveness of controls encompass both the suitability of the design of controls and their operating effectiveness:

- *Controls were suitably designed*. Suitably designed controls, if complied with satisfactorily, provide reasonable assurance of achieving the entity's cybersecurity objectives based on the control criteria. Suitably designed controls operate as designed by persons who have the necessary authority and competence to perform the controls.
- *Controls operated effectively*. Suitably designed controls operate effectively if they provide reasonable assurance of achieving the entity's cybersecurity objectives based on the control criteria.

Management's Responsibilities During the Planning of a Cybersecurity Examination

Management needs to understand its responsibilities in the cybersecurity engagement. Management's responsibilities include the following:

- Identifying the types of information created, used, and stored by the entity and the systems used that are subject to cybersecurity risks
- Identifying the entity's cybersecurity objectives
- Identifying and analyzing the risks that could prevent the entity from achieving its cybersecurity objectives based on the entity's business objectives, including the cyber risks arising from interactions with third parties with access to one or more of the entity's information systems
- Designing, implementing, operating, monitoring, and documenting controls that are effective to achieve the entity's cybersecurity objectives
- Defining the scope of the engagement, including whether the examination will cover the entity's cybersecurity risk management program or only a portion of that program, and the time frame of the examination
- Selecting the description criteria against which the presentation of the description will be evaluated and the control criteria against which the effectiveness of controls within the cybersecurity risk

management program will be evaluated and stating both in management's assertion

- Preparing the description of the entity's cybersecurity risk management program in accordance with the description criteria
- Preparing a written assertion, to accompany the description, about whether
  - — the description is presented in accordance with the description criteria and
  - — the controls were effective to achieve the entity's cybersecurity control objectives based on the control criteria
- Having a reasonable basis for its assertion
- Agreeing to provide the practitioner with the following:
  - — Access to all information, such as records and documentation, including service-level agreements, of which management is aware, that is relevant to the description of the entity's cybersecurity risk management program and the assertion
  - — Access to additional information that the practitioner may request from management for the purpose of the cybersecurity risk management examination
  - — Unrestricted access to persons within the entity from whom the practitioner determines it is necessary to obtain evidence relevant to the cybersecurity risk management examination
  - — If internal auditors will provide direct assistance to the practitioner, written acknowledgment that those internal auditors will be allowed to follow the practitioner's instructions without management intervention
  - — Written representations at the conclusion of the engagement, which will include the following:
    - All known matters that might contradict the presentation of the description in accordance with the description criteria or the effectiveness of controls to achieve the cybersecurity objectives
    - Any communication from regulatory agencies or others related to the presentation of the description or the effectiveness of controls relevant to the cybersecurity risk management program
    - All deficiencies in internal control relevant to the engagement, of which management is aware
    - Any known actual, suspected, or alleged fraud or noncompliance with laws or regulations affecting the description or the effectiveness of controls
    - Any known events subsequent to the period covered by the engagement up to the date of the practitioner's report that would have a material

effect on the description or the effectiveness of controls

- Other matters the practitioner deems appropriate (for example, discussion of matters considered material)

Management acknowledges these responsibilities in an engagement letter or other suitable form of written communication.

Defining the Scope and Time Frame of the Engagement

Management is responsible for determining the subject matter of the cybersecurity risk management examination. In some situations, management may engage the practitioner to report on only a portion of the entity's cybersecurity risk management program; in other circumstances, management may engage the practitioner to report on only the suitability of design of the controls within that program. When considering the subject matter of the examination, management needs to obtain an understanding of the needs of intended users to determine whether the subject matter of the examination is likely to meet their needs.

In addition to the specific subject matter to be covered by the engagement, management is responsible for determining whether the description and assertion are to be presented as of a specified *point in time* or for a *period of time* and the time frame they would address.

Cybersecurity Risk Management Examination Addresses Only a Portion of the Entity's Cybersecurity Risk Management Program

Although the cybersecurity risk management examination usually addresses an entity-wide cybersecurity risk management program, there may be circumstances in which management may engage the practitioner to examine and report on only a portion of that program. The cybersecurity risk management examination may be limited to any of the following:

- One or more specific business units, segments, or functions of an entity
  - — when those units, segments, or functions operate under an *entity-wide* cybersecurity risk management program or
  - — when those units, segments, or functions operate under an *independent* cybersecurity risk management program
- One or more specific types of information used by the entity

In those situations, the description is tailored to disclose only information about the portion of the cybersecurity risk management program (that is, the particular business unit, segment, or type of information) within the scope of the engagement. Likewise, when evaluating whether the description is presented in accordance with the description criteria, consideration would be given to whether the description addresses all relevant aspects of the portion of the cybersecurity risk management program within the scope of the engagement. For example, if the engagement addresses only one specific business unit, and that unit's cybersecurity risk management program relies on aspects of the

entity-wide program, the description would also include disclosure of those aspects of the entity-wide program relevant to that business unit.

Cybersecurity Risk Management Examination Addresses Only the Suitability of the Design of Controls Within the Entity's Cybersecurity Risk Management Program (Design-Only Examination)

In some circumstances, management may not be prepared to make an assertion about whether the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives. In such situations, rather than making an assertion about whether controls were effective to achieve the entity's cybersecurity objectives, management may make an assertion about the suitability of the design of controls within the program.

Such an examination, referred to as a *design-only cybersecurity risk management examination* (design-only examination), would include the following two subject matters: (1) the description of the entity's cybersecurity risk management program and (2) the suitably of design of the controls implemented within that program to achieve the entity's cybersecurity objectives. Accordingly, a design-only examination would not provide report users with sufficient information to assess the effectiveness of controls within that program. However, the resulting report (design-only report) may be useful to report users who want to obtain an understanding of the entity's cybersecurity risk management program and an overview of the security policies and processes implemented within that program.

If the practitioner is concerned that intended users are likely to misunderstand the practitioner's opinion on the description and design only, the practitioner may restrict the use of a design-only report to board members, management, others within the organization, and specific third parties (specified parties) who are likely to understand it.

Selecting the Description Criteria and the Control Criteria to Be Used in the Cybersecurity Risk Management Examination

As previously discussed, two distinct sets of criteria are used in the cybersecurity risk management examination: description criteria and control criteria. Management is responsible for selecting both sets of criteria to be used.

Management may select any description and control criteria, as long as they are suitable and available to intended users. According to the attestation standards, criteria are suitable when they exhibit all of the following characteristics:

- *Relevance*. Criteria are relevant to the subject matter.
- *Objectivity*. Criteria are free from bias.
- *Measurability*. Criteria permit reasonably consistent measurements, qualitative or quantitative, of subject matter.
- *Completeness*. Criteria are complete when subject matters prepared in accordance with them do not omit relevant factors that could reasonably be expected to affect decisions of the report users made on the basis of that subject matter.

The relative importance of each characteristic to a particular engagement is a matter of professional judgment.

Criteria also need to be available to report users to allow them to understand how the entity has prepared its description and evaluated the effectiveness of controls in achieving the entity's cybersecurity objectives. Criteria that are publicly available, included in the description, or included in the practitioner's report are all considered available to report users. Sometimes, criteria are available only to certain report users; in this case, the practitioner is required by the attestation standards to include an alert restricting the use of the report to those parties.

Description Criteria

The description criteria in *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* may be used by management when preparing and evaluating the description of the entity's cybersecurity risk management program and by the practitioner when evaluating that description. The description criteria included in *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* are categorized into the following sections:

a. *Nature of Business and Operations*. Disclosures about the nature of the entity's business and operations

b. *Nature of Information at Risk*. Disclosures about the principal types of sensitive information the entity creates, collects, transmits, uses, and stores that is susceptible to cybersecurity risk

c. *Cybersecurity Risk Management Program Objectives* (*Cybersecurity Objectives*). Disclosures about the entity's principal cybersecurity objectives related to availability, confidentiality, integrity of data, and integrity of processing and the process for establishing, maintaining, and approving them

d. *Factors that Have a Significant Effect on Inherent Cybersecurity Risks*. Disclosures about factors that have a significant effect on the entity's inherent cybersecurity risks, including the

  i. characteristics of technologies, connection types, service providers, and delivery channels used by the entity;

  ii. organizational and user characteristics; and

  iii. environmental, technological, organizational, and other changes during the period covered by the description at the entity and in its environment.

e. *Cybersecurity Risk Governance Structure*. Disclosures about the entity's cybersecurity risk governance structure, including the processes for establishing, maintaining, and communicating integrity and ethical values, providing board oversight, establishing accountability, and hiring and developing qualified personnel

f. *Cybersecurity Risk Assessment Process*. Disclosures related the entity's process for

  i. identifying cybersecurity risks and environmental, technological, organizational, and other changes that could have a significant effect on the entity's cybersecurity risk management program;

ii. assessing the related risks to the achievement of the entity's cybersecurity objectives; and

iii. identifying, assessing, and managing the risks associated with vendors and business partners

g. *Cybersecurity Communications and the Quality of Cybersecurity Information*. Disclosures about the entity's process for communicating cybersecurity objectives, expectations, responsibilities, and related matters to both internal and external users, including the thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both

h. *Monitoring of the Cybersecurity Risk Management Program*. Disclosures related to the process the entity uses to assess the effectiveness of controls included in its cybersecurity risk management program, including information about the corrective actions taken when security events, threats, vulnerabilities, and control deficiencies are identified

i. *Cybersecurity Control Processes*. Disclosures about

i. the entity's process for developing a response to assessed risks, including the design and implementation of control processes;

ii. the entity's IT infrastructure and its network architectural characteristics; and

iii. the key security policies and processes implemented and operated to address the entity's cybersecurity risks

Applying the description criteria in actual situations requires judgment. Therefore, in addition to the description criteria, each criterion also presents implementation guidance. The implementation guidance presents factors to consider when making judgments about the nature and extent of disclosures called for by each criterion. The implementation guidance does not address all possible situations; therefore, users should carefully consider the facts and circumstances of the entity and its environment in actual situations when applying the description criteria.

The description criteria in *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* were promulgated by the Assurance Services Executive Committee (ASEC), which is designated by the Council of the AICPA under the AICPA Code of Professional Conduct to issue measurement criteria. Therefore, such criteria are considered suitable for use in the cybersecurity risk management examination. Because the description criteria also are published by the AICPA and made available to the general public, they are considered available to report users. Therefore, the description criteria are both suitable and available criteria for use in the cybersecurity risk management examination.

As cybersecurity services continue to evolve, other description criteria may be developed. If management believes that other description criteria are suitable (that is, that other criteria exhibit the characteristics of suitable criteria previously discussed), management could select and use such criteria when developing and assessing the presentation of the description in the cybersecurity risk management examination.

Control Criteria

When selecting the control criteria to be used in the evaluation of the effectiveness of controls within the entity's cybersecurity risk management program, management may select any criteria, as long as the criteria are both suitable and available to users. Management may select the criteria for the security, availability, and confidentiality categories in the *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* as the control criteria.

Applying the trust services criteria in actual situations requires judgment. Therefore, each criterion also contains points of focus. The COSO framework states that points of focus represent important characteristics of the criteria. Consistent with the COSO framework, the points of focus may assist management when designing, implementing, and operating controls over security, availability, and confidentiality. In addition, the points of focus may assist both management and the practitioner when evaluating whether the controls were suitably designed and operated to meet the entity's cybersecurity risk management objectives based on the trust services criteria.

The security, availability, and confidentiality criteria in *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* were promulgated by the ASEC, which has determined that the trust services criteria for security, availability, and confidentiality are suitable for use in the cybersecurity risk management examination. Because they are also made available to general users, the trust services criteria for security, availability, and confidentiality are both suitable and available control criteria for the cybersecurity risk management examination.

If management selects different criteria as either the description criteria or control criteria, the practitioner is responsible for determining whether he or she agrees with management's assessment about the suitability and availability of the other criteria. If the practitioner determines that the selected criteria are not suitable, the practitioner typically works with management of the entity to identify suitable criteria.

Preparing the Description of the Entity's Cybersecurity Risk Management Program in Accordance With the Description Criteria

As previously discussed, the description of the entity's cybersecurity risk management program is intended to provide report users with information that will enable them to better understand the entity's cybersecurity risk management program. For example, disclosures about the environment in which the entity operates, the process used to develop its cybersecurity objectives, commitments made to customers and others, responsibilities involved in operating and maintaining a cybersecurity risk management program, and the nature of the IT components used, allow users to better understand the context in which the processes and controls operate within the entity's cybersecurity risk management program.

Ordinarily, a description of an entity's cybersecurity risk management program is prepared in accordance with the description criteria when it

- describes the cybersecurity risk management program the entity has implemented (that is, placed in operation);
- includes information about each of the description criteria in *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program*; and
- does not omit or distort information that is likely to be relevant to users' decisions.

Management may organize its description in the manner it deems most effective, as long as each criterion is addressed within the description. Management may use various formats, such as narratives, flowcharts, tables, or graphics, or a combination thereof, to prepare the description. In addition, the degree of detail to be included in the description is generally a matter of judgment. The description is intended to be prepared at a level of detail sufficient to provide the context that users need to understand the entity's cybersecurity risk management program; however, it is not intended to include disclosures at such a detailed level that the likelihood of a hostile party exploiting a security vulnerability is increased. Furthermore, unless specifically required by a criterion, disclosures need not be quantified.

Consideration of the implementation guidance presented for each criterion in *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* will assist management when making judgments about the nature and extent of disclosures required by each criterion. However, the implementation guidance does not address all possible situations; therefore, the facts and circumstances in actual situations should be carefully considered when determining how the description criteria should be applied.

In certain circumstances, consideration should also be given to whether additional disclosures are necessary to supplement the description. Deciding whether such additional disclosures are necessary involves consideration of whether they are likely to effect the decisions of report users. Additional disclosures may include, for example,

- significant interpretations made in applying the criteria in the engagement circumstances (for example, what constitutes a security event or a security incident);
- subsequent events, depending on their nature and significance; and,
- when reporting on only a portion of the entity-wide cybersecurity risk management program, a significant security incident that occurred in another portion of that program not covered by the engagement.

Materiality Considerations When Preparing, and Evaluating the Presentation of, the Description in Accordance With the Description Criteria

As previously discussed, applying the description criteria requires judgment. One of those judgments involves the level of materiality that applies when preparing and evaluating the description of the entity's cybersecurity risk management program in accordance with the description criteria. Because the description criteria call for disclosure of primarily nonfinancial information, most descriptions will be presented in narrative form. Thus, materiality

considerations are mainly qualitative in nature and center around whether there are misstatements in, or omissions of, the information disclosed that could reasonably be expected to influence users' decisions. For that reason, an understanding of the perspectives and information needs of intended users of the report is necessary to the assessment of materiality.

Qualitative factors to be considered include matters such as whether

- the description is prepared at a level of detail likely to be meaningful to users.
- each of the description criteria in *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* has been addressed without using language that omits or distorts the information.
- the characteristics of the presentation are appropriate, since variations in presentation may occur.

For example, a description would not be presented in accordance with the description criteria if it

- omits information involving one or more significant business units or segments, when the engagement addresses the entity-wide cybersecurity risk management program.
- contains statements that cannot be objectively evaluated. (For example, describing an entity as being the "world's best" or "most respected in the industry" is subjective and, therefore, could be misleading to report users.)
- contains or implies certain facts that are not true (for example, that certain IT components exist when they do not, or that certain processes and controls have been implemented when they are not being performed).
- omits or distorts significant information related to any of the description criteria in a manner that might affect users' decisions.

Nevertheless, a description prepared in accordance with the description criteria is not required to disclose every matter related to the entity's cybersecurity risk management program that every user might consider useful when making decisions. For example, a description presented in accordance with the description criteria may omit certain information related to the entity's cybersecurity risk management program when that information is unlikely to be significant (in other words, it is immaterial) to report users' decisions.

When evaluating whether the description describes the cybersecurity risk management program the entity has implemented (that is, placed in operation), management considers whether there is alignment between the key security policies and processes described in the description and the controls the entity has designed and implemented to achieve the entity's cybersecurity objectives. Although management's description only includes information about the key security policies and processes, such key security policies and processes should be supported by controls designed and implemented to achieve the entity's cybersecurity objectives. The lack of comprehensive alignment between the key security policies and processes included in the description and the underlying controls necessary to achieve the entity's cybersecurity objectives would be an indicator of a description misstatement.

If the practitioner believes that the description is misstated or otherwise misleading, the practitioner ordinarily would ask management to amend the description by including the omitted information or revising the misstated information. If management refuses to amend the description, the practitioner considers the effect on his or her opinion about whether the presentation of the description is in accordance with the description criteria.

Preparing the Written Assertion

As previously stated, management is responsible for preparing the written assertion. In its assertion, management confirms, to the best of its knowledge and belief, that

a. the description was prepared in accordance with the description criteria.

b. controls within the cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

Having a Reasonable Basis for Management's Assertion

As previously discussed, management is responsible for having a reasonable basis for its assertion about the description and the effectiveness of controls within the cybersecurity risk management program. Furthermore, because management's assertion generally addresses the effectiveness of controls over a specified period of time, management's basis for its assertion should cover the same time frame as the assertion.

The implementation of an effective cybersecurity risk management program is a significant endeavor for most entities, requiring the design and operation of technology solutions and complex processes and procedures, including those governing interactions with third parties (customers, vendors, business partners, and others) and their information systems. Because of these complexities, controls within the entity's cybersecurity risk management program are unlikely to be effective without regular monitoring and assessment of controls. Therefore, monitoring and assessment of controls is ordinarily a key component of management's basis for its assertion.

For those reasons, management generally will need to perform a formal assessment of the effectiveness of its controls to make its assertion. In most cases, during the assessment process, management will do the following:

a. Evaluate the effectiveness of the entity's procedures for identifying

i. cybersecurity objectives based on the entity's business objectives (for instance, delivery of services, production of goods, or protection of assets);

ii. information and other assets of the entity that are at risk, based on the scope of the engagement and defined cybersecurity objectives; and

iii. the threats to the information and other assets based on internal and external threat intelligence data, inherent vulnerabilities of information assets and other assets, and the linkages between such vulnerabilities and identified threats.

b. Evaluate the effectiveness of the processes it uses to design and implement controls to mitigate the risks. Evaluating the effectiveness of such processes may involve comparing the results of monitoring activities and reviewing the results of independent assessments and other activities designed to continuously improve controls based on lessons learned from security events.

c. Assess the effectiveness of controls, particularly controls that monitor the effectiveness of other controls, to provide reasonable assurance of achieving the entity's cybersecurity objectives. (This is particularly important when aspects of the entity's cybersecurity risk management program controls have been outsourced to service providers.)

In addition to the factors discussed in the preceding paragraph, the effectiveness of the entity's cybersecurity controls is highly dependent on the existence of an accurate and complete inventory of the entity's information assets and standard acquisition processes and configuration settings. If these do not exist, it may be difficult, or even impossible, for management to have a reasonable basis for its assertion.

Management's basis for its assertion usually relies heavily on monitoring of controls. Monitoring activities typically include ongoing activities, separate evaluations, or a combination of the two. Ongoing monitoring activities are ordinarily built into the normal recurring activities of an entity's cybersecurity risk management program and include activities such as the regular review by management of key system reports and management participation in incident management processes. In addition, monitoring activities may include the periodic evaluations of controls through (*a*) assessments performed by the internal audit function or by knowledgeable personnel who are independent of the function being evaluated; (*b*) performance of penetration testing; and (*c*) review of reports of independent certifications made against established specifications (for example, International Standardization Organization and International Electrotechnical Commission [ISO/IEC] Standard 27001 and HITRUST CSF). When such monitoring activities do not exist or they appear to be inadequate, it may be difficult, if not impossible, for management to have a reasonable basis for its assertion.

Management generally documents the assessment in a variety of ways, such as through the use of policy manuals, narratives, flowcharts, decision tables, procedural write-ups, or questionnaires. The nature and extent of documentation usually varies, depending on the size and complexity of the entity and its monitoring activities.

Consideration of Third Parties

Monitoring activities are of increased importance if the entity has identified cybersecurity threats and vulnerabilities arising from interactions with third parties. As used in this document, the term *third parties* includes customers, vendors, business partners, and others who have access to one or more of the entity's information systems, store confidential entity information on their systems, or otherwise transmit information back and forth between themselves and the entity or on behalf of the entity.

Therefore, it is important for management to assess the cybersecurity risks arising from interactions with third parties, particularly when third parties operate controls necessary to achieve the entity's cybersecurity objectives.

If management determines the risks associated with third parties are likely to be material to the achievement of the entity's cybersecurity objectives (for example, due to the nature of access the third party has to the entity's systems and information assets, or because of the controls the third party operates on behalf of the entity), monitoring controls at the entity are needed to allow management to determine whether the processes and controls performed by the third parties effectively address the identified risks. Such monitoring controls may include, but are not limited to, a combination of the following:

- Conducting assessments of whether third-party contractual agreements are in accordance with the entity's policies
- Conducting periodic discussions with third parties and their employees
- Inspecting completed third-party security questionnaires and submitted documents to support their responses
- Conducting regular site visits to the third parties' locations to observe the execution of controls
- Inspecting results of internal audit tests over the third parties' controls
- Inspecting type 2 SOC 2 reports on aspects of the third parties' operations that relate to their security, availability, and confidentiality controls pursuant to the attestation standards

Management is responsible for the effectiveness of all processes and controls related to the entity's cybersecurity risk management program, regardless of who performs the specific processes and controls. Therefore, unless management has processes and controls that monitor the effectiveness of the processes and controls performed by third parties, it may be difficult, if not impossible, for management to have a reasonable basis for its assertion. For that reason, the practitioner ordinarily would make inquiries of management about the entity's use of third parties, including the nature and extent of the entity's monitoring controls, to determine whether such controls are likely to be sufficient in the circumstances.

Management's Responsibilities at or Near Engagement Completion

Management's responsibilities at or near completion of the cybersecurity risk management examination include the following:

- Modifying the description, if appropriate
- Providing management's written assertion
- Providing written representations, as previously discussed
- Informing the practitioner of subsequent events
- Distributing the report to appropriate parties

Modifying Management's Assertion

As previously discussed, management provides the practitioner with a written assertion about whether the description is presented in accordance with the description criteria and whether the controls within the cybersecurity risk

management program were effective to achieve the entity's cybersecurity objectives. Management's written assertion is generally expected to align with the practitioner's opinion by reflecting the same modifications.

The following is an example of modifications (indicated with bold text) that might be made to management's assertion when controls were not effective to achieve the entity's cybersecurity objectives and the practitioner has modified that component in his or her report:

> [*Assertion paragraph*]
>
> We assert that the description throughout the period [*date*] to [*date*] is presented in accordance with the description criteria. We have performed an evaluation of the effectiveness of the controls within the cybersecurity risk management program throughout the period [*date*] to [*date*] using the [*name of the control criteria, e.g., the criteria for security, availability, and confidentiality set forth in TSP section 100*, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy *(AICPA,* Trust Services Criteria*) or other suitable criteria*] (control criteria). Based on this evaluation, we assert that, **with the exception of the matter described in the following paragraph**, the controls were effective to achieve the entity's cybersecurity objectives throughout the period [*date*] to [*date*] based on the control criteria.
>
> **The description of our cybersecurity risk management program states on page 8 that application changes are tested prior to their implementation. The procedures, however, do not include a requirement for scanning application code for known vulnerabilities prior to placing the change into operation. As a result, the controls were not effective to meet criterion CC8.1, *The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.***

Providing Written Representations to the Practitioner

During the cybersecurity risk management examination, management makes many oral and written representations to the practitioner in response to specific inquiries or through the presentation of the description of the entity's cybersecurity risk management program and its assertion.

Written representations from management ordinarily confirm representations explicitly or implicitly given to the practitioner, indicate and document the continuing appropriateness of such representations, and reduce the possibility of misunderstanding concerning the matters that are the subject of the representations. The attestation standards require the practitioner to request written representations in the form of a letter from management.

At a minimum, written representations requested in the cybersecurity risk management examination should

a. include management's assertion about the subject matters based on the criteria.

b. state that

   i. all relevant matters are reflected in the measurement or evaluation of the subject matters or assertion,

ii. all known matters contradicting the subject matters or assertion are included, and

iii. any communication from regulatory agencies or others affecting the subject matters or assertion have been disclosed to the practitioner, including communications received between the end of the period addressed in the written assertion and the date of the practitioner's report.

c. acknowledge management's responsibility for

i. the subject matters and the assertion,

ii. selecting the criteria, and

iii. determining that such criteria are appropriate for management's purposes.

d. state that any known events subsequent to the period (or point in time) of the subject matters being reported on that would have a material effect on the subject matters or assertion have been disclosed to the practitioner.

e. state that management has provided the practitioner with all relevant information and access.

f. state that the responsible party believes the effect of uncorrected misstatements (description misstatements and deficiencies) are immaterial, individually and in the aggregate, to the subject matters.

g. state that management has disclosed to the practitioner

i. all deficiencies in internal control relevant to the cybersecurity risk management examination of which it is aware;

ii. its knowledge of any actual, suspected, or alleged fraud or noncompliance with laws or regulations affecting the subject matters;

iii. identified security incidents that significantly affected the entity's achievement of its cybersecurity objectives; and

iv. other matters the practitioner deems appropriate (such as discussion of matters considered material).

The written representations required are separate from, and in addition to, management's written assertion. They are usually made in the form of a representation letter, addressed to the practitioner, dated as of the date of the practitioner's report, and they should address the subject matters and periods referred to in the practitioner's opinion.

Informing the Practitioner About Subsequent Events and Subsequently Discovered Facts

Events or transactions may occur after the specified period of time covered by the examination engagement, but prior to the date of the practitioner's report, that could have a significant effect on the description of the entity's cybersecurity risk management program or the conclusion about the effectiveness of controls within that program. In such circumstances, disclosure in the description or in management's assertion may be necessary to prevent users of the cybersecurity risk management examination report from being misled.

The following are examples of events that could affect the description of the entity's cybersecurity risk management program or management's assertion:

- After the period covered by the examination engagement, management discovered that, during the last quarter of that period, the IT security director provided all the programmers with access to the production data files, enabling them to modify data.
- After the period covered by the examination engagement, management discovered that a confidentiality breach occurred at the entity during the period covered by the practitioner's report.

If such events exist, management should inform the practitioner, who should apply appropriate procedures to obtain evidence regarding the events. After obtaining information about the event(s), the practitioner ordinarily will discuss the matter with management to determine whether the facts existed at the date of the report and, if so, whether persons who would attach importance to these facts are currently using, or likely to use, the cybersecurity risk management examination report (which includes management's description and assertion and the practitioner's report).

Specific actions to be taken at that point depend on a number of factors, including the time elapsed since the date of the practitioner's report and whether issuance of a subsequent report is imminent. Depending on the circumstances, the practitioner may determine that notification of persons currently using or likely to use the practitioner's report is necessary. This may be the case, for example, when

- the cybersecurity risk management examination report is not to be relied upon because
  - — the description, management's assertion, or the practitioner's report needs revision or
  - — the practitioner is unable to determine whether revision is necessary and
  - — issuance of a subsequent practitioner's report is not imminent.

If the practitioner believes the event is of such a nature and significance that its disclosure is necessary to prevent users of the cybersecurity risk management examination report from being misled, the practitioner should determine whether information about the event is adequately disclosed in the description or management's assertion.

Sometimes, events discovered subsequent to the period covered by the examination engagement would likely have had no effect on either the presentation of the description in accordance with the description criteria or the effectiveness of controls, because the underlying situation did not exist until after the period covered by the cybersecurity risk management examination report. However, the matter may be sufficiently important to warrant disclosure by management in its description and, potentially, emphasis by the practitioner in the practitioner's report. The following are examples of such events:

- The entity was acquired by another entity.
- The entity experienced a significant operating disruption.

- A data center-hosting entity that provides applications and technology that enable user entities to perform essential business functions made significant changes to its information systems, including a system conversion or significant outsourcing of operations.

Appendix B

Illustrative Comparison of the Cybersecurity Risk Management Examination with a SOC 2 Examination and Related Reports

This appendix is nonauthoritative and is included for informational purposes only.

The following table compares the cybersecurity risk management examination with a SOC 2 engagement and related reports. Within the Cybersecurity Risk Management Examination and the SOC 2 Engagement columns, certain text is set in bold to highlight key distinctions between the two types of engagement:

	Cybersecurity Risk Management Examination[1]	***SOC 2 Engagement*** [2,3]
What is the purpose of the report?	To provide **intended users** with useful information about an entity's cybersecurity risk management program for making informed decisions	To provide a broad range of **system users** with information about controls at the service organization relevant to security, availability, processing integrity, confidentiality, or privacy to support users' evaluations of their own systems of internal control

(*continued*)

[1] In a SOC 2 engagement, when the entity uses the services of a subservice organization, management may elect to use the *inclusive method* or the *carve-out method* to address those services in its description of its system. Those concepts are defined and discussed in the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, and Privacy (SOC 2®)* (the SOC 2 guide).

In the cybersecurity risk management examination, however, management is responsible for all of the controls within the entity's cybersecurity risk management program, regardless of whether those controls are performed by the entity or by a service organization. Therefore, the description criteria in appendix C, "Description Criteria for Use in the Cybersecurity Risk Management Examination," require the description to address all of the controls within the entity's cybersecurity risk management program.

[2] Some of an entity's business partners may need a detailed understanding of controls implemented by the entity and the operating effectiveness of those controls to enable them to design and operate their own control activities. For example, business partners whose IT systems are interconnected with systems at the entity may need to understand the specific logical access protection over the interconnected systems implemented by the entity.

This guide is not intended to meet the needs of business partners who need a detailed understanding of the entity's specific controls and their operating effectiveness. The SOC 2 guide provides guidance for practitioners engaged to examine and report on system controls at a service organization. In addition, the AICPA intends to develop a vendor supply chain guide to provide guidance for practitioners engaged to examine and report on system controls at a manufacturer or distributer. The vendor supply chain guide is expected to be issued in 2018.

[3] For illustrative purposes, this table focuses specifically on a type 2 SOC 2 report, which includes both an opinion on suitability of design and operating effectiveness of controls.

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

	Cybersecurity Risk Management Examination	*SOC 2 Engagement*
Who are the intended users?	Management, directors, analysts, investors, and others whose decisions might be affected by the effectiveness of the entity's cybersecurity risk management program	Management of the service organization and other specified parties **with sufficient knowledge and understanding of the service organization and its system**
Under what professional standards and implementation guidance is the engagement performed?	AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements*, in AICPA *Professional Standards*	AT-C section 105, *Concepts Common to All Attestation Engagements*, and AT-C section 205, *Examination Engagements*,[4] in AICPA *Professional Standards*
	The AICPA Guide *Reporting on an Entity's Cybersecurity Risk Management Program and Controls*	The AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)*[5]
Who is the responsible party?	Management of an **entity**	Management of a **service organization**
Is the report appropriate for general use or restricted to specified parties?	**Appropriate for general use**[6]	**Restricted to user entity personnel and specified parties**, such as independent auditors and practitioners of user entities, prospective user entities, and regulators, who have sufficient knowledge and understanding of the following matters:[7]

[4] As discussed in the preface to this guide, the clarified attestation standards are effective for practitioner's reports dated on or after May 1, 2017. Prior to that, SOC 2 engagements were performed in accordance with AT section 101, *Attest Engagements* (AICPA, *Professional Standards*).

[5] The AICPA is in the process of updating the SOC 2 guide to incorporate revisions needed to make the guide more responsive to users' cybersecurity concerns. The revised guide is expected to be issued in 2017.

[6] The term *general use* refers to reports whose use is not restricted to specified parties. Nevertheless, as discussed in chapter 4, "Forming the Opinion and Preparing the Practitioner's Report," practitioners may decide to restrict the use of their report to specified parties.

[7] Because the report is only appropriate for users that possess such knowledge and understanding, the SOC 2 report is restricted to the use of such specified users.

	Cybersecurity Risk Management Examination	*SOC 2 Engagement*
		• The nature of the service provided by the service organization • How the service organization's system interacts with user entities and other parties • Internal control and its limitations • The nature of user entity responsibilities and their role in the user entities' internal control as it relates to service organizations • The nature of subservice organizations and how their services to a service organization may affect user entities • The applicable trust services criteria • The risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks
What is the subject matter of management's assertion and the engagement?	The description of the **entity's cybersecurity risk management program** based on the description criteria	The description of the **service organization's system** as it relates to one or more of the categories in the trust services criteria
	The effectiveness of controls within that program to achieve the entity's cybersecurity objectives based on the control criteria	Suitability of design and operating effectiveness of controls at a service organization relevant to security, availability, processing integrity, confidentiality, or privacy based on the criteria

(*continued*)

	Cybersecurity Risk Management Examination	*SOC 2 Engagement*
What are the criteria for the engagement?	The **description criteria** included in appendix C, "Description Criteria for Use in the Cybersecurity Risk Management Examination," of this guide	Paragraphs 1.26–1.27 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* contain the **criteria for the description** of the service organization's system.
	The trust services criteria for security, availability, and confidentiality included in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), and presented in appendix D, "Trust Services Criteria for Security, Availability, and Confidentiality for Use as Control Criteria in the Cybersecurity Risk Management Examination," of this guide. Such criteria are suitable for use as **control criteria.**[8,9]	TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), contains the **criteria for evaluating the design and operating effectiveness of controls**.

,

[8] For both the description criteria and control criteria in a cybersecurity risk management examination, suitable criteria other than those outlined in this guide may also be used.

[9] Concurrent with the issuance of this guide, the AICPA issued revisions to the extant trust services criteria. The 2017 trust services criteria presented in this document will be codified as TSP section 100. The extant trust services criteria issued in 2016 will be available in TSP section 100A through December 15, 2018. After that date, the 2016 criteria will be considered superseded. During the transition period (April 15, 2017, through December 15, 2018), practitioners should distinguish in their reports whether the 2016 or the 2017 trust services criteria have been used.

In addition, the AICPA will continue to make available the 2014 trust services criteria in TSP section 100A-1 until March 31, 2018, to ensure they remain available to report users. Those criteria were considered superseded for practitioner reports for periods ended on or after December 15, 2016.

Because cybersecurity risk management examination engagements are new service offerings, entities that elect to use the trust services criteria as the control criteria in such engagements should use the revised trust services criteria for security, availability, and confidentiality presented in appendix D.

	Cybersecurity Risk Management Examination	*SOC 2 Engagement*
What are the contents of the report?	A description of the **entity's cybersecurity risk management program** A written assertion by management about whether (*a*) the description of the entity's cybersecurity risk management program was presented in accordance with the description criteria and (*b*) controls within the program were effective in achieving the entity's cybersecurity objectives based on the control criteria A practitioner's report that contains an opinion about whether (*a*) the description of the entity's cybersecurity risk management program was presented in accordance with the description criteria and (*b*) the controls within that program were effective in achieving the entity's cybersecurity objectives based on the control criteria	A description of the **service organization's system** A written assertion by management of the service organization regarding the description of the service organization's system and the suitability of the design and the operating effectiveness of the controls in meeting the applicable trust services criteria A service auditor's[10] report that contains an opinion on the fairness of the presentation of the description of the service organization's system and the suitability of the design and operating effectiveness of the controls to meet the criteria **In a type 2 report, a description of the service auditor's tests of controls and the results of the tests**

[10] The practitioner in a SOC 2 examination is referred to as a *service auditor*.

Appendix C

Description Criteria for Use in the Cybersecurity Risk Management Examination

This appendix is nonauthoritative and is included for informational purposes only.

The description criteria and related implementation guidance in this appendix has been extracted from *Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program* issued in April 2017 by the AICPA's Assurance Services Executive Committee. The complete text may be found at www.aicpa.org/cybersecurityriskmanagement.

NATURE OF BUSINESS AND OPERATIONS
DC1: The nature of the entity's business and operations, including the principal products or services the entity sells or provides and the methods by which they are distributed
Implementation Guidance
When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:
• *The entity's principal markets, including the geographic locations of those markets, and changes to those markets*
• *If the entity operates more than one business, the relative importance of the entity's operations in each business and the basis for management's determination (for example, revenues or asset values)*
NATURE OF INFORMATION AT RISK
DC2: The principal types of sensitive information created, collected, transmitted, used, or stored by the entity
Implementation Guidance
When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:
• *Information regarding individuals that warrants protection based on law, commitment, or reasonable expectation of confidentiality (for example, personally identifiable information, protected health information, and payment card data)*
• *Third-party entity information (for example, information subject to confidentiality requirements in contracts) that warrants protection based on law, commitment, or reasonable expectation of confidentiality, availability, and integrity*
• *Entity information (for example, trade secrets, corporate strategy, and financial and operational data) whose confidentiality, availability and integrity is necessary to the achievement of the entity's business objectives*

(*continued*)

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

CYBERSECURITY RISK MANAGEMENT PROGRAM OBJECTIVES (*CYBERSECURITY OBJECTIVES*)
DC3: The entity's principal cybersecurity risk management program objectives (cybersecurity objectives) related to availability, confidentiality, integrity of data, and integrity of processing
Implementation Guidance   *When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:*
• *An entity ordinarily establishes cybersecurity objectives that address the following:*   — *Commitments made to customers, vendors, business partners, and others related to the security and availability of information and systems, including commitments related to public well-being as it relates to the entity's products and operations, infrastructure, and extended supply chains*   — *Laws and regulations to which the entity is subject as a result of the types of information it possesses or uses (for example, protected health information and personally identifiable information)*   — *Commitments made as part of a certification and authorization process for government agencies and other parties*   — *Industry standards to which the entity is subject as a result of the types of information it uses (for example, Payment Card Industry Data Security Standards for organizations that accept or process credit card transactions) and*   — *Other business initiatives*
• *An entity's cybersecurity objectives depend on the nature of the entity's business and the industry in which it operates; accordingly, they should reflect the entity's specific cybersecurity risks. The following is an example of cybersecurity objectives an entity might establish.*   ***Availability***   *Enabling timely, reliable, and continuous access to and use of information and systems to support operations and to*   • *comply with applicable laws and regulations;*   • *meet contractual obligations and other commitments;*   • *provide goods and services to customers without disruption;*   • *safeguard entity assets and assets held in custody for others; and*   • *facilitate decision making in a timely manner.*

Confidentiality

Protecting information from unauthorized access and disclosure, including means for protecting proprietary information and personal information subject to privacy requirements, to

- *comply with applicable laws and regulations;*
- *meet contractual obligations and other commitments; and*
- *safeguard the informational assets of an entity.*

Integrity of Data

Guarding against improper capture, modification or destruction of information to support the following:

- *The preparation of reliable financial information for external reporting purposes*
- *The preparation of reliable nonfinancial information for external reporting purposes*
- *The preparation of reliable information for internal use*
- *Information nonrepudiation and authenticity*
- *The completeness, accuracy, and timeliness of processing*
- *Management, in holding employees and users accountable for their actions*
- *The storage, processing, and disclosure of information, including personal and third-party information*

Integrity of Processing

Guarding against improper use, modification, or destruction of systems to support the following:

- *The accuracy, completeness, and reliability of information, goods, and services produced*
- *The safeguarding of entity assets*
- *Safeguarding of life and health*

Guarding against the unauthorized use or misuse of processing capabilities that could be used to impair the security or operations of external parties

- *An entity may consider risk appetite when establishing its cybersecurity objectives. An entity's risk appetite refers to the amount of risk it is willing to accept to achieve its business objectives. Risk appetite often affects the entity's risk management philosophy, influences the entity's culture and operating style, and guides resource allocation. Therefore, it might be helpful for an entity to describe its cybersecurity objectives in relation to its risk appetite.*

(*continued*)

DC4: The process for establishing, maintaining, and approving cybersecurity objectives to support the achievement of the entity's objectives
Implementation Guidance
When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:
• *The process for establishing cybersecurity objectives based on the entity's business and strategic objectives established by the board of directors*[1] *and management*
• *The process for obtaining board of director or executive management approval of the entity's cybersecurity objectives*
• *The use of security management and control frameworks in establishing the entity's cybersecurity objectives and developing and maintaining controls within the entity's cybersecurity risk management program, including disclosure of the particular framework(s) used (for example, NIST Cybersecurity Framework, ISO 27001/2 and related frameworks, or internally- developed frameworks based on a combination of sources)*
FACTORS THAT HAVE A SIGNIFICANT EFFECT ON INHERENT CYBERSECURITY RISKS
DC5: Factors that have a significant effect on the entity's inherent cybersecurity risks, including the (1) characteristics of technologies, connection types, use of service providers, and delivery channels used by the entity, (2) organizational and user characteristics, and (3) environmental, technological, organizational and other changes during the period covered by the description at the entity and in its environment.
Implementation Guidance
When making judgments about the nature and extent of disclosures to include about the characteristics of technologies, connection types, use of service providers, and delivery channels used by the entity, consider the following:
• *Use of outsourcing such as cloud computing and IT-hosted services*
• *Use of mobile devices, platforms, and deployment approaches*
• *Network architecture and strategy, including the extent of the use of virtualization*
• *Types of application and infrastructure (for example, DB, OS types and technologies) and the source (for example, internally developed or purchased without modification) of such applications and infrastructure*

[1] The term *board of directors* is used throughout this document to refer to those individuals with responsibility for overseeing the strategic direction of the entity and the obligations related to the accountability of the entity. Depending on the nature of the entity, such responsibilities may be held instead by a supervisory board for a corporation, a board of trustees for a not-for-profit entity, a board of governors or commissioners for a government entity, general partners for a partnership, or an owner for a small business.

• *Types of service providers that store, process, and transmit sensitive data or access the entity's systems, the nature of the services provided, and the nature of their access and connectivity to environment and sensitive data*
• *Types of other external party access and connectivity to information systems and sensitive data*
• *Nature of external-facing web applications and the nature of applications developed in-house*
• *Dependency on strategically significant IT equipment and systems that are no longer supported or would be difficult to repair or replace in the event of failure*
• *Dependency on strategically significant IT equipment and systems based on emerging technologies*
When making judgments about the nature and extent of disclosures to include about organizational and user characteristics, consider the following:
• *IT organization size and structure (for example, centralized versus decentralized, insourced or outsourced)*
• *Types of user groups (for example, employees, customers, vendors, and business partners)*
• *Whether the entity's information assets, employees, customers, vendors, or business partners are located in countries deemed high risk by management as part of its risk assessment process*
• *The distribution of responsibilities related to the cybersecurity risk management program between business functions (for example, operating units, risk management, and legal) and IT*
• *Business units with IT systems administered under a separate management structure (for example, outside of a centralized IT function)*
When making judgments about the nature and extent of disclosures to include about environmental, technological, organizational, and other changes at the entity and in its environment during the period covered by the description, consider the following:
• *Changes to the entity's principal products, services, or distribution methods*
• *Changes to business unit, IT, and security personnel*
• *Significant changes to entity processes, IT architecture and applications, and the processes and systems used by outsourced service providers*
• *Acquisitions and other business units that have not been fully integrated into the cybersecurity risk management program including the integration or segmentation strategy used for the acquiree's IT systems, and the current state of those activities*
• *Changes to legal and regulatory requirements*
• *Divestures and other cessation of operations, particularly those that have ongoing service support obligations for systems related to those operations (if any), and the current status of those activities*

(*continued*)

DC6: For security incidents that (1) were identified during the 12-month period preceding the period end date of management's description and (2) resulted in a significant impairment of the entity's achievement of its cybersecurity objectives, disclosure of the following (*a*) nature of the incident; (*b*) timing surrounding the incident; and (*c*) extent (or effect) of those incidents and their disposition
Implementation Guidance
When making judgments about the nature and extent of disclosures to include about this criterion, consider the following regarding the incident:
• *Was considered sufficiently significant based on law or regulation to require public disclosure*
• *Had a material effect on the financial position or results of operations and required disclosure in financial statement filings*
• *Resulted in sanctions by any legal or regulatory agency*
• *Resulted in withdrawal from material markets or cancellation of material contracts*
CYBERSECURITY RISK GOVERNANCE STRUCTURE
DC7: The process for establishing, maintaining, and communicating integrity and ethical values to support the functioning of the cybersecurity risk management program
Implementation Guidance
When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:
• *How management sets the tone at the top*
• *The establishment and enforcement of standards of conduct for entity personnel*
• *The process used to identify and remedy deviations from established standards*
• *Consideration of contractors and vendors in process for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner*
DC8: The process for board oversight of the entity's cybersecurity risk management program
Implementation Guidance
When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:
• *The extent of the board of directors' cybersecurity and IT expertise or access to external cybersecurity and IT expertise, or both*
• *Identification of the board committee designated with oversight of the entity's cybersecurity risk management program, if any*

• *The frequency and detail with which the board or committee reviews or provides input into cybersecurity-related matters, including board oversight of security incidents*
DC9: Established cybersecurity accountability and reporting lines
Implementation Guidance
When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:
• *The responsibility for the review and oversight of the cybersecurity risk management program by senior management*
• *The identification of the designated cybersecurity leader (for example, chief information security officer), and the reporting of that individual to executive management and board of directors*
• *The roles and responsibilities of entity personnel who perform cybersecurity controls and activities*
• *The process for addressing the oversight and management of external parties (for example, vendors) when establishing structures, reporting lines, authorities, and responsibilities*
DC10: The process used to hire and develop competent individuals and contractors and to hold those individuals accountable for their cybersecurity responsibilities
Implementation Guidance
When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:
• *The process for considering the competence of qualified personnel with cybersecurity responsibilities, including the performance of background checks, assessment of educational levels and certifications, requirements for ongoing training, hiring contractors, and the use of offshore recruiting*
• *The program for providing cybersecurity awareness and training to employees and contractors based on their cybersecurity responsibilities and access to information and information systems*
• *The process for making sure that employees and contractors have the resources necessary to carry out their cybersecurity responsibilities*
• *The process for identifying the types and levels of cybersecurity professionals needed*
• *The processes used to communicate performance expectations and hold individuals accountable for the performance of their responsibilities*
• *The processes to update communication and accountability mechanisms and monitor employee compliance with their responsibilities and entity policies*
• *The process used to reward individuals for performance and the process used to align the measures used to the achievement of the entity's objectives*

(*continued*)

CYBERSECURITY RISK ASSESSMENT PROCESS
DC11: The process for (1) identifying cybersecurity risks and environmental, technological, organizational and other changes that could have a significant effect on the entity's cybersecurity risk management program and (2) assessing the related risks to the achievement of the entity's cybersecurity objectives
Implementation Guidance *When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:*
• *The use of inventory management to classify the entity's information assets, including hardware, virtualized systems and software (licensed and public domain), according to their nature, criticality, and sensitivity*
• *The identification of the roles responsible for or participating in the risk assessment process*
• *How the process includes the consideration of the types, likelihood, and impact of risks to information assets, including manufacturing and industrial control systems, from potential threats including:* — *Intentional (for example, fraud) and unintentional internal and external acts* — *Identified and unidentified threats* — *Those risks arising from different types of employee personnel (for example, finance, administrative, operations, IT, and sales and marketing) and others (for example, contractors, vendor employees, and business partners) with access to information and systems*
• *How the process includes the consideration of identified and unidentified vulnerabilities and control deficiencies*
• *Obtaining threat and vulnerability information from information-sharing forums and other sources*
• *The on-going process for identifying changes in the entity and its environment that would result in new risks or changes to existing risks, including these:* — *The use of new technologies* — *Changes to the regulatory, economic, and physical environment in which the entity operates* — *New business lines* — *Changes to the composition of existing business lines* — *Changes in available resources* — *Acquired or divested business operations* — *Rapid growth* — *Changing operational presence in foreign countries* — *Changing political climates*

- *The process for identifying the need for and performing ad hoc risk assessments*
- *The roles responsible and accountable for identifying and assessing changes*

DC12: The process for identifying, assessing, and managing the risks associated with vendors and business partners

Implementation Guidance

When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:

- *The process for identifying vendors and business partners affecting the entity's cybersecurity risk management program and maintaining an inventory of those parties*
- *How the process takes into consideration the types, likelihood, and impact of risks to information assets (including manufacturing and industrial control systems) from potential threats, including the risks arising from the use of external parties that store, process, or transmit sensitive information on the entity's behalf (for example, suppliers, customers, vendors, business partners, and those entities' relevant vendors and business partners)*
- *The process for identifying and evaluating risks that could be mitigated through the purchase of cybersecurity insurance*
- *How the entity manages risks to the achievement of its cybersecurity objectives arising from vendors and business partners, including the following:*
  - *Establishing specific requirements for a vendor and other business partner engagement that includes scope of services and product specifications, roles and responsibilities, compliance requirements, and service levels*
  - *Assessing, on a periodic basis, the risks that the vendors and business partners represent to the achievement of the entity's objectives, including risks that arise from those entities' relevant vendors and business partners (often referred to as fourth party risk)*
  - *Assigning responsibility and accountability for the management of associated risks*
  - *Establishing communication and resolution protocols for service and product issues, including reporting of identified threats*
  - *Establishing exception-handling procedures*
  - *Periodically assessing the performance of vendors and business partners and those entities' relevant vendors and business partners*
  - *Implementing procedures for addressing associated risks*

(*continued*)

CYBERSECURITY COMMUNICATIONS AND QUALITY OF CYBERSECURITY INFORMATION
DC13: The process for internally communicating relevant cybersecurity information necessary to support the functioning of the entity's cybersecurity risk management program, including (1) objectives and responsibilities for cybersecurity and (2) thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both
Implementation Guidance   *When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:*
• *Methods used to communicate to personnel, including executive management, information to enable them to understand and carry out their cybersecurity responsibilities (for example, through the use of*   — *Awareness programs, including training about detecting and avoiding social engineering threats and security breach reporting and response*   — *Job descriptions*   — *Acknowledgement of code of conduct and policies,*   — *Employee signed confidentiality agreements, and*   — *Policy and procedures manuals)*
• *Communications with the board of directors to enable members to have the information, including training and reference materials, needed to fulfill their roles*
• *The process for creating and updating communications, including considerations of timing, audience, and nature of information when selecting the communication method to be used*
• *The use of various communication channels, such as whistle-blower hotlines, to enable anonymous or confidential communication when normal channels are inoperative or ineffective*
DC14: The process for communicating with external parties regarding matters affecting the functioning of the entity's cybersecurity risk management program
Implementation Guidance   *When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:*
• *The existence and use of open communication channels that allow input from customers, consumers, vendors, business partners, external auditors, regulators, financial analysts, and others to provide management and the board of directors with relevant information*
• *The process for creating and updating communications regarding cybersecurity, including considerations of timing, audience, and nature of information when selecting the communication method to be used*

- *The use of various communication channels, such as whistle-blower hotlines, to enable anonymous or confidential communication when normal channels are inoperative or ineffective*

- *The process by which legal, regulatory, and fiduciary requirements, including required communication of data breaches and incidents, are considered when making communications*

MONITORING OF THE CYBERSECURITY RISK MANAGEMENT PROGRAM

DC15: The process for conducting ongoing and periodic evaluations of the operating effectiveness of key control activities and other components of internal control related to cybersecurity

Implementation Guidance

When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:

- *The variety of different types of ongoing and separate evaluations used, which may include a combination of periodic and continuous internal audit assessments, penetration testing, and independent certifications made against established security and other specifications (for example, ISO 27001 and HITRUST)*

- *The process for considering the rate of change in business and business processes when selecting and developing such evaluations*

- *The process for performing the ongoing and periodic evaluations, including whether (a) the design and current state of the entity's cybersecurity risk management program, including the controls, are used to establish a baseline; (b) evaluators have sufficient knowledge to understand what is being evaluated; and (c) the scope and frequency of the evaluations is commensurate with the risk*

DC16: The process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the board of directors, as appropriate

Implementation Guidance

When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:

- *The process by which management and the board of directors, as appropriate, assess results of ongoing and periodic evaluations, including whether the process considers the remediation of identified security threats, vulnerabilities, and control deficiencies*

- *The process for communicating identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate*

- *The process for monitoring remediation of identified deficiencies*

(*continued*)

CYBERSECURITY CONTROL PROCESSES
DC17: The process for developing a response to assessed risks, including the design and implementation of control processes
Implementation Guidance   *When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:*
• *The process to align controls with risk responses needed to protect information assets and to detect, respond to, mitigate and recover from security events based on the assessed risks*
• *The consideration of the environment in which the entity operates, the complexity of the environment, the nature and scope of the entity's operations, and its specific characteristics when selecting and developing control processes*
• *The process for including a range and variety of controls (for example, manual and automated controls and preventive and detective controls) in risk mitigation activities to achieve a balanced approach to the mitigation of identified cybersecurity risks*
• *The use of risk transfer strategies, including the purchase of insurance, to address risks that are not addressed by controls*
DC18: A summary of the entity's IT infrastructure and its network architectural characteristics
Implementation Guidance   *When making judgments about the nature and extent of disclosures to include about this criterion, consider the following:*
• *The use of segmentation, where appropriate, and baseline configurations of both physical and virtual end points, devices, firewalls, routers, switches, operating systems, databases, and applications*
• *The use of infrastructure and network elements provided by outsourced service providers*
DC19: The key security policies and processes implemented and operated to address the entity's cybersecurity risks, including those addressing the following: ***a.*** **Prevention of intentional and unintentional security events**   ***b.*** **Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents**   ***c.*** **Management of processing capacity to provide for continued operations during security, operational, and environmental events**   ***d.*** **Detection, mitigation, and recovery from environmental events and the use of back-up procedures to support system availability**

e. **Identification of confidential information when received or created, determination of the retention period for that information, retention of the information for the specified period, and destruction of the information at the end of the retention period**
Implementation Guidance
When making judgments about the nature and extent of disclosures to include about the key security policies and processes, consider the following:
• *The existence of a formal security policy established to implement the entity's cybersecurity strategy*
• *Key topics addressed by the security policy*
When making judgments about the nature and extent of disclosures to include about the prevention of intentional and unintentional security events, consider the following:
• *Protection of data whether at-rest, during processing, or in-transit*
• *Data loss prevention*
• *User identification, authentication, authorization, and credentials management*
• *Physical and logical access provisioning and de-provisioning, including remote access*
• *Privileged account management*
• *IT asset management, including hardware and software commissioning, configuration, maintenance, and decommissioning, as well as physical and logical servers and other devices*
• *Operating location and data center physical security and environmental safeguards*
• *Monitoring and managing changes to systems made internally or by external parties, including software acquisition, development, and maintenance and patch management*
When making judgments about the nature and extent of disclosures to include about the detection of security events; identification of security incidents; development of a response to those incidents; and implementation activities to mitigate and recover from identified security incidents; consider the following:
• *The deployment of tools and programs, the implementation of monitoring processes and procedures, or operation of other measures to identify anomalies, analyzing anomalies to identify security events, and communicating identified security events to appropriate parties*
• *The deployment of procedures to measure the effectiveness of activities planned in the event of a disruption to operations that requires the recovery of processing at alternate locations and the updating of plans based on the result of those procedures*

(*continued*)

• *The process by which management identifies security incidents from detected security events*
• *The process by which management identifies security incidents based on notification of security events received from third parties*
• *The process by which management evaluates security incidents and assesses the corrective actions needed to respond to and mitigate the harm from incidents*
• *The process by which management assesses the impact of security incidents to data, software, and infrastructure*
• *The process by which management restores operations after identified security incidents, including the oversight and review of the recovery activities by executive management*
• *The process by which the incident response plan is updated based on the analysis of lessons learned*
• *The process used to communicate information about the security incident, including the nature of the incident, restoration actions taken, and activities required for future prevention of the event to management and executive management*
• *The process used to make communications to affected third parties about the security incident*
• *The process for periodically testing the incident response plan*
When making judgments about the nature and extent of disclosures to include about the management of processing capacity to provide for continued operations during security, operational, and environmental events, consider the following:
• *The deployment of tools and programs, the implementation of monitoring processes and procedures, or operation of other measures to monitoring capacity usage*
• *The process for forecasting capacity needs and the process for requesting system changes to address those needs*
• *The procedures for assessing the accuracy of the capacity forecasting process and revising the process to improve accuracy*
When making judgments about the nature and extent of disclosures to include about the detection, mitigation, and recovery from environmental events and the use of back-up procedures to support system availability, consider the following:
• *The deployment of tools and programs, the implementation of monitoring processes and procedures, or operation of other measures to identify developing environmental threat events and the mitigation of those threats*
• *The processes identifying data for backup and for backing up and restoring data to support continued availability in the event of the destruction of data within systems*

• *The process for developing and maintaining a business continuity plan, including procedures for the recovery of operations in the event of a disaster at key processing locations*
• *Key topics addressed by the business continuity plan, including identification and prioritization of systems and data for recovery and provision for alternate processing infrastructure in the event normal processing infrastructure becoming unavailable*
• *Procedures for periodically testing the procedures set forth in the business continuity plan*
When making judgments about the nature and extent of disclosures to include about the identification of confidential information when received or created; determination of the retention period for that information; retention of the information for the specified period; and destruction of the information at the end of the retention period, consider the following:
• *The process for establishing retention periods for types of confidential information and identifying the information when received or created and associating the information to a specific retention period*
• *The process for identifying information classified as confidential*
• *The process for preventing the destruction of identified information during its specified retention period*
• *The process for identifying information that has reached the end of its retention period and information that is an exception to the retention policies*
• *The process for destroying information identified for destruction*

Appendix D

Trust Services Criteria for Security, Availability, and Confidentiality for Use as Control Criteria in the Cybersecurity Risk Management Examination

This appendix is nonauthoritative and is included for informational purposes only.

The trust services criteria for security, availability, and confidentiality and the related points of focus in this appendix have been extracted from TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*), issued in April 2017 by the AICPA's Assurance Services Executive Committee. The complete text may be found at www.aicpa.org/cybersecurityriskmanagement.

The following table presents the trust services criteria and the related points of focus for security, availability, and confidentiality, which are applicable to a cybersecurity risk management examination. In the table, criteria and related points of focus that come directly from the Committee of Sponsoring Organizations of the Treadway Commission's (COSO's) 2013 *Internal Control—Integrated Framework* (COSO framework)[1] are presented using a normal font. In contrast, criteria and points of focus that apply to engagements using the trust services criteria are presented in *italics*.

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	CONTROL ENVIRONMENT
CC1.1	**COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Sets the Tone at the Top—The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.

(*continued*)

[1] ©2017, Committee of Sponsoring Organizations of the Treadway Commission (COSO). All rights reserved. Used by permission. See www.coso.org.

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• Establishes Standards of Conduct—The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.
	• Evaluates Adherence to Standards of Conduct—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.
	• Addresses Deviations in a Timely Manner—Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers Contractors and Vendor Employees in Demonstrating Its Commitment—Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.*
CC1.2	**COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Establishes Oversight Responsibilities—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
	• Applies Relevant Expertise—The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action.
	• Operates Independently—The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Supplements Board Expertise—The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, through the use of a subcommittee or consultants.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
CC1.3	**COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers All Structures of the Entity—Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.
	• Establishes Reporting Lines—Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.
	• Defines, Assigns, and Limits Authorities and Responsibilities—Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.
	Additional points of focus specifically related to all engagements using the trust services criteria:
	• *Addresses Specific Requirements When Defining Authorities and Responsibilities—Management and the board of directors consider requirements relevant to security, availability, processing integrity, confidentiality, and privacy when defining authorities and responsibilities.*
	• *Considers Interactions With External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities—Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.*
CC1.4	**COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Establishes Policies and Practices—Policies and practices reflect expectations of competence necessary to support the achievement of objectives.

(*continued*)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• Evaluates Competence and Addresses Shortcomings—The board of directors and management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings.
	• Attracts, Develops, and Retains Individuals—The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.
	• Plans and Prepares for Succession—Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers the Background of Individuals—The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.*
	• *Considers the Technical Competency of Individuals—The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.*
	• *Provides Training to Maintain Technical Competencies— The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.*
CC1.5	**COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Enforces Accountability Through Structures, Authorities, and Responsibilities—Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• Establishes Performance Measures, Incentives, and Rewards—Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.
	• Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance—Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.
	• Considers Excessive Pressures—Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.
	• Evaluates Performance and Rewards or Disciplines Individuals—Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and provide rewards or exercise disciplinary action, as appropriate.
	COMMUNICATION AND INFORMATION
CC2.1	**COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Identifies Information Requirements—A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.
	• Captures Internal and External Sources of Data—Information systems capture internal and external sources of data.
	• Processes Relevant Data Into Information—Information systems process and transform relevant data into information.
	• Maintains Quality Throughout Processing—Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.

(*continued*)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
CC2.2	**COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Communicates Internal Control Information—A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.
	• Communicates With the Board of Directors—Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.
	• Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.
	• Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the information.
	Additional points of focus specifically related to all engagements using the trust services criteria:
	• *Communicates Responsibilities—Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.*
	• *Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters—Entity personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints to personnel.*
	• *Communicates Objectives and Changes to Objectives —The entity communicates its objectives and changes to those objectives to personnel in a timely manner.*
	• *Communicates Information to Improve Security Knowledge and Awareness—The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
CC2.3	**COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Communicates to External Parties—Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.
	• Enables Inbound Communications—Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant information.
	• Communicates With the Board of Directors—Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.
	• Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.
	• Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.
	Additional point of focus that applies only to an engagement using the trust services criteria for confidentiality:
	• *Communicates Objectives Related to Confidentiality and Changes to Objectives— The entity communicates, to external users, vendors, business partners and others whose products and services are part of the system, objectives and changes to objectives related to confidentiality.*
	Additional point of focus that applies only to an engagement using the trust services criteria for privacy:
	• *Communicates Objectives Related to Privacy and Changes to Objectives—The entity communicates, to external users, vendors, business partners and others whose products and services are part of the system, objectives related to privacy and changes to those objectives.*

(*continued*)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	RISK ASSESSMENT
CC3.1	**COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	Operations Objectives • Reflects Management's Choices—Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.
	• Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.
	• Includes Operations and Financial Performance Goals—The organization reflects the desired level of operations and financial performance for the entity within operations objectives.
	• Forms a Basis for Committing of Resources—Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.
	External Financial Reporting Objectives • Complies With Applicable Accounting Standards—Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.
	• Considers Materiality—Management considers materiality in financial statement presentation.
	• Reflects Entity Activities—External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.
	External Nonfinancial Reporting Objectives • Complies With Externally Established Frameworks—Management establishes objectives consistent with laws and regulations or standards and frameworks of recognized external organizations.
	• Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.
	• Reflects Entity Activities—External reporting reflects the underlying transactions and events within a range of acceptable limits.

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	Internal Reporting Objectives • Reflects Management's Choices—Internal reporting provides management with accurate and complete information regarding management's choices and information needed in managing the entity.
	• Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.
	• Reflects Entity Activities—Internal reporting reflects the underlying transactions and events within a range of acceptable limits.
	Compliance Objectives • Reflects External Laws and Regulations—Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.
	• Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Establishes Sub-objectives to Support Objectives—Management identifies sub-objectives related to security, availability, processing integrity, confidentiality, and privacy to support the achievement of the entity's objectives related to reporting, operations, and compliance.*
CC3.2	**COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels—The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.
	• Analyzes Internal and External Factors—Risk identification considers both internal and external factors and their impact on the achievement of objectives.

(*continued*)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• Involves Appropriate Levels of Management—The entity puts into place effective risk assessment mechanisms that involve appropriate levels of management.
	• Estimates Significance of Risks Identified—Identified risks are analyzed through a process that includes estimating the potential significance of the risk.
	• Determines How to Respond to Risks—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.
	Additional points of focus specifically related to all engagements using the trust services criteria:
	• *Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities—The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.*
	• *Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties—The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.*
	• *Considers the Significance of the Risk—The entity's consideration of the potential significance of the identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.*
CC3.3	**COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers Various Types of Fraud—The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• Assesses Incentives and Pressures—The assessment of fraud risks considers incentives and pressures.
	• Assesses Opportunities—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts.
	• Assesses Attitudes and Rationalizations—The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate actions.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers the Risks Related to the Use of IT and Access to Information—The assessment of fraud risks includes consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information.*
CC3.4	**COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Assesses Changes in the External Environment—The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.
	• Assesses Changes in the Business Model—The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.
	• Assesses Changes in Leadership—The entity considers changes in management and respective attitudes and philosophies on the system of internal control.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Assesses Changes in Systems and Technology—The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.*
	• *Assesses Changes in Vendor and Business Partner Relationships—The risk identification process considers changes in vendor and business partner relationships.*

(*continued*)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	MONITORING ACTIVITIES
CC4.1	**COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.**
	The following points of focus highlight important characteristics relating to this criterion:
	Points of focus specified in the COSO framework:
	• Considers a Mix of Ongoing and Separate Evaluations—Management includes a balance of ongoing and separate evaluations.
	• Considers Rate of Change—Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.
	• Establishes Baseline Understanding—The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.
	• Uses Knowledgeable Personnel—Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.
	• Integrates With Business Processes—Ongoing evaluations are built into the business processes and adjust to changing conditions.
	• Adjusts Scope and Frequency—Management varies the scope and frequency of separate evaluations depending on risk.
	• Objectively Evaluates—Separate evaluations are performed periodically to provide objective feedback.
	Additional point of focus specifically related to all engagements using the trust services criteria:
	• *Considers Different Types of Ongoing and Separate Evaluations—Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.*
CC4.2	**COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.**

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Assesses Results—Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.
	• Communicates Deficiencies—Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.
	• Monitors Corrective Action—Management tracks whether deficiencies are remedied on a timely basis.
	CONTROL ACTIVITIES
CC5.1	**COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Integrates With Risk Assessment—Control activities help ensure that risk responses that address and mitigate risks are carried out.
	• Considers Entity-Specific Factors—Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.
	• Determines Relevant Business Processes—Management determines which relevant business processes require control activities.
	• Evaluates a Mix of Control Activity Types—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.
	• Considers at What Level Activities Are Applied—Management considers control activities at various levels in the entity.
	• Addresses Segregation of Duties—Management segregates incompatible duties, and where such segregation is not practical, management selects and develops alternative control activities.

(*continued*)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
CC5.2	**COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls—Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.
	• Establishes Relevant Technology Infrastructure Control Activities—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.
	• Establishes Relevant Security Management Process Controls Activities—Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.
	• Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.
CC5.3	**COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.**
	The following points of focus, specified in the COSO framework, highlight important characteristics relating to this criterion:
	• Establishes Policies and Procedures to Support Deployment of Management's Directives—Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.
	• Establishes Responsibility and Accountability for Executing Policies and Procedures—Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• Performs in a Timely Manner—Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.
	• Takes Corrective Action—Responsible personnel investigate and act on matters identified as a result of executing control activities.
	• Performs Using Competent Personnel—Competent personnel with sufficient authority perform control activities with diligence and continuing focus.
	• Reassesses Policies and Procedures—Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.
	Logical and Physical Access Controls
CC6.1	***The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Identifies and Manages the Inventory of Information Assets—The entity identifies, inventories, classifies, and manages information assets.*
	• *Restricts Logical Access—Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.*
	• *Identifies and Authenticates Users—Persons, infrastructure and software are identified and authenticated prior to accessing information assets, whether locally or remotely.*
	• *Considers Network Segmentation—Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.*
	• *Manages Points of Access—Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.*

(*continued*)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Restricts Access to Information Assets—Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules for information assets.*
	• *Manages Identification and Authentication—Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure and software.*
	• *Manages Credentials for Infrastructure and Software—New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.*
	• *Uses Encryption to Protect Data—The entity uses encryption to supplement other measures used to protect data-at-rest, when such protections are deemed appropriate based on assessed risk.*
	• *Protects Encryption Keys—Processes are in place to protect encryption keys during generation, storage, use, and destruction.*
CC6.2	***Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Controls Access Credentials to Protected Assets—Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.*
	• *Removes Access to Protected Assets When Appropriate—Processes are in place to remove credential access when an individual no longer requires such access.*
	• *Reviews Appropriateness of Access Credentials—The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
CC6.3	***The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Creates or Modifies Access to Protected Information Assets—Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.*
	• *Removes Access to Protected Information Assets—Processes are in place to remove access to protected information assets when an individual no longer requires access.*
	• *Uses Role-Based Access Controls—Role-based access control is utilized to support segregation of incompatible functions.*
CC6.4	***The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Creates or Modifies Physical Access—Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on authorization from the system's asset owner.*
	• *Removes Physical Access—Processes are in place to remove access to physical resources when an individual no longer requires access.*
	• *Reviews Physical Access—Processes are in place to periodically review physical access to ensure consistency with job responsibilities.*
CC6.5	***The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:

(*continued*)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Identifies Data and Software for Disposal—Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.*
	• *Removes Data and Software From Entity Control—Procedures are in place to remove data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.*
CC6.6	***The entity implements logical access security measures to protect against threats from sources outside its system boundaries.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restricts Access—The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.*
	• *Protects Identification and Authentication Credentials—Identification and authentication credentials are protected during transmission outside its system boundaries.*
	• *Requires Additional Authentication or Credentials—Additional authentication information or credentials are required when accessing the system from outside its boundaries.*
	• *Implements Boundary Protection Systems—Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.*
CC6.7	***The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restricts the Ability to Perform Transmission—Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement and removal of information.*
	• *Uses Encryption Technologies or Secure Communication Channels to Protect Data—Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Protects Removal Media—Encryption technologies and physical asset protections are used for removable media (such as USB drives and back-up tapes), as appropriate.*
	• *Protects Mobile Devices—Processes are in place to protect mobile devices (such as laptops, smart phones and tablets) that serve as information assets.*
CC6.8	***The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restricts Application and Software Installation—The ability to install applications and software is restricted to authorized individuals.*
	• *Detects Unauthorized Changes to Software and Configuration Parameters—Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.*
	• *Uses a Defined Change Control Process—A management-defined change control process is used for the implementation of software.*
	• *Uses Antivirus and Anti-Malware Software—Antivirus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware.*
	• *Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software—Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.*
	System Operations
CC7.1	***To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Uses Defined Configuration Standards—Management has defined configuration standards.*

(*continued*)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Monitors Infrastructure and Software—The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.*
	• *Implements Change-Detection Mechanisms—The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.*
	• *Detects Unknown or Unauthorized Components—Procedures are in place to detect the introduction of unknown or unauthorized components.*
	• *Conducts Vulnerability Scans—The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.*
CC7.2	***The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Implements Detection Policies, Procedures, and Tools—Detection policies and procedures are defined and implemented, and detection tools are implemented on infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.*
	• *Designs Detection Measures—Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.*
	• *Implements Filters to Analyze Anomalies—Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Monitors Detection Tools for Effective Operation—Management has implemented processes to monitor the effectiveness of detection tools.*
CC7.3	***The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Responds to Security Incidents—Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.*
	• *Communicates and Reviews Detected Security Events—Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.*
	• *Develops and Implements Procedures to Analyze Security Incidents—Procedures are in place to analyze security incidents and determine system impact.*
CC7.4	***The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Assigns Roles and Responsibilities—Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.*
	• *Contains Security Incidents—Procedures are in place to contain security incidents that actively threaten entity objectives.*
	• *Mitigates Ongoing Security Incidents—Procedures are in place to mitigate the effects of ongoing security incidents.*
	• *Ends Threats Posed by Security Incidents—Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.*
	• *Restores Operations—Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.*

(*continued*)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Develops and Implements Communication Protocols for Security Incidents—Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.*
	• *Obtains Understanding of Nature of Incident and Determines Containment Strategy—An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.*
	• *Remediates Identified Vulnerabilities—Identified vulnerabilities are remediated through the development and execution of remediation activities.*
	• *Communicates Remediation Activities—Remediation activities are documented and communicated in accordance with the incident response program.*
	• *Evaluates the Effectiveness of Incident Response—The design of incident response activities is evaluated for effectiveness on a periodic basis.*
	• *Periodically Evaluates Incidents—Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.*
CC7.5	***The entity identifies, develops, and implements activities to recover from identified security incidents.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Restores the Affected Environment—The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.*
	• *Communicates Information About the Event—Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and external).*
	• *Determines Root Cause of the Event—The root cause of the event is determined.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Implements Changes to Prevent and Detect Recurrences—Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.*
	• *Improves Response and Recovery Procedures—Lessons learned are analyzed, and the incident response plan and recovery procedures are improved.*
	• *Implements Incident Recovery Plan Testing—Incident recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.*
	Change Management
CC8.1	***The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Manages Changes Throughout the System Lifecycle—A process for managing system changes throughout the lifecycle of the system and its components (infrastructure, data, software and procedures) is used to support system availability and processing integrity.*
	• *Authorizes Changes—A process is in place to authorize system changes prior to development.*
	• *Designs and Develops Changes—A process is in place to design and develop system changes.*
	• *Documents Changes—A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.*
	• *Tracks System Changes—A process is in place to track system changes prior to implementation.*
	• *Configures Software—A process is in place to select and implement the configuration parameters used to control the functionality of software.*
	• *Tests System Changes—A process is in place to test system changes prior to implementation.*

(*continued*)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Approves System Changes—A process is in place to approve system changes prior to implementation.*
	• *Deploys System Changes—A process is in place to implement system changes.*
	• *Identifies and Evaluates System Changes—Objectives affected by system changes are identified, and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.*
	• *Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents—Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified, and the change process is initiated upon identification.*
	• *Creates Baseline Configuration of IT Technology—A baseline configuration of IT and control systems is created and maintained.*
	• *Provides for Changes Necessary in Emergency Situations —A process is in place for authorizing, designing, testing, approving and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent timeframe).*
	Additional points of focus that apply only in an engagement using the trust services criteria for confidentiality:
	• *Protects Confidential Information—The entity protects confidential information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to confidentiality.*
	Risk Mitigation
CC9.1	***The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Considers Mitigation of Risks of Business Disruption—Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the entity's objectives during response, mitigation, and recovery efforts.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Considers the Use of Insurance to Mitigate Financial Impact Risks—The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.*
CC9.2	***The entity assesses and manages risks associated with vendors and business partners.***
	The following points of focus, specifically related to all engagements using the trust services criteria, highlight important characteristics relating to this criterion:
	• *Establishes Requirements for Vendor and Business Partner Engagements—The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.*
	• *Assesses Vendor and Business Partner Risks—The entity assesses, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives.*
	• *Assigns Responsibility and Accountability for Managing Vendors and Business Partners—The entity assigns responsibility and accountability for the management of risks associated with vendors and business partners.*
	• *Establishes Communication Protocols for Vendors and Business Partners—The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.*
	• *Establishes Exception Handling Procedures From Vendors and Business Partners —The entity establishes exception handling procedures for service or product issues related to vendors and business partners.*
	• *Assesses Vendor and Business Partner Performance—The entity periodically assesses the performance of vendors and business partners.*
	• *Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments—The entity implements procedures for addressing issues identified with vendor and business partner relationships.*
	• *Implements Procedures for Terminating Vendor and Business Partner Relationships — The entity implements procedures for terminating vendor and business partner relationships.*

(*continued*)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	Additional points of focus that apply only to an engagement using the trust services criteria for confidentiality:
	• *Obtains Confidentiality Commitments from Vendors and Business Partners—The entity obtains confidentiality commitments that are consistent with the entity's confidentiality commitments and requirements from vendors and business partners who have access to confidential information.*
	• *Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's confidentiality commitments and requirements.*
	ADDITIONAL CRITERIA FOR AVAILABILITY
A1.1	***The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for availability, highlight important characteristics relating to this criterion:
	• *Measures Current Usage—The use of the system components is measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.*
	• *Forecasts Capacity—The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.*
	• *Makes Changes Based on Forecasts—The system change management process is initiated when forecasted usage exceeds capacity tolerances.*
A1.2	***The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services availability criteria, highlight important characteristics relating to this criterion:

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Identifies Environmental Threats—As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.*
	• *Designs Detection Measures—Detection measures are implemented to identify anomalies that could result from environmental threat events.*
	• *Implements and Maintains Environmental Protection Mechanisms— Management implements and maintains environmental protection mechanisms to prevent and mitigate against environmental events.*
	• *Implements Alerts to Analyze Anomalies—Management implements alerts that are communicated to personnel for analysis to identify environmental threat events.*
	• *Responds to Environmental Threat Events—Procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on a periodic basis. This includes automatic mitigation systems (for example, uninterruptable power system and generator back-up subsystem).*
	• *Communicates and Reviews Detected Environmental Threat Events—Detected environmental threat events are communicated to and reviewed by the individuals responsible for the management of the system, and actions are taken, if necessary.*
	• *Determines Data Requiring Backup—Data is evaluated to determine whether backup is required.*
	• *Performs Data Backup—Procedures are in place for backing up data, monitoring to detect back-up failures, and initiating corrective action when such failures occur.*
	• *Addresses Offsite Storage—Back-up data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environmental threat event affecting both sets of data is reduced to an appropriate level.*
	• *Implements Alternate Processing Infrastructure—Measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable.*

(*continued*)

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
A1.3	***The entity tests recovery plan procedures supporting system recovery to meet its objectives.***
	The following points of focus, which apply only to an engagement using the trust services criteria for availability, highlight important characteristics relating to this criterion:
	• *Implements Business Continuity Plan Testing—Business continuity plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.*
	• *Tests Integrity and Completeness of Back-Up Data—The integrity and completeness of back-up information is tested on a periodic basis.*
	ADDITIONAL CRITERIA FOR CONFIDENTIALITY
C1.1	***The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.***
	The following points of focus, which apply only to an engagement using the trust services criteria for confidentiality, highlight important characteristics relating to this criterion:
	• *Identifies Confidential information—Procedures are in place to identify and designate confidential information when it is received or created and to determine the period over which the confidential information is to be retained.*
	• *Protects Confidential Information From Destruction—Procedures are in place to protect confidential information from erasure or destruction during the specified retention period of the information.*
C1.2	***The entity disposes of confidential information to meet the entity's objectives related to confidentiality.***
	The following points of focus, which apply only to an engagement using the trust services criteria for confidentiality, highlight important characteristics relating to this criterion:
	• *Identifies Confidential Information for Destruction—Procedures are in place to identify confidential information requiring destruction when the end of the retention period is reached.*

TSP Ref. #	TRUST SERVICES CRITERIA AND POINTS OF FOCUS
	• *Destroys Confidential Information—Procedures are in place to erase or otherwise destroy confidential information that has been identified for destruction.*

Appendix E

Illustrative Management Assertion in the Cybersecurity Risk Management Examination

This illustration is nonauthoritative and is included for informational purposes only.

[*ABC Entity's Letterhead*]

Assertion of the Management of ABC Entity

Introduction

We have prepared the accompanying description of ABC Entity's cybersecurity risk management program titled [*insert title of management's description*] throughout the period [*date*] to [*date*] (description) based on the criteria for a description of an entity's cybersecurity risk management program identified in [*name of the description criteria, e.g., AICPA* Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program] (description criteria). An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented. We have established ABC Entity's cybersecurity objectives, which are presented on page ___ of the description. We have also identified the risks that would prevent those objectives from being achieved and have designed, implemented, and operated controls to address those risks.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in an entity's cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Assertion

We assert that the description throughout the period [*date*] to [*date*] is presented in accordance with the description criteria. We have performed an evaluation of the effectiveness of the controls within the cybersecurity risk management program throughout the period [*date*] to [*date*] using the [*name of the control criteria, e.g., the criteria for security, availability, and confidentiality set*

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy *(AICPA,* Trust Services Criteria*) or other suitable criteria*] (control criteria). Based on this evaluation, we assert that the controls were effective throughout the period [*date*] to [*date*] to achieve the entity's cybersecurity objectives based on the control criteria.

Appendix F-1

Illustrative Accountant's Report in the Cybersecurity Risk Management Examination

This illustration is nonauthoritative and is included for informational purposes only.

Independent Accountant's Report

To Management of ABC Entity:

Scope

We have examined the accompanying description of ABC Entity's cybersecurity risk management program titled [*insert title of management's description*] throughout the period [*date*] to [*date*] (description) based on the description criteria noted below. We have also examined the effectiveness of the controls within that program to achieve the entity's cybersecurity objectives based on the control criteria noted below.

The criteria used to prepare the description are [*name of the description criteria, e.g., AICPA* Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program] (description criteria); the criteria used to evaluate whether the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives are [*name of the control criteria, e.g., the criteria for security, availability, and confidentiality set forth in TSP section 100,* 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy *(AICPA,* Trust Services Criteria*) or other suitable criteria*] (control criteria).

An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that were not prevented.

Entity's Responsibilities

ABC Entity's management is responsible for the following:

- Establishing the entity's cybersecurity objectives, which are presented on page XX of the description
- Designing, implementing, and operating the cybersecurity risk management program, including the controls within that program, to achieve the entity's cybersecurity objectives
- Preparing the accompanying description of the entity's cybersecurity risk management program
- Providing an assertion about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether controls within the cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives

When preparing its assertion titled [*insert title of management's assertion*], ABC Entity management is responsible for (*a*) selecting, and identifying in its

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

assertion, the description criteria and the control criteria and (*b*) having a reasonable basis for its assertion about whether the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives by performing an assessment of the effectiveness of those controls based on the control criteria. The description of the entity's cybersecurity risk management program and management's assertion accompany this report.

Accountant's Responsibilities

Our responsibility is to express an opinion, based on our examination, about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls within the program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

Our examination included

- obtaining an understanding of the entity's cybersecurity objectives and its cybersecurity risk management program;
- assessing the risks that the description was not presented in accordance with the description criteria and that the controls within that program were not effective; and
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria and whether the controls were effective.

Our examination also included performing such other procedures as we considered necessary in the circumstances. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in a cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects,

- the description of ABC Entity's cybersecurity risk management program throughout the period [*date*] to [*date*] is presented in accordance with the description criteria and
- the controls within that program were effective throughout the period [*date*] to [*date*] to achieve the entity's cybersecurity objectives based on the control criteria.

[*Accountant's signature*]

[*Accountant's city and state*]

[*Date of the accountant's report*]

Appendix F-2

Illustrative Accountant's Report in a Cybersecurity Risk Management Examination that Addresses Only the Suitability of the Design of Controls Implemented Within the Entity's Cybersecurity Risk Management Program (Design-Only Report) as of a Point in Time

This illustration is nonauthoritative and is included for informational purposes only.

Independent Accountant's Report

To Management of ABC Entity:

Scope

We have examined the accompanying description of ABC Entity's cybersecurity risk management program titled [*insert title of management's description*] as of [*date*] (description) based on the description criteria noted below. We have also examined the suitability of the design of controls implemented within that program to achieve the entity's cybersecurity objectives based on the control criteria noted below.

The criteria used to evaluate the description are [*name of the description criteria*, *e.g., AICPA* Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program] (description criteria); the criteria used to evaluate the suitability of the design of the controls implemented within the entity's cybersecurity risk management program to achieve the entity's cybersecurity objectives are [*name of the control criteria, e.g., the criteria for security, availability, and confidentiality set forth in TSP section 100,* 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy *(AICPA,* Trust Services Criteria*) or other suitable criteria*] (control criteria).

An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that were not prevented.

Entity's Responsibilities

ABC Entity's management is responsible for the following:

- Establishing the entity's cybersecurity objectives, which are presented on page XX of the description
- Designing, implementing, and operating the cybersecurity risk management program, including the controls within that program, to achieve the entity's cybersecurity objectives

- Preparing the accompanying description of the entity's cybersecurity risk management program
- Providing an assertion about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether controls implemented within the cybersecurity risk management program were suitably designed to achieve the entity's cybersecurity objectives.

When preparing its assertion titled [*insert title of management's assertion*], ABC Entity management is responsible for (*a*) selecting, and identifying in its assertion, the description criteria and the control criteria and (*b*) having a reasonable basis for its assertion about whether the controls implemented within the entity's cybersecurity risk management program were suitably designed to achieve the entity's cybersecurity objectives by performing an assessment of the suitability of the design of those controls based on the control criteria. The description of the entity's cybersecurity risk management program and management's assertion accompany this report.

Accountant's Responsibilities

Our responsibility is to express an opinion, based on our examination, about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether the controls implemented within that program were suitably designed to achieve the entity's cybersecurity objectives based on the control criteria.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls implemented within the program were suitably designed to achieve the entity's cybersecurity objectives based on the control criteria.

Our examination included

- obtaining an understanding of the entity's cybersecurity objectives and its cybersecurity risk management program;
- assessing the risks that the description was not presented in accordance with the description criteria and that the controls implemented within that program were not suitability designed; and
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria and whether the controls implemented were suitably designed.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

We did not perform any procedures regarding the operating effectiveness of the controls and, accordingly, we do not express an opinion thereon.

We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management

program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in a cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects,

- the description of ABC Entity's cybersecurity risk management program as of [*date*] is presented in accordance with the description criteria and
- the controls implemented within that program were suitably designed to achieve the entity's cybersecurity objectives as of [*date*] based on the control criteria.

[*Accountant's signature*]

[*Accountant's city and state*]

[*Date of the accountant's report*]

Appendix G

Illustrative Cybersecurity Risk Management Report

This appendix is nonauthoritative and is included for informational purposes only.

Note:

Although the AICPA Guide Reporting on an Entity's Cybersecurity Risk Management Program and Controls describes the components of a cybersecurity risk management report and the information to be included therein, it does not mandate specific formats for most of the information to be presented. Entity management and the practitioner may organize and present the required information in a variety of formats.

The format of the illustrative cybersecurity risk management report presented in this nonauthoritative appendix is included for illustrative purposes only. The illustrative cybersecurity risk management report contains all the required components of such a report, including (*a*) management's assertion, (*b*) the accountant's report, and (*c*) the description of the entity's cybersecurity risk management program.

Report on XYZ Manufacturing's Description of its Cybersecurity Risk Management Program and the Effectiveness of Controls Within the Program Throughout the Period January 1, 20X1, to December 31, 20X1

CONTENTS

Section 1—Assertion of the Management of XYZ Manufacturing

Introduction

We have prepared the attached XYZ Manufacturing's Description of its Cybersecurity Risk Management Program throughout the period January 1, 20X1, to December 31, 20X1, (description) based on the criteria for a description of an entity's cybersecurity risk management program identified in the AICPA *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* (description criteria). An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented. We have established XYZ Manufacturing's cybersecurity objectives, which are presented on page XX of the description. We have also identified the risks that would prevent those objectives from being achieved and have designed, implemented, and operated controls to address those risks.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in an entity's cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Assertion

We assert that the description throughout the period January 1, 20X1, to December 31, 20X1, is presented in accordance with the description criteria. We have performed an evaluation of the effectiveness of the controls included within the cybersecurity risk management program throughout the period January 1, 20X1, to December 31, 20X1, using the criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) (control criteria). Based on this evaluation, we assert that the controls were effective throughout the period January 1, 20X1, to December 31, 20X1, to achieve the entity's cybersecurity objectives based on the control criteria.

Section 2—Independent Accountant 's Report

To Management of XYZ Manufacturing:

Scope

We have examined the accompanying XYZ Manufacturing's Description of its Cybersecurity Risk Management Program throughout the period January 1, 20X1, to December 31, 20X1, (description) based on the description criteria noted below. We have also examined the effectiveness of the controls within that program to achieve the entity's cybersecurity objectives based on the control criteria noted below.

The criteria used to prepare the description are the AICPA's *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* (description criteria); the criteria used to evaluate whether the

controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives are the criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) (control criteria).

An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that were not prevented.

Entity's Responsibilities

XYZ Manufacturing's management is responsible for the following:

- Establishing the entity's cybersecurity objectives, which are presented on page XX of the description.
- Designing, implementing, and operating the cybersecurity risk management program, including the controls within that program, to achieve the entity's cybersecurity objectives
- Preparing the accompanying description of the entity's cybersecurity risk management program
- Providing an assertion about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether controls within the cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives.

When preparing its assertion titled *Assertion of the Management of XYZ Manufacturing*, management is responsible for (*a*) selecting, and identifying in its assertion, the description criteria and the control criteria and (*b*) having a reasonable basis for its assertion about whether the controls within the entity's cybersecurity risk management program were effective to achieve the entity's cybersecurity objectives by performing an assessment of the effectiveness of those controls based on the control criteria. The description of the entity's cybersecurity risk management program and management's assertion accompany this report.

Accountant's Responsibilities

Our responsibility is to express an opinion, based on our examination, about whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether the controls within that program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls within the program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

Our examination included

- obtaining an understanding of the entity's cybersecurity objectives and its cybersecurity risk management program;
- assessing the risks that the description was not presented in accordance with the description criteria and that the controls within that program were not effective; and
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria and whether the controls were effective.

Our examination also included performing such other procedures as we considered necessary in the circumstances. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in a cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects,

- the description of XYZ Manufacturing's cybersecurity risk management program throughout the period January 1, 20X1, to December 31, 20X1, is presented in accordance with the description criteria and
- the controls within that program were effective throughout the period January 1, 20X1, to December 31, 20X1, to achieve the entity's cybersecurity objectives based on the control criteria.

Baker, Jones, and Eagle, CPAs

Athens, Georgia

March 1, 20X2

Section 3—XYZ Manufacturing's Description of its Cybersecurity Risk Management Program

Note to readers: *The following illustrative description of an entity's cybersecurity risk management program, which is based on the operations of a hypothetical company, illustrates how a company might prepare and present a description of its cybersecurity risk management program in accordance with the description criteria. The description criteria have been included within the presentation for illustrative purposes.*

Nature of Business and Operations

DC1: The nature of the entity's business and operations, including the principal products or services the entity sells or provides and the methods by which they are distributed

XYZ Manufacturing (XYZ or the Company) is a leading manufacturer, distributor, and retailer of reproduction consumer products and objects from various historical periods, with an emphasis on classical Greece, ancient Rome, and medieval Europe. The Company's products allow consumers to emulate a noncontemporary lifestyle in one or more facets of their lives. Merchandise is provided across a broad range of categories including kitchen and dining, furniture, bedding and bath, lighting solutions, and arts, crafts, and sewing. The Company operates through three key segments: manufacturing (30 percent of revenue), online retail (40 percent of revenue), and wholesale (30 percent of revenue).

XYZ's online retail and wholesale operations offer products manufactured by the Company and sourced under contract from other manufacturers. Online retail also offers products sourced from other wholesalers.

The Company serves its primary markets of North America and Europe from its headquarters in Athens, Georgia, and Rome, Italy, respectively, and has major operating facilities throughout the U.S. and Europe. Manufacturing is located in Shanghai, China. In 2015, the Company entered into a joint venture with UVW Trading of Hong Kong to expand into Asian markets, where the Company's products hold strong appeal from a novelty perspective. Distribution is provided by commercial carriers.

Nature of Information at Risk

DC2: The principal types of sensitive information created, collected, transmitted, used, or stored by the entity

The Company creates, obtains, distributes, uses, and stores a wide variety of information in its operations. In addition to information common to the operation of entities similar to XYZ, such as regulatory compliance information and personnel records, the Company uses the following information:

- Financial information, which is used for both internal and external reporting purposes. Internal financial information and external financial information, prior to publication, is considered confidential and is treated as insider information.
- Confidential sales information, including customer lists, confidential wholesale pricing information, and order information
- Payment card information used in online retail and wholesale transactions, including cardholder names and card numbers. This

information may be retained for customer convenience on XYZ systems for ease of ordering

- Online retail customer profile information used to provide customers with a personalized lifestyle experience
- Confidential product information including product specifications, new design ideas, and branding strategies
- Proprietary information provided by business partners, including manufacturing data, sales and pricing information, and licensed designs
- Confidential employee information

Cybersecurity Risk Management Program Objectives (Cybersecurity Objectives)

DC3: The entity's principal cybersecurity risk management program objectives (cybersecurity objectives) related to availability, confidentiality, integrity of data, and integrity of processing

Under the direction of the XYZ board of directors, management establishes the objectives of the Company. Based on these objectives, management also establishes specific objectives for its cybersecurity risk management program. Because substantially all Company operations involve the use of IT, the Company makes no distinction between information security and cybersecurity.

XYZ Manufacturing's cybersecurity objectives are the following:

Availability

Enabling timely, reliable, and continuous access to and use of information and systems to support operations and to

- provide
  - — online retail store availability 24-hours a day year-round
  - — customer experiences related to system response and dropped transactions meeting benchmarks established by management
  - — manufacturing system availability during scheduled shifts
  - — timely information from the enterprise resource planning (ERP) system to suppliers and management to support decision making
  - — wholesale online, field sales support, and customer service center systems availability as committed
  - — accurate product availability and delivery information
- support the delivery of products to customers as committed
- comply with applicable laws and regulations
- safeguard assets

Confidentiality

Protecting information from unauthorized access and disclosure, including means for protecting proprietary information and personal information subject to privacy requirements, to safeguard

- employee and customer information, including credit card information, in accordance with laws, regulations, and card brand requirements
- confidential corporate data related to sales and financial reporting
- confidential business transactions related to the information of business partners and others
- the intellectual property of the Company, its business partners, and others

Integrity of Data

Guarding against improper capture, modification or destruction of information to support

- the preparation of reliable
  - — financial and nonfinancial information for external reporting purposes
  - — information for internal use
- nonrepudiation and authenticity of transactions from online systems
- the completeness, accuracy, and timeliness of manufacturing, delivery of goods, and information processing
- management, in holding employees, vendor and business partner employees, and customers accountable for their actions
- the storage, processing, and disclosure of information, including personal and third-party information

Integrity of Processing

Guarding against improper use, modification, or destruction of systems in order to support

- the accuracy, completeness, and reliability of product delivery and transaction processing
- the manufacture of goods to product specifications
- the efficient operation of production
- the safeguarding of the life and health of employees in production facilities

Guarding against the improper use or misuse of processing capabilities that that could be used to impair the security or operations of external parties

DC4: The process for establishing, maintaining, and approving cybersecurity objectives to support the achievement of the entity's objectives

The Company's board of directors, with the support of management and outside resources engaged by the board, reviews and updates its formal business strategy annually. Based on that strategy, management and the board annually establish or update the Company's overall business objectives, including objectives over operations, compliance, and reporting. At the completion of this process, the overall objectives are approved.

Upon approval of the Company's business strategy and overall objectives, management uses a top-down approach to establish or update specific business objectives for business units and functions, including information technology, within the organization. This process includes budgeting resources and establishing metrics for the achievement of the objectives. At the completion of this process, the specific business objectives and the budget is submitted to the board for approval.

As part of the development of specific business objectives, the chief information security officer (CISO) updates the Company's cybersecurity objectives with the objectives of the business units and other functional areas. These cybersecurity objectives are then approved by the Company's executive management, including the CEO, COO, CFO, chief risk officer (CRO), general counsel (GC), and the CIO.

The Company's cybersecurity risk management program is based on specifications set forth in the National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity" (NIST cybersecurity framework) and International Standardization Organization and International Electrotechnical Commission (ISO/IEC) standards. The Company's portfolio of security controls is based on ISO/IEC controls and, for systems containing cardholder information, the Payment Card Industry Data Security Standards.

Factors that have a Significant Effect on Inherent Cybersecurity Risks

DC5: Factors that have a significant effect on the entity's inherent cybersecurity risks, including the (1) characteristics of technologies, connection types, use of service providers, and delivery channels used by the entity; (2) organizational and user characteristics; and (3) environmental, technological, organizational and other changes during the period covered by the description at the entity and its environment

Technologies, connection types, service providers, and delivery channels. The Company uses the following technologies, connection types, service providers, and delivery channels:

- An integrated ERP system is used to manage manufacturing, wholesale, and retail operations. The ERP system is interfaced with the manufacturing, wholesale, and online retail systems to provide an integrated IT environment.
- Online retail operations are supported by a software-as-a-service (SaaS) cloud provider. The integrated solution provided permits the Company to design and maintain its retail site in an effective and efficient manner. Online wholesale operations are supported through a third-party system that interfaces with the ERP

system. The system is hosted on a network of virtual servers hosted in XYZ's primary data center.

- Wholesale call center services are outsourced with the call center's systems interfaced with the ERP system to facilitate ordering and problem resolution. The interface with the call center is over a virtual network connection. Custom-developed software is used to interface the call center system to the ERP interface.
- Field sales automation is provided through the use of company-owned tablet devices running third-party software customized for the Company. Tablets access the ERP system through a virtual private network (VPN) system.
- Manufacturing is controlled through a network of midrange systems running widely used manufacturing system software. This software is modified and maintained by Company IT personnel.
- All connectivity to external users occurs through defined access points managed by routers.
- Routers are also used to segment the network within the Company.
- Transmissions to vendors and other third parties are sent through defined channels.

Organizational and user characteristics. The Company's IT function is headed by a chief information officer (CIO) and is divided into application services, technology services, and information security. The Company uses a centralized organizational model to support company applications and technology. The online retail and call center vendor relationships are managed by designated personnel in technology services reporting to the chief technology officer (CTO). The information security group is headed by the CISO and consists of security architecture and technical support, application security, and security operations center personnel. Security operations center personnel are primarily responsible for user administration, second-level security support, security event monitoring, and security incident response and management.

Users of the system primarily consist of the following:

- Consumers whose access is restricted to the online retail system provided by the vendor.
- Wholesale customers whose employees have access to catalog information, order status, order functionality, and account functionality through the internet module of the wholesale system. Customer personnel are assigned user IDs via a master customer account that is also used to administer the accounts. Customer personnel accounts are assigned defined roles established by the Company.
- UVW personnel whose access is similar to wholesale customer access.
- Call center service organization personnel, who access the wholesale system through assigned user accounts that are restricted to a defined call center role.
- All XYZ employees, who are assigned unique user IDs that grant them default company access and email access, with the exception

of manufacturing line personnel in Shanghai who are not granted access.

- Product vendors, who are granted limited access to the ERP system to pick up purchase orders and inquire about the status of invoices. This access is provided through a module of the ERP system through a vendor account and password.

Although IT assets are located in all countries of operation, the Company does not deem any countries to be of higher risk than others.

Environmental, technological, organizational, and other changes during the period. In December of 20XX, the Company added manufacturing operations in Shanghai, China, through the acquisition of an established brass foundry. At the time of acquisition, the foundry ran its business operations using off-the-shelf software on a local area network. The Company completed migration of all foundry data processes to the ERP system in March of the current year.

The Company is in the process of finishing its new manufacturing facility and upgrading manufacturing and foundry equipment as part of a modernization program. As part of this program, it is modernizing foundry floor equipment, replacing existing manual equipment with new equipment that uses leading industrial control systems. These systems will be integrated with the ERP system to enhance production operations and reporting. The new facility is expected to be operational by November. The process for adding new system components related to this change is subject to the cybersecurity risk management program and controls over those components are implemented as part of the change management process.

DC6: For security incidents that (1) were identified during the 12-month period preceding the period end date of management's description and (2) resulted in a significant impairment of the entity's achievement of its cybersecurity objectives, disclosure of the following: (a) nature of the incident; (b) timing surrounding the incident; and (c) extent (or effect) of these incidents and their disposition

XYZ utilizes a number of both manual and automated security monitoring capabilities to identify security events that occur in the environment. During the period under assessment, the Company experienced an incident that resulted in a compromise of sensitive data from a SQL injection attach on a web application. The attack was detected approximately 66 hours after the event and was remediated within 5 days of detection. XYZ Manufacturing incurred costs related to the notification of and credit monitoring for affected parties (commercial customer information and personally identifiable information of retail customers), as well as fees associated with the retention of outside cybersecurity expertise to conduct forensic investigation of the affected systems and, later, an independent evaluation of security measures to ensure that remediation actions were sufficient to address the identified threats. The incident was fully resolved and remediated, and XYZ has made the necessary adjustments to its systems and processes, as well as to the affected service provider systems and processes, to reduce the likelihood that similar incidents could reoccur.

Cybersecurity Risk Governance Structure

DC7: The process for establishing, maintaining, and communicating integrity and ethical values to support the functioning of the cybersecurity risk management program

Management sets the organizational tone through policies, a code of ethics, a commitment to hiring competent employees, and the development of reward structures that promote an effective internal control and governance structure. The board of directors meets quarterly with members of executive management to review financial and operational performance, including the entity's cybersecurity risk management program.

Employees are required to sign the employee handbook upon hire, acknowledging their acceptance and adherence to the Company's policies and code of conduct. Such policies and the code of conduct have been designed to promote integrity and ethical values throughout the workplace. The information security policy includes information about the following:

- Information privacy, confidentiality, and acceptable use
- Electronic communications
- Data management
- Disclosure

DC8: The process for board oversight of the entity's cybersecurity risk management program

The XYZ board of directors includes various outside directors with industry knowledge and experience including one board member who is a former IT director of an S&P 100 company with 15 plus years of experience in IT and cybersecurity and serves as the board's subject matter expert on cybersecurity matters. Additionally, the XYZ CISO joins the quarterly board meeting to present an overview of the Company's cybersecurity risk management program, including activities of the entity's risk governance committee. Feedback and action items are provided by the board, which is actively engaged in overseeing this key business risk.

The risk governance committee was established to coordinate the risk assessment and management efforts of the entity and its units. The committee, which is chaired by the CRO and consists of the CISO, CCO, external specialists, and IT and business line personnel, ensures that (*a*) cybersecurity risks arising from both internal and external sources are identified and evaluated, (*b*) controls are properly designed and implemented to address all areas as appropriate, and (*c*) controls operate effectively to achieve the entity's cybersecurity objectives. Areas evaluated include systems development, computer operations, program changes, and access to programs and data.

As part of the CISO's quarterly presentations, the results of the XYZ information security team's program assessments are presented and discussed, as well as any corrective action needed as a result of the assessments. The presentations also include summaries of the Company's vendor and business partner oversight program. Under the program, Company personnel perform an annual review of vendor and business partner relationships to evaluate whether the Company is in compliance with industry standards and best practices.

DC9: Established cybersecurity accountability and reporting lines

Under the direction of the risk governance committee, the CISO is responsible for overseeing the cybersecurity risk management program and executing the entity's strategy and other decisions agreed upon by executive management and the board of directors. The CISO reports administratively to the CIO, with an escalation point to the CEO. The CISO presents a quarterly cybersecurity update to the board of directors to report on the state of the entity's cybersecurity risk management program.

The CISO also chairs the information security committee. The information security team, which consists of representatives from all departments in XYZ, is a centralized team of cybersecurity practitioners, subject matter experts, and IT personnel who support the information security operations of the organization (such as systems administrators, software engineers, network engineers, and security analysts). The duties, responsibilities, and hierarchy of employees on the information security team are defined in a role matrix and form the foundation of the entity's cybersecurity risk management program. The information security committee defines and approves the strategy, policies, and standards underlying the entity's cybersecurity risk management program. The results of the annual risk assessment, periodic internal audits, and quarterly external independent assessments are provided to the CISO and the information security committee throughout the year in order to continuously adapt the program to align with new and emerging threats and potential vulnerabilities. The activities of the information security committee are overseen by the risk governance committee.

Alongside the CISO is the CTO, who also reports administratively to the CIO but with an escalation point to the CEO. The CTO is responsible for managing the technology and resources that support the internal operations of the company. This includes overseeing policy and processes regarding relationships with vendors and business partners that may contribute to the cybersecurity risk management program. These policies and processes are administered through the vendor and business partner oversight program discussed in a later section.

DC10: The process used to hire and develop competent individuals and contractors and to hold those individuals accountable for their cybersecurity responsibilities

Applicants with a role in the cybersecurity risk management program are hired based on their ability to satisfy the job duties and responsibilities of the position and fulfill the goals and expectations of the entity. They are evaluated on their level of education, the merits of their past experience, a positive performance history, and knowledge of relevant cybersecurity controls and processes. Before employment, all applicants must also pass a thorough background check.

Upon hiring, employees are required to sign the employee handbook, acknowledging their acceptance and adherence to the Company's policies and any associated confidentiality and nondisclosure agreements.

Upon hiring and annually thereafter, all employees must successfully complete training courses covering basic information security practices that support the functioning of an effective cybersecurity risk management program. Employees with job responsibilities that fall directly within the cybersecurity risk management program (such as IT personnel, IT management, and internal auditors) have minimum training and continuing education requirements each year.

Employees in the cybersecurity risk management program are encouraged to maintain an active role in relevant cybersecurity information sharing forums, special interest groups, and professional associations to stay up to date on new and emerging cybersecurity risks that may impact the entity or its operating environment.

Contractors are required to follow the same onboarding process as employees and are subject to the same background checks and security awareness training requirements as employees. Employees' and contractors' compliance with security awareness training requirements is monitored on a semiannual basis by human resources.

XYZ has established an entity-wide hierarchy and reporting structure that is codified within an organizational chart maintained on the corporate intranet by human resources. XYZ has prepared a role matrix for employees and managers who have roles within the cybersecurity risk management program. The role matrix defines key job duties and responsibilities in the context of the overall program. Additional information security responsibilities and practices for certain roles within the entity are described in the Company's information security policy and the employee handbook.

All employees go through an annual performance review cycle. At the beginning of each calendar year, employees and their immediate supervisors establish goals and expectations for their job performance over the upcoming year based on the job duties and responsibilities described in the role matrix. Employees then receive a mid-year and year-end performance review from their supervisors that assesses the employees' performance against the agreed-upon goals and expectations. Based on the results of their performance review, employees receive merit increases in compensation and are eligible for bonuses and promotion, respective of their seniority, experience, and position within the organization.

Employees whose performance is not in alignment with established goals and expectations for job performance, or who are not fulfilling their job responsibilities, may be referred to human resources by their supervisor to develop a performance enhancement plan.

If an employee violates any statute of the employee handbook or the Company's policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the Company, whether purposefully or not, the employee is subject to sanctions up to and including termination of employment.

Cybersecurity Risk Assessment Process

DC11: The process for (1) identifying cybersecurity risks and environmental, technological, organizational and other changes that could have a significant effect on the entity's cybersecurity risk management program and (2) assessing the related risks to the achievement of the entity's cybersecurity objectives

XYZ maintains a detailed inventory of all information systems, including manufacturing and industrial control systems. All such assets are assigned ownership by a designated department or team within the entity and prioritized based on the asset's business value and criticality to the organization. Information and data assets are subject to the data management policy that defines parameters for the ownership, classification, security, storage, and retention of data. Software and hardware assets are subject to the information systems

management policy that defines parameters for the acquisition, development, maintenance, security and disposal of information system assets.

On an annual basis, the information security team performs a risk assessment that identifies internal and external cyber threats and vulnerabilities to the organization. Information system assets are analyzed to identify associated threats to those assets and vulnerabilities that may be exploited. The resulting risks are then scored based on their likelihood and potential impact to the organization. The assessment includes consideration of the inherent and residual risks that may reside with external parties and the cybersecurity controls to address those risks. Specific policies and procedures are in place to assess and manage the requisition and engagement of vendors or business partners with consideration for the cyber threats and vulnerabilities such relationships may present.

Results of the risk assessment are evaluated by relevant management against criteria for risk acceptance to identify new or existing protective measures and develop or enhance information security policies and procedures.

Internal audit conducts periodic cybersecurity assessments that include working with process owners and IT support personnel to identify specific security threats and vulnerabilities and to identify how the associated risks are being addressed. Additionally, quarterly vulnerability assessments and penetration tests are performed by an external party to identify specific technical threats and vulnerabilities.

DC12: The process for identifying, assessing, and managing the risks associated with vendors and business partners

XYZ considers the inherent risk of working with vendors and business partners as part of the annual risk assessment performed by the information security team. Internal and external cyber threats and vulnerabilities are identified and assessed based on the likelihood that they could prevent the entity from achieving its cybersecurity objectives. Specific policies and procedures are in place to assess and manage the requisition and engagement of vendors. Consideration is given to the cyber threats and vulnerabilities such relationships may present and whether XYZ's controls reduce such risks to a level consistent with XYZ's cybersecurity objectives and risk acceptance.

XYZ has established a tiering system in which each vendor is assigned a tier (1–3) based upon the inherent risk of the goods and services the vendor provides, the overall operational significance of the vendor to achieving XYZ's business objectives, and the sensitivity of data that resides within the vendor's environment. Business partners are evaluated using the same tiering structure, based on the cybersecurity risk associated with each business partner.

The entity's vendor and business partner oversight program requires that all contracts with vendors or business partners clearly address (*a*) the size, scope, and nature of services being provided; (*b*) the hardware, software, and information requirements related to the provision of such services; (*c*) the responsibilities of each party; (*d*) the requirements for information security to meet XYZ's standards; (*e*) the ability to perform independent audits of the effectiveness of internal control processes; and (*f*) the requirement to obtain and review a third-party attestation report.

Disclosure of any confidential or personally identifiable information (PII) to a vendor or business partner is provided only on an as-needed basis and only if

the vendor or business partner has enacted appropriate information security and privacy controls. All vendors and business partners with access to confidential information are subject to confidentiality and privacy agreements and other contractual confidentiality provisions, which must be signed and acknowledged before access to XYZ's systems and data is granted.

The vendor and business partner oversight team ensures that XYZ and its vendors and business partners stay current with existing contractual obligations, information security and privacy regulations, certification compliance requirements, and industry standards. The vendor and business partner oversight team performs an ongoing annual review of vendor and business partner relationships to (*a*) reevaluate the services provided and any cybersecurity threats and vulnerabilities arising from the relationship; (*b*) consider whether the assessed risks are being addressed appropriately by each party's contractual agreements, information security controls and processes; and (*c*) evaluate whether the entity's vendor and business partner oversight program complies with industry standards and best practices. The review process includes obtaining security questionnaires, conducting personnel interviews, performing walkthroughs, performing site visits, and conducting IT scanning and testing. In addition, when available, the review process may also include obtaining and reviewing third-party attestation reports.

The CISO and the information security team participate in cybersecurity information sharing forums, special interest groups, and professional associations to increase information sharing between knowledgeable parties and to stay up to date on changes in the regulatory, economic, and physical environment in which the Company operates. As an international manufacturer, XYZ Manufacturing maintains communicative relationships with relevant governing and regulatory bodies to stay abreast of changes to laws and regulations that impact the organization as they arise.

Internally, consideration of the entity's cybersecurity risk management program is an integral part of proposed changes to existing business lines or operations, the development or acquisition of new business lines or operations, decisions about doing business in new geographies or markets, and the adoption of new technologies or processes throughout the business. The information security team, led by the CISO, is involved in the decision-making process related to changes that could impact the size, scope, or operational nature of the business. In this capacity, the team may perform ad hoc, focused risk assessments to identify new risks to the organization and associated impacts to be considered during the decision-making process; the team may also reevaluate the design of controls to ensure continued protection.

Additionally, on an annual basis, the information security team performs a full risk assessment that identifies internal and external cyber threats and vulnerabilities to the organization. During the annual risk assessment, the team considers both internal changes to XYZ operational processes (such as new or modified lines of business, new or modified operating procedures, new geographies or markets, new technologies or services used) and external changes (such as new or changing regulatory requirements, industry standards, economic circumstances, emerging risks) that could affect the entity. New controls are designed in response to identified threats and existing controls are assessed to ensure they reflect changes to the size, scope, and operational nature of the business.

Cybersecurity Communications and Quality of Cybersecurity Information

DC13: The process for internally communicating relevant cybersecurity information necessary to support the functioning of the entity's cybersecurity risk management program, including (1) objectives and responsibilities for cybersecurity and (2) thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both

The internal communication of cybersecurity information for employees according to their role in the cybersecurity risk management program is described in the XYZ information security policy, which is available to all employees on the Company intranet. Additionally, the employee handbook identifies certain information security responsibilities and practices, depending on the employee's role within the organization. At the time of hiring, all employees must provide sign-off, acknowledging acceptance of and adherence to the Company's policies.

Upon hiring, and annually thereafter, all employees must successfully complete training courses covering basic information security practices that support the functioning of an effective cybersecurity risk management program. The training courses are designed to assist employees in identifying and responding to social engineering attacks (phishing, tailgating) and in avoiding inappropriate security practices (for example, writing down passwords or leaving sensitive material unattended). XYZ periodically assesses employees' awareness of corporate policy by attempting to tailgate into buildings, sending simulated phishing emails, and performing desk sweeps, among other tactics. If an employee is found to be violating Company policies, additional training is provided or other disciplinary actions are taken.

Employees with job responsibilities that fall directly within the cybersecurity risk management program (IT personnel, IT management, internal audit, and the like) have additional requirements to complete technical and job-specific training throughout the year. Additionally, those employees who have direct access to customer and employee data (for example, sales, customer service, human resources, IT helpdesk, and finance) will receive specific training around incident management, information handling, and data protection.

Training and other programs related to employee cybersecurity awareness incorporate materials developed internally by XYZ in collaboration with industry- and cybersecurity-focused vendors or business partners. These vendors or business partners provide expertise and tools to develop, perform, track, and test employees' compliance with cybersecurity-awareness policies and standards.

XYZ has established a cybersecurity awareness program (CAP) that periodically distributes reminders of information security practices to all employees and sends internal communications to promote security awareness and to provide the latest security news. CAP is also responsible for (*a*) monitoring cybersecurity risk associated with vendors and business partners who have access to the entity's system; (*b*) monitoring forums and news sites for information regarding potential breaches; (*c*) reviewing vendors' and business partners' cybersecurity examination reports on an annual basis; and (*d*) maintaining ongoing, direct contact with vendors and business partners to address any issues identified.

On an annual basis, XYZ updates the cybersecurity training program and CAP to incorporate changes in the threat landscape and new tactics being executed by threat actors. XYZ also evaluates lessons learned from any previous incidents and incorporates changes into the programs as necessary.

An incident hotline is available to all employees to report information security events they have been involved in or witnessed (such as phishing attacks, malware, lost or stolen devices, and inappropriate information disclosure). XYZ receives a quarterly attestation from the outsourced call center that all hotline personnel have completed XYZ's CAP and are aware of defined policies related to information protection, data handling, and incident response.

The CISO presents a quarterly update to the board of directors to report on the state of the entity's cybersecurity risk management program. During the update, the CISO presents the status of ongoing efforts to develop and maintain the program in response to (*a*) prior security events at the organization, (*b*) changes in XYZ's operational procedures, (*c*) changes to legal and regulatory requirements affecting the organization, (*d*) results of audits and testing by internal and external parties, and (*e*) new and emerging cybersecurity risks to the organization.

DC14: The process for communicating with external parties regarding matters affecting the functioning of the entity's cybersecurity risk management program

XYZ has a disclosure policy defining when, by whom, and to what extent external parties are informed of matters relevant to the functioning of XYZ's cybersecurity risk management program. All disclosures to external parties are made in accordance with applicable laws and regulations at the state and federal level. Any such legal requirements are considered in the development and maintenance of the disclosure policy during annual review. Employees are educated on the policies and procedures for reporting and disclosing cybersecurity incidents or events through the XYZ information security policy and XYZ Employee Handbook.

XYZ may become aware of matters affecting the functioning of the entity's cybersecurity risk management program via its existing monitoring processes, as well as via notification by third parties or law enforcement. When such matters arise, they are immediately reviewed by the XYZ risk governance committee to determine relevance and applicability. Where necessary or appropriate, the matter may be treated as a security incident and handled via XYZ's security incident response process, as described later.

As is typical business practice by most organizations, XYZ restricts communication of matters related to the functioning of XYZ's cybersecurity program to only those stakeholders and business partners who have a need to know such information. This information may be communicated via mediums appropriate to the nature of the information and the urgency of the situation, and may include conference calls, electronic mail, memoranda, or in-person meetings. In the rare instance when public disclosure of such matters would be necessary or appropriate, XYZ's legal counsel and corporate communications representative are responsible for jointly distributing and communicating such disclosure.

Monitoring of the Cybersecurity Risk Management Program

DC15: The process for conducting ongoing and periodic evaluations of the operating effectiveness of key control activities and other components of internal control related to cybersecurity

XYZ uses several mechanisms to assess the ongoing effectiveness of internal controls designed to mitigate cybersecurity risks. Assessment and monitoring of the program are designed to meet the requirements of the NIST cybersecurity framework and ISO 27001.

Internal audit conducts periodic cybersecurity assessments and tests of internal controls that include (*a*) working with process owners and IT support personnel to identify specific security threats and vulnerabilities and how the associated risk is being addressed and (*b*) tests of the design, implementation, and operating effectiveness of internal controls that address cybersecurity risks. Members of the internal audit team have the requisite knowledge of and experience with cybersecurity risks and controls.

XYZ also uses external parties to independently evaluate the state of the cybersecurity risk management program. Quarterly vulnerability assessments and annual penetration tests are performed by an external service provider to identify specific technical threats and vulnerabilities and to benchmark the environment against leading cybersecurity practices. In addition, the entity obtains for its SaaS vendor an annual web application security assessment report. Every two years, XYZ engages a service provider to perform an independent assessment of the cybersecurity risk management program to evaluate alignment with leading industry practices and consistency with Company policies in order to identify gaps and potential opportunities for improvement.

Both internal and external evaluations are made using a risk-based approach that may vary the nature, timing, and extent of testing. The criteria for such evaluations, including the nature and frequency of such evaluations, are reviewed during the annual risk assessment and modified as needed, with consideration for changes to XYZ's operational processes, including changes to the size, scope, and operational nature of the business, recent security threats or incidents, new or emerging risks, and changes in industry standards.

DC16: The process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the board of directors, as appropriate

On a quarterly basis, the information security team performs a risk assessment update that identifies changes to internal and external cyber threats and vulnerabilities to the organization. Results are evaluated by the risk governance committee, to identify whether new protective measures or enhanced information security policies and procedures are needed. The risk governance committee is also tasked with monitoring vulnerabilities, allocating resources to address them, and reprioritizing remediation initiatives, as necessary. Key performance indicators related to average closure time have also been defined and are monitored by the committee on a monthly basis.

The results of all monitoring activities, regardless of source, are entered into a vulnerability tracking system for evaluation and identification of remediation activities that may be needed. Identified vulnerabilities are assessed with regard to the likelihood and magnitude of exploitation. All vulnerabilities evaluated are identified for remediation or additional monitoring. Responsibilities for corrective action plans are assigned and completion dates determined. The information security committee reviews the list of open vulnerabilities on a monthly basis to monitor progress toward resolution and to identify trends and responses. On a quarterly basis, the risk governance committee and executive management receive summary reports of vulnerability management activities.

In addition, the CISO presents cybersecurity risk management program results, including vulnerability management activities, to the board of directors during each of its regularly scheduled meetings.

Cybersecurity Control Activities

DC17: The process for developing a response to assessed risks, including the design and implementation of control processes

A risk governance committee was established by XYZ to coordinate the risk assessment and management efforts of the entity and its units. The committee, which is chaired by the CRO and consists of the CISO, CCO, external specialists, and IT and business line personnel, ensures that risks are evaluated and that controls are designed, implemented, and operated to address all areas, as appropriate, to detect, respond to, mitigate, and recover from security events based on the assessed risks. Areas for evaluation include systems development, computer operations, program changes, and access to programs and data. Implemented controls include preventive and detective controls, such as manual, automated, or IT-dependent controls based on the environment in which the entity operates; the nature and scope of the entity's operations and its specific characteristics.

Business processes are documented in standard operating manuals; however, the risk governance committee also has business operations liaisons in each business area that are responsible for the ownership and documentation of key risk areas for the business operations. In 2014, the risk governance committee enhanced their key risk considerations for business areas to include specific consideration of cybersecurity risks.

The risk governance committee business liaisons annually revisit the risk assessments and validate the existence of controls to mitigate identified risks. The controls are captured in the Company's controls repository (CR), which is an inventory of the operations, risks, and controls associated with each business area. The CR is used to conduct quarterly self-assessments of controls and also serves as an input into the Company's annual controls maturity assessment, which is conducted by internal audit and reported to the risk governance committee.

The Company contracts for insurance coverage, including business disruptions, for risks which cannot be cost effectively mitigated through other techniques.

DC18: A summary of the entity's IT infrastructure and its network architectural characteristics

XYZ employs both internally hosted and cloud-based applications to support its manufacturing, retail, and wholesale operations. Cloud-based applications are provided through an arrangement with ABC Cloud under a service contract whereby XYZ retains the responsibility for specific server configuration and operating system change management, and ABC Cloud provides server support and maintenance. Company applications run primarily on Unix family operating systems and use industry standard database management systems. The manufacturing system uses a proprietary midrange operating system supplied by a leading IT manufacturer. The application was developed in house using the integrated operating system database. Field sales application tablets use an industry standard operating system.

XYZ has segmented its ERP financial reporting systems from its externally facing retail, wholesale, and call center interfaces through the use of Cisco ASA

firewalls, which are configured, managed, and supported by XYZ IT personnel. The firewall configurations and rules follow standards created by XYZ IT management under the direction of the CISO. All connectivity to external users occurs through defined access points protected by a redundant firewall complex. Firewalls are also used to segment the network within the Company.

Wholesale call center services are outsourced, with the call center's systems interfaced with the ERP system to facilitate ordering and problem resolution. The interface with the call center is over a virtual network connection. Custom-developed software is used to interface the call center system to the ERP interface.

The call center service provider facilities are reviewed annually by XYZ through their previously defined vendor and business partner oversight program. These vendor and business partner assessments focus on areas specific to the security configurations of the hosted applications, as well as to the network architecture related to XYZ's interfaces to the vendors.

ABC Cloud's SaaS is also reviewed annually through XYZ's vendor and business partner oversight program; however, given the nature of the responsibilities defined within the cloud agreement, XYZ configures its server settings in line with XYZ's corporate standards. XYZ has defined a standard build for cloud-based server configurations and uses that as the baseline from which servers are configured to support the SaaS environment. Also, monitoring of the configurations for adherence and compliance with defined standards is conducted by XYZ IT support personnel, as well as through the corporate internal audit and risk management teams.

Field sales automation is provided through the use of Company-owned tablet devices running third-party software customized for the Company. Tablets access the ERP system through a cellular-based VPN system that uses two-factor, token-based authentication.

DC19: The key security policies and processes implemented and operated to address the entity's cybersecurity risks, including those addressing the following:

- **a.** ***Prevention of intentional and unintentional security events***
- **b.** ***Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents***
- **c.** ***Management of processing capacity to provide for continued operations during security, operational, and environmental events***
- **d.** ***Detection, mitigation, and recovery from environmental events and the use of backup procedures to support system availability***
- **e.** ***Identification of confidential information when received or created, determination of the retention period for that information, retention of the information for the specified period, and destruction of the information at the of the retention period***

XYZ has defined a set of information security standards and policies that are under the direction and ownership of the CIO and implemented through the

CISO. The standards and policies address the management and implementation of security controls, ranging from the physical security of facilities and equipment to the logical security at the data element layer. The information security policies and standards are designed to provide information to employees, contractors, and vendors that is aligned to their job or functional responsibilities, while also contemplating segregation of functions that may otherwise create a segregation of duties conflict.

Security policies are published on the Company's intranet, included in onboarding packages, and reiterated through annual training that all employees are required to take and acknowledge. Security policies related to relationships with vendors and business partners are enforced through contractual commitments and related service-level agreements (SLAs) and, where possible, are monitored for adherence through XYZ's vendor and business partner oversight program.

The key components of the XYZ information security policy are discussed in the following paragraphs.

Prevention of intentional and unintentional security events. The Company has the following processes in place to prevent intentional and unintentional security events:

Physical and Logical Access Provisioning, De-provisioning, and Transfers (Including Remote Access). XYZ employees are granted network access only after completing security-awareness training. Users are granted access to XYZ systems and data based on their job role. Access requests are approved by the user's manager prior to access being granted. Upon termination, human resources sends a notification through the ticketing system, which is routed to the user administration team to remove user account access for the terminated user. Human resources provides a weekly list of terminations, which is then cross-referenced against the user account list to identify any user accounts that have not been properly terminated. User accounts that are inactive for 60 days are automatically disabled. For access modifications, the user's manager is required to submit and approve an access request ticket via the ticketing system, which is routed to the user administration team for processing.

Authentication. Users are required to authenticate using a unique user ID and password before being granted access to the network. The network domain password policy is configured to include password minimum length, expiration intervals, complexity, history, and an invalid password account-lockout threshold. A new user's account password is set to pre-expire so that the password must be reset the first time a user logs in to the network.

Credentials Management. Access is granted based on role-based security profiles that provide segregation of duties and limit transaction access. XYZ application and data owners review access rights on a semiannual basis. On an annual basis, the roles and the transactions assigned to the roles must be reviewed.

Privileged User Management. Access to privileged user or superuser accounts is authorized by management. Users with privileged user accounts are provided with a standard (nonprivileged) user account for use on a daily basis (for email and personal productivity software), and are only permitted to use their superuser accounts when performing administrative tasks. All superuser account access is logged and monitored. On a quarterly basis, the user administration team performs an access review of privileged access.

Database Security. Database administrators are the only individuals that can access XYZ databases. All database access and activity are logged. Database account access is reviewed twice a year for continued appropriateness. Direct data changes require approval, which should be documented within the Company's ticketing system and handled via the change management process.

Data Loss Prevention (DLP). The Company has a DLP solution that monitors and provides alerts about (and can take action regarding) the transmission or removal of confidential data outside of the Company or on noncompany-owned devices. The DLP solution is configured to encrypt external storage devices and prevent the saving of sensitive data to removable media. Hard drives of all servers, workstations, and laptops are encrypted. XYZ Manufacturing and its vendors utilize transport layer security for encryption of transmissions across the Internet to XYZ web servers and the email system. A VPN requiring multifactor authentication is used for all remote access to XYZ's internal network, ensuring that data is encrypted in transit when sent across the Internet from a Company computer system. Site-to-site VPNs are also utilized with certain XYZ vendors to provide encrypted channels for communication between locations.

Data Destruction. Data that exceeds its retention period is removed from systems and all backup media. Data that is labeled as confidential is erased using secure deletion techniques approved by the U.S. government (multi-pass overwrite). All computer hard drives are required to be securely deleted before disposal, and a certificate of destruction is obtained from the third-party organization that disposes of all computer equipment for XYZ.

Data Backup. Nightly incremental backups of all production servers and daily backups of production databases are conducted. Every month end, the Company is required to perform a full backup of the production servers. Backup tapes are encrypted and sent to a third-party vendor for storage. An automated backup system is implemented to monitor the completion of scheduled backups. When a backup job is not completed successfully, operations personnel create an incident ticket and assign personnel to resolve the failure.

Virus Detection and Prevention. Antivirus software is required to be installed on all XYZ servers, desktops, laptops, and email infrastructure and is centrally managed to ensure timely delivery of signature updates. The antivirus software settings are preconfigured for automatic updates and locked to prevent any user tampering or disabling. Email filtering software is in place to restrict and reject emails that contain certain malicious file types, including executable files. The Company's antivirus administrator is required to perform a quarterly inventory reconciliation against a system inventory list.

Firewalls and Perimeter Security. XYZ Manufacturing deploys enterprise firewalls at the perimeter of the network and in other strategic locations throughout the network in an active failover configuration. Only a minimal number of ports and services are allowed into the XYZ environment. All firewalls are managed using a centralized console, and XYZ installs monitoring software on the firewalls to provide alerts when changes occur at the administrative level. Firewall rulesets are reviewed twice a year to ensure that they are appropriately configured.

Secure System Configuration. Configuration specifications are installed on all systems before they are implemented into production. Monthly vulnerability and configuration scans to validate that all systems remain configured in accordance with XYZ's security hardening standards are performed. When updates

to existing standards are made, the changes are implemented on production systems.

Intrusion Prevention. A threat intelligence database is regularly updated. Packets identified by the threat intelligence database that meet a certain risk threshold or exhibit certain characteristics are automatically dropped and prevented from entering the XYZ network.

Change Management. A change approval board (CAB) that consists of representation from all IT departments within XYZ is in place. On a weekly basis, the CAB meets to review upcoming system and application changes, which are requested via the Company's online ticketing software. All changes are required to have a documented back-out plan. All changes are required to have a documented test plan. All members of the CAB approve a change before it can be implemented. In the weekly CAB meeting, the previous week's changes are reviewed. A root cause analysis report is completed for any changes that did not go as planned before they can be reconsidered.

Application Changes. Change requestors submit a change request within the Company's ticketing system. An application analyst reviews the change request and develop a project change budget estimate. On a monthly basis, application change requests and associated budgets are reviewed and categorized by IT and the business owners and ranked according to priority. Development occurs in a development environment that is separate from the production environment, using test data. Once development is completed, user acceptance testing takes place. Once user acceptance testing is completed, the business owner who sponsored the change and the applicable application analyst are required to approve the change within the ticket. The IT operations team migrates changes into production after they have been approved by the CAB. Emergency changes are required to be documented and logged in the ticketing system after changes are completed, and the CAB conducts an after-action review to approve the changes retroactively.

Patch Management. When new patches are released, they are reviewed by a group of IT personnel, including a representative from the information security team. The team assigns a priority level to each patch. Patches that are assigned a rating of "critical" are applied to all affected systems within 7 days. Patches that are assigned a rating of "high" are applied to all affected systems within 30 days. Patches that are assigned a rating of "medium" are applied within 60 days. All other patches are applied in regular system updates that typically occur quarterly. Once assigned a patch criticality rating, a patch is assigned to the appropriate IT system administrator for evaluation and testing in the XYZ test lab. When testing is completed, a change ticket is entered in the ticketing system, and the patch is reviewed and approved by the CAB. Monthly, the information security team is required to conduct vulnerability scanning of all systems to ensure that patches are properly in place. Any missing patches are immediately ticketed and a resolution is required within 5 business days.

Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents. Due to the pervasive use of IT to conduct business operations and deliver products and services to customers, the ability to detect a security event in a timely manner is of significant importance. Accordingly, XYZ Manufacturing has defined formal key security policies and processes focused on identifying cybersecurity

issues to detect security events. These policies and processes are focused on the following:

- Utilizing continuous security monitoring tools and programs to assist in identifying anomalies within the network and supporting infrastructure environment—inclusive of security event information relevant to third-party vendors
- Implementing security monitoring processes and procedures and other measures to identify anomalies in information flow, access, data communications, and the operation of business-critical systems
- Analyzing anomalies to identify security events and to detect abnormal events or data movement using historical baseline or behavioral analytics data to determine what is considered to be abnormal
- Escalating identified security events that occur through the course of business operations and ongoing communications, both within and outside of the organization

Detection of Security Events. A dedicated security team is available 24/7. Administrative activity and supporting infrastructure components are monitored through manual analysis and automated alerts where risk-based security monitoring, or a triage approach, is performed based on inherent risk of the anomaly or security event detected and the potential impact that said event could have on the Company's business operating environment. Security monitoring procedures are documented and consistently followed; documentation updates are made to the relevant security monitoring procedures related documentation when required or when significant procedure-related changes are made. Regular security monitoring and detection-based reporting capabilities with metrics are mapped to business drivers for security monitoring purposes. Vendor-related and custom signatures are updated regularly based on threat intelligence information gathered for security-detection purposes. Centrally stored or monitored logs are maintained, and correlation and alerting capabilities are performed on a limited basis when unusual activity is suspected based on the information gathered from the security incident and event management (SIEM) system.

Development of a Response Plan. The incident response sections of the Cybersecurity Incident Response and Recovery Plan (CIRP) includes tactical procedures to help "triage," contain, monitor, or eradicate a security incident, including procedures to do the following:

- Respond to, recover from, and restore normal business operations in a timely manner with minimal, or no, business interruption or loss of data
- Continuously improve the cybersecurity risk management program to limit the likelihood and impact of future incidents based on lessons learned from the Company's own experiences and those of others
- Communicate with employees, stakeholders, regulators, and other constituents in a structured manner about the nature of the security incident, impact to the organization and others (if applicable), and the corrective action taken to recover

The incident response sections of the CIRP have been created based on a threat scenario risk assessment performed annually as part of the review of the plan. The plan is focused on responding to those threat scenarios that have the highest impact and likelihood of occurring based on the business and markets in which the Company operates and the current technology environment. The incident response sections of the CIRP include the following key information:

- Response plan owners (those who can activate the plan), team members, and contact information for plan owners and team members
- Defined criteria required to activate the response plan
- Target business and IT performance metrics for operating in a "business as usual" environment
- Linkage to the business impact analysis and critical path recovery items within the disaster recovery (DR) and business continuity (BC) plans
- Alternate internal and external communication and operating methods to use when primary methods are unavailable
- Communication plan for notifying internal stakeholders (including legal, human resources, marketing, and investor relations), retained service providers (external counsel, forensics investigators, and the like), and external stakeholders (such as customers, vendors, regulators, and law enforcement) to manage expectations and information disclosure as part of the overall response effort. The communication plan also includes communication templates for certain formal internal and external communications, including, but not limited to, internal IT outage notifications and public press releases
- Facility recovery procedures providing linkage to the DR and BC plans regarding the hosted hot site facility located in Syracuse, NY, and the alternate call center located in Troy, MI
- Data response procedures providing linkage to the backup policies and procedures, as well as the DR plan, regarding offsite data storage and backup media
- Hardware and software access procedures enabling IT service and operations during response and recovery procedures
- Response and recovery metrics focused on the target response and recovery milestones to enable effective management, measurement, and monitoring of recovery activities
- Detailed incident response and recovery procedures to be executed based on the identification of the root cause, including operational steps to eradicate any infections, malicious code, unauthorized user accounts, and the like, and restore systems in accordance with priority and dependencies

It should also be noted that mitigating processes and controls are evaluated as part of the current CIRP-related processes and controls in place to detect and respond to security incidents and events. (These mitigation process and control factors may be directly related to the CIRP or may be part of other security monitoring related controls.)

The CIRP is reviewed annually and approved by the following members of management:

- CISO
- CIO
- CTO
- CRO
- GC
- Chief Marketing and Communications Officer
- Director, Security Operations
- Director, Crisis and Response Management

Implementation Activities to Mitigate and Recover from Identified Security Incident. The plan activation process begins when one or more of the incident response and recovery plan owners are informed of a cybersecurity event for which incident response is imminent or underway. The plan owner will ensure details about the cybersecurity event are clearly understood and documented to the extent necessary to enable future communications. This includes the identification of security monitoring or other mitigating processes and control factors which may be present and reduce the overall impact of the identified security event. Should the plan owner decide to activate the plan, he or she will convene an emergency meeting of the CIRP leadership team (including the CIO, CISO, CRO, GC, VP of human resources, and CFO) to determine

- immediate tasks,
- departments and functions required to carry out the plan based on the cybersecurity event,
- the initial communication plan and the individual assigned to execute the plan.

Once agreement is made, the leadership team is responsible for notifying members of their teams and others, including external advisors (such as investor relations and external general counsel) about the plan activation, initial decisions made, and assigned actions.

Once activated, XYZ considers the current cybersecurity event and its effects on systems and business operations. The Company refers to the appropriate sections of the BC and DR plans, as well as the relevant and applicable data backup logs, to identify the following:

- Where the IT systems and IT infrastructure affected by the cybersecurity event reside within the asset prioritization hierarchy
- Where the business operations affected by the cybersecurity incident or event reside within the operations prioritization hierarchy
- The planned alternative IT systems (such as the failover or load-balanced servers and network devices) and business processing activities (for instance, manual sales order forms) for the effected components of the environment
- The time prior to the cybersecurity incident or event from when the Company will be able to respond to and recover from (recovery point objective [RPO]) for the affected IT systems and IT infrastructure

- The maximum length of time until IT systems, IT infrastructure, and business processes affected by the cybersecurity incident or event is returned to normal business operation, after which significant negative impact may occur (recovery time objective [RTO])

For each IT asset (hardware and software, including virtualized assets) affected by the cybersecurity event, an evaluation will be made to determine the appropriate response and recovery actions, such as the following:

- Decommission and replace
- Reconfigure with enhancements (firmware updates, vendor patches, configuration changes)
- Reconfigure with no enhancements

Recognizing that the Company may not be able to complete the chosen recovery action in a timely manner in relation to the RTO, an alternative solution will be determined to enable a return to normal processing.

Data restoration is based on the activities outlined in the backup and recovery policies and procedures. The backup procedures apply to the following:

- Network devices—such as configurations, access control lists, and firmware
- Physical and virtual servers (DNS servers, email servers, FTP servers, application servers, database servers, web servers)—operating systems, application programs, and application data
- Networked file shares
- End user computing (desktops, laptops, tablets, mobile devices) and peripherals (such as printers and copy machines)
- Telephone and voicemail systems

XYZ Manufacturing leverages a global backup management solution to manage the backup processing and monitoring of all IT assets connected to the environment. The backup solution is connected to a virtual storage area network (SAN) and supplemented by real-time disk imaging to an offsite facility for the highest-value IT assets and data. Moderate- and lower-value information and IT assets are backed up to electronic, removable media and stored at a secure offsite facility for the period of time defined by the backup and recovery policies and procedures. Backup method and frequency is based on the volume and frequency of information processing and the importance of the data or IT asset.

Restoration of data, software, and configurations is made using the global backup management solution. Prior to restoring data, software, and configurations to the live environment, the Company will conduct tests in the security sandbox against the backup media to determine if the cybersecurity event is present. Based on results, the Company may seek to leverage an older backup or execute the eradication techniques that were successfully employed in the production environment.

Communications related to a cybersecurity event are governed by the CIRP leadership team. Throughout recovery efforts, XYZ will communicate to the extent possible, and as required, with employees, stakeholders, regulators, or law enforcement through formal written and verbal communications (email, press releases, mass voicemail) that are structured to be informative, easy to understand, and transparent and that address the following:

- Current understanding of the cybersecurity incident or event
- The known impact of the cybersecurity incident or event
- The current status of remedial action being taken in response to the cybersecurity incident or event

Communications are tailored to specific audiences (all employees, individuals of whom specific action is required, public domain), leveraging templates that have previously been created and preapproved by appropriate members of executive management and external advisors.

Within ten business days of returning to "business as usual," the CIRP requires a formal meeting of the full cybersecurity incident response and recovery team. The purpose of the meeting (which may be held via teleconference, videoconference, or in person) is to discuss lessons learned from the event and additional actions required. Defined criteria are included within the CIRP to help determine the structure of the meeting, the documentation required, and the monitoring that will be performed to ensure any new correction action agreed upon or implemented since the occurrence of the cybersecurity incident or event continues to operate over a period of time. During the meeting, at a minimum, the following are discussed:

- Identified breakdown in processes or controls, if any
- Enhancements that may need to be made to the process for identifying security monitoring or other mitigating processes and control factors which may be present in the environment and reduce the overall impact of the identified security event, prior to plan activation
- Changes required to standard configurations and the status of changes to other comparable systems that have yet to be attacked (as well as confirmation that those systems have not been compromised)
- Changes to the CIRP or the response team that would benefit incident response or recovery capabilities
- Capital investments or additional operating expenses required to more effectively prevent or detect a similar cybersecurity incident or event
- Changes to business partner relationships that may enable better response or recovery actions to be taken for future cybersecurity incidents or events
- Changes to CIRP test scenarios

The meeting minutes from the discussion are documented and appended to the CIRP.

Once per quarter, as part of the crisis management and incident response readiness activities, formal tests of response and recovery procedures are performed. Tests are based on overall-business-based scenarios that have been developed to confirm awareness of and education about the CIRP and related plans (such as the DR and BC), as well as to hone plan content in an effort to continuously improve response and recovery capabilities.

Tests performed during three of the four quarters are "tabletop" exercises in conference rooms, leveraging tele- and videoconferencing as necessary to conduct a virtual simulation with the CIRP team and other stakeholders. Tests

performed during the other quarter involve a real-life simulation where a simulated cybersecurity incident or event is triggered. Only the CIRP leadership team is initially aware of the simulation. XYZ executes the response and recovery plan in a "real life" situation until the point when communication with internal and external stakeholders would be required. The Company then completes the simulation as if it were a real event. Test results produced from this simulated event are formally discussed; ongoing updates are made to the CIRP as deemed necessary.

Management of processing capacity to provide for continued operations during security, operational, and environmental events. Policies and processes are implemented to address capacity management and include the use of the Information Technology Infrastructure Library (ITIL) IT service management framework for capacity management. Performance management and capacity monitoring tools are used to real-time information to the network operations centers. Alert levels are established based on asset priority and failover capability for the load-balanced and redundant components. Alerts may be in the form of a yellow or red color indicator on the operator console within the network operations centers. The automatic creation of a problem ticket in the service management system for investigation and resolution, or an automated text and email to the on-call IT operations lead, is acceptable.

Detection, mitigation, and recovery from environmental events and the use of backup procedures to support system availability. Policies and processes are implemented to address the detection, mitigation and recovery from environmental threats. The primary computer facility houses key IT infrastructure for the Company's integrated ERP system and midrange platforms supporting manufacturing software. The facility has been specifically designed to mitigate the risk of environmental threats to the computer hardware operations and include protection from fire and the loss or fluctuation of power, cooling, and humidity.

Fire suppression systems, in combination with smoke detection and hand-held fire extinguishers, are installed throughout the Company's facilities. Preventive maintenance is performed annually along with required inspections. An uninterruptible power supply (UPS) system provides continuous conditioned power through its strings of batteries to all infrastructure hardware to control unanticipated power interruptions. Maintenance for the UPS and batteries is performed at least quarterly. Emergency generator systems are required to be installed within the secure perimeter of the data center facilities. They are sized to provide 100 percent of the data center's electrical service in the event of a utility service failure. These generators have scheduled maintenance performed at least quarterly. The temperature and humidity inside the data center is controlled by dedicated air conditioning systems for computer hardware. These units act independently of any general building air conditioning. Maintenance is performed at least tri-annually. The data center environment, temperature, humidity, power, and fire prevention systems are required to be monitored through a building management system within the command operations center. Operations personnel man the facility 24 hours a day, 7 days a week.

Physical Access. Access to the computer facility entrances and to the network operations centers (including the raised floor areas) is controlled by the badge access reader system. Building access points are required to be locked at all hours except for the main entrance, which can be unlocked during normal business hours and manned by a security guard. At each facility entrance, visitors

are required to provide relevant identification, such as name, representing company, and employee contact. All visitors receive a visitor badge and sign in on the visitor log. All personnel are required to display their badge at all times while in the facility. Visitors are escorted while in restricted-access areas of the facility; when leaving, they are required to sign out on the visitor log. Video cameras are monitored 24/7 and provide surveillance over the interior and exterior of the building. All camera activity is recorded on digital video and retained for at least 60 days.

Backup Media. Data and programs are backed up in accordance with defined schedules. The backup schedule, rotation schedule, and retention period of tapes at the offsite storage facility are determined based on business need. The offsite tape storage is located approximately 30 miles from the computer facility. Backup job failures are monitored and tracked to resolution through the incident management process. Monitoring tools established in the job scheduling and monitoring process are utilized to monitor backup jobs. Job monitoring tools are in place to automatically generate an incident ticket in the incident management system for backup failures. Tape management systems are used to manage tape activities in the data center. Features of these systems include onsite media inventory, offsite media inventory, picking list for the vault, distribution list for the vault, and scratch lists.

The tape management systems produce reports to facilitate tape movement between the tape racks and drives in the data center as well as between the data center and the offsite facility. Tape rotation is monitored. Reports are reconciled daily and discrepancies are evaluated and resolved. Periodic inventories of tapes located both onsite and at the offsite facility are required to be conducted. Backup media is periodically tested. Periodic testing of backup media is coordinated by the business continuity team and performed by the appropriate technology groups.

Alternate Processing. BC plans are in place for all major business units and updated on an annual basis. DR plans are in place to support BC plans covering the critical IT infrastructure and networking equipment. The DR plan is updated annually. The main data center is physically separated from business operating units and dedicated solely to processing functions. The DR plans are reviewed annually and tested at least once a year. During a testing exercise, locations that are part of the testing exercise access the DR location through VPNs to segregate the network and prevent interruption to production services.

All business units with RTOs of less than 72 hours participate in a DR exercise once every three years. Business units with RTOs of 48 hours or less participate in the recovery testing exercise on an annual basis. The results of the tests are documented and assembled into a problem and resolution log.

Identification of confidential information when received or created, determination of the retention period for that information, retention of the information for the specified period, and destruction of the information at the of the retention period. Policies and processes are implemented to address capacity management and include the following:

Data Classification and Retention. The data classification and retention policy and relevant security and confidentiality policies describe how information is designated as confidential and ceases to be confidential. The handling, destruction, maintenance, storage, backup, and distribution and transmission of confidential information are documented in the data classification and

retention policy, XYZ's general business terms, and in some cases, in customer and business partner-specific contracts and service-level agreements.

Confidential policies and processes have been implemented to limit access to logical input routines and physical input media to authorized individuals. Each type of confidential information is classified, handled, secured, retained, and disposed of. All nonpublic customer information is confidential. Data that carries a confidential classification is subject to the Company's information security policy, which defines protection requirements, access rights, and access restrictions, as well as retention and destruction requirements. Customer, vendor, and business partner information is presumed to be confidential (as a default) unless obviously not.

As part of their standard process for establishing service levels and operational protocols with vendors or business partners such as ABC Cloud and UVW Trading, XYZ will evaluate data shared between the two organizations and agree on what is confidential. XYZ also requests that business partners disclose their security, data classification, and retention policies to ensure that XYZ's data is afforded the proper retention and information protection. The CISO, with the information security team, is responsible for maintaining and updating confidentiality, system security, and related policies.

At the time of hire or affiliation, the code of conduct and confidentiality agreements that employees are required to sign prohibit any disclosures, beyond the extent authorized, of information and other data to which the employee has been granted access. Individual manufacturing contracts also define how confidential information is authorized and rescinded. Signed nondisclosure agreements are required from third parties before information designated as confidential can be shared with them. XYZ's business partners are also subject to nondisclosure agreements or other contractual confidentiality provisions, as outlined in the Business Associate Agreement. Customer contracts, service-level agreements, and vendor contracts are negotiated before performance or receipt of service and formally signed off on by management.

Logical Access. Customers, groups of individuals, or other entities are restricted from accessing confidential information, other than their own. Users, contractors, or vendors who have the ability to access confidential information are properly authorized or supervised, in line with the Company's employees. The information supervisor for a business unit determines whether users require access to confidential information to perform their specific job functions.

Data Retention. Retention periods, and policies for ensuring retention during the specified period and proper disposal of data at the end of the retention period, are also outlined in the data classification and retention policy. The retention period assigned to data is based on the (1) classification of the data, (2) regulatory requirements and legal statutes, and (3) the general requirements of the business.

During the designated retention period, XYZ ensures that backup media (whether offline or online) are stored in a protected environment for the duration of the designated document retention period. Computer backup media is included. When the retention period has ended, XYZ Manufacturing destroys the information securely. Electronic information and other information is disposed of securely by proven means.

Appendix H

Definitions

This appendix is nonauthoritative and is included for informational purposes only.

For purposes of this guide, certain key terms are defined as follows:

access to personal information. The ability of the data subject to view personal information held by an entity. This ability may be complemented by an ability to update or correct the information. Access defines the intersection of identity and data, that is, who can do what to which data. Access is one of the fair information practice principles. Individuals must be able to find out what personal information an entity has on file about them and how the information is being used. Individuals need to be able to correct erroneous information in such records.

architecture. The design of the structure of a system, including logical components, and the logical interrelationships of a computer, its operating system, a network, or other elements.

authentication. The process of verifying the identity or other attributes claimed by or assumed of an entity (user, process, or device) or the process of verifying the source and integrity of data.

authorization. The process of granting access privileges to a user, program, or process by a person that has the authority to grant such access.

board, board of directors, or directors. Individuals with responsibility for overseeing the strategic direction of the entity and the obligations related to the accountability of the entity. Depending on the nature of the entity, such responsibilities may be held by a board of directors or supervisory board for a corporation, a board of trustees for a not-for-profit entity, a board of governors or commissioners for a government entity, general partners for a partnership, or an owner for a small business.

business partner. An individual or business (and its employees), other than a vendor, who has some degree of involvement with the entity's business dealings or agrees to cooperate, to any degree, with the entity (for example, a computer manufacturer who works with another company who supplies them with parts).

collection. The process of obtaining personal information from the individual directly (for example, through the individual's submission of an Internet form or a registration form) or from another party such as a business partner.

commitments. Declarations made by management to customers regarding performance of the entity or its goods or services. Commitments can be communicated in written individualized agreements, standardized contracts, service-level agreements, or published statements (for example, a security practices statement). A commitment may relate to one or more trust services categories. Commitments may be made on many different aspects of the service being provided, including the following:

- Specification of the algorithm used in a calculation

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

- The hours a system will be available
- Published password standards
- Encryption standards used to encrypt stored customer data

component. One of the five elements of internal control, including the control environment, risk assessment, control activities, information and communication, and monitoring activities.

compromise. Refers to a loss of confidentiality, integrity, or availability of information, including any resultant impairment of (1) processing integrity or availability of systems or (2) the integrity or availability of system inputs or outputs.

contractor. An individual, other than an employee, engaged to provide services to an entity in accordance with the terms of a contract.

control. A policy or procedure that is part of internal control. Controls exist within each of the five COSO internal control components: control environment, risk assessment, control activities, information and communication, and monitoring.

control activity. An action established through policies and procedures to enable management's directives to mitigate risks to the achievement of objectives are carried out.

consent. This privacy requirement is one of the fair information practice objectives. Individuals must be able to prevent the collection of their personal data, unless legally required. If an individual has a choice about the use or disclosure of his or her information, consent is the individual's way of giving permission for the use or disclosure. Consent may be affirmative (for example, opting in) or implied (for example, not opting out). There are two types of consent:

- **explicit consent.** A requirement that an individual "signifies" his or her agreement with a data controller by some active communication between the parties.
- **implied consent.** When consent may reasonably be inferred from the action or inaction of the individual.

COSO. The Committee of Sponsoring Organizations of the Treadway Commission. COSO is a joint initiative of five private sector organizations and is dedicated to providing thought leadership through the development of frameworks and guidance on enterprise risk management, internal control, and fraud deterrence. (See www.coso.org.)

cybersecurity objectives. The objectives that an entity establishes to address the cybersecurity risks that could otherwise threaten the achievement of the entity's overall business objectives.

cybersecurity risk management examination. An examination engagement to report on whether (*a*) management's description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and (*b*) the controls included in that program were effective to achieve the entity's cybersecurity objectives based on the control criteria. A cybersecurity risk management examination is performed in accordance with the attestation standards and this guide.

cybersecurity risk management examination report. The end product of the cybersecurity risk management examination, which includes management's description of the entity's cybersecurity risk management program, management's assertion, and the practitioner's report.

cyberspace. The interdependent network of information system infrastructures including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.

data subjects. The individual about whom personal information is collected.

deficiency. Used to identify misstatements in which controls were not suitably designed or did not operate effectively.

description misstatement. Used when describing differences between (or omissions in) the presentation of the description of the cybersecurity risk management program and the description criteria.

design. As used in the COSO definition of internal control, the internal control system design is intended to provide reasonable assurance of the achievement of an entity's objectives, if those controls operated as designed.

design-only cybersecurity risk management examination. An examination engagement to report on (*a*) whether management's description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and (*b*) the suitably of the design of controls implemented within that program to achieve the entity's cybersecurity objectives.

deviation. Used to identify misstatements in which the operation of a control was not effective in a specific instance. A deviation may, individually or in combination with other deviations, result in a deficiency.

disclosure. The release, transfer, provision of access to, or divulgence in any other manner of information outside the entity holding the information. Disclosure is often used interchangeably with the terms *sharing* and *onward transfer*.

disposal. A phase of the data lifecycle that pertains to how an entity removes or destroys data or information.

environmental protections and **safeguards.** Controls and other activities implemented by the entity to detect, prevent, and manage the risk of casualty damage to the physical parts of the information system (for example, protections from fire, flood, wind, earthquake, power surge, or power outage).

entity. A legal entity or management operating model of any size established for a particular purpose. A legal entity may, for example, be a business enterprise, a not-for-profit organization, a government body, or an academic institution. The management operating model may follow product or service lines, divisions, or operating units, with geographic markets providing for further subdivisions or aggregations of performance.

entity-wide. Activities that apply across the entity—most commonly in relation to entity-wide controls.

external parties (or external users). Individuals, other than internal users, who are authorized by customers, entity management, or other authorized parties to interact with the entity's information system.

information and systems. Refers to information in electronic form during its use, processing, transmission, and storage and systems that use such information to process, transmit or transfer, and store information.

information assets. Data and the associated software and infrastructure used to process, transmit, and store information.

infrastructure. The collection of physical or virtual resources that supports an overall IT environment, including the server, storage, and network components.

inherent limitations. Those limitations present in all internal control systems. The limitations relate to the preconditions of internal control, external events beyond the entity's control, limits of human judgment, the reality that breakdowns can occur, and the possibility of management override and collusion.

inherent risks. Risks to the achievement of objectives in the absence of any actions management might take to alter either the risk likelihood or impact.

inherent cybersecurity risks. Inherent risks arising from cybersecurity threats and vulnerabilities of information assets that would prevent the entity's cybersecurity objectives from being achieved.

internal control. A process, effected by an entity's board of directors, management, and other personnel, designed to provide reasonable assurance regarding the achievement of objectives relating to operations, reporting, and compliance.

internal users. Personnel whose job function causes them to be members of the people component of the information system.

management override. Management's overruling of prescribed policies or procedures for illegitimate purposes with the intent of personal gain or an enhanced presentation of an entity's financial condition, compliance status, or cybersecurity risk management program.

outsourced service providers. A service provider vendor that performs business processes, operations, or controls on behalf of the entity when such business processes, operations, or controls are necessary to achieve the entity's objectives.

personal information. Information that is, or can be about or related to, an identifiable individual.

policy[ies]. Management or board member statements of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. Policies serve as the basis for procedures.

privacy commitments. Declarations made by management regarding the performance of a system processing personal information. Such commitments can be communicated in written agreements, standardized contracts, service level agreements, or published statements (for example, a privacy practices statement). In addition, privacy commitments may be made on many different aspects of the service being provided, including the following:

- Types of information processed by the system

- Employees, third parties, and other persons that can access the information
- Conditions under which information can be processed without consent

Examples of privacy commitments include the following:

- The organization will not process or transfer information without obtaining the data subject's consent.
- The organization will provide a privacy notice to customers once in 6 months or when there is a change in the organization's business policies.
- The organization will respond to access requests within 10 working days of receiving the request from its customers.

privacy notice. A written communication by entities that collect personal information, to the individuals about whom personal information is collected, about the entity's (*a*) policies regarding the nature of the information that they will collect and how that information will be used, retained, disclosed, and disposed of or anonymized and (*b*) commitment to adhere to those policies. A privacy notice also includes information about such matters as the purpose of collecting the information, the choices that individuals have related to their personal information, the security of such information, and how individuals can contact the entity with inquiries, complaints, and disputes related to their personal information. When a user entity collects personal information from individuals, it typically provides a privacy notice to those individuals.

report users. Intended users of the practitioner's report in accordance with AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*). There may be a broad range of report users for a general purpose report, but only a limited number of specified parties for a report that is restricted in accordance with paragraph .64 of AT-C section 205.

retention. A phase of the data lifecycle that pertains to how long an entity stores information for future use or reference.

risk. The possibility that an event will occur and adversely affect the achievement of objectives.

risk of material misstatement. The risk that management's description of the entity's cybersecurity risk management program is not presented in accordance with the description criteria or that controls within that program were not effective to achieve the entity's cybersecurity objectives.

risk response. The decision to accept, avoid, reduce, or share a risk.

risk tolerance. The acceptable variation relative to performance to the achievement of objectives.

security event. An occurrence, arising from actual or attempted unauthorized access or use by internal or external parties, that impairs or could impair the availability, integrity, or confidentiality of information or systems, result in unauthorized disclosure or theft of information or other assets, or cause damage to systems.

security incident. A security event that requires action on the part of an entity in order to protect information assets and resources.

senior management. The CEO or equivalent organizational leader and senior management team.

service provider. A vendor (such as a service organization) engaged to provide services to or on behalf of the entity. Service providers include outsourced services providers as well as vendors that provide services not associated with business functions such as janitorial, legal, and audit services.

SOC 2 examination. An examination engagement to report on the fairness of the presentation of management's description of the service organization's system, the suitability of the design of the controls included in the description, and, when a type 2 report is being issued, the operating effectiveness of those controls. The SOC 2 examination is performed in accordance with the attestation standards and AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)*.

stakeholder. Parties that are affected by the entity, such as shareholders, investors, the communities in which the entity operates, employees, customers, and suppliers.

subsequent events. Events or transactions that occur after the specified period of time covered by the engagement, but prior to the period end date of management's description, that could have a significant effect on the description of the entity's cybersecurity risk management program.

system. Refers to the infrastructure, software, people, processes, and data that are designed, implemented, and operated to work together to achieve one or more specific business objectives (for example, delivery of services or production of goods) in accordance with management-specified requirements. As used in this document, systems include manual, automated, and partially automated systems that are used for information processing, manufacturing and production, inventory management and distribution, information storage, and support functions within an organization.

system boundaries. The specific aspects of an entity's infrastructure, software, people, procedures, and data necessary to perform a function or provide a service. When the systems for multiple functions or services share aspects, infrastructure, software, people, procedures, and data, the systems will overlap, but the boundaries of each service's system will differ. In an engagement that addresses the confidentiality and privacy criteria, the system boundaries cover, at a minimum, all the system components as they relate to the life cycle of the confidential and personal information within well-defined processes and informal ad hoc procedures.

system components. Refers to the individual elements of a system. System components can be classified into the following five categories: infrastructure, software, people, processes, and data.

system requirements. Specifications regarding how the system should function to meet the entity's commitments to customers and relevant laws, regulations, and guidelines of industry groups, such as business or trade associations. Requirements are often specified in the entity's system policies and procedures, system design documentation, contracts with customers,

and government regulations. Examples of system requirements are as follows:

- Employee fingerprinting and background checks established in government banking regulations
- System edits that restrict the values accepted for system input, which are defined in application design documents
- Maximum acceptable intervals between periodic reviews of workforce member logical access, as documented in the security policy manual
- Data definition and tagging standards, including any associated metadata requirements, established by industry groups or other bodies, such as the Simple Object Access Protocol
- Business processing rules and standards established by regulators, for example, security requirements under the Health Insurance Portability and Accountability Act (HIPAA)

System requirements may result from the entity's commitments relating to security, availability, processing integrity, confidentiality, or privacy. For example, a commitment to programmatically enforce segregation of duties between data entry and data approval creates system requirements regarding user access administration.

third party. An individual or organization other than the entity and its employees. Third parties may be customers, vendors, business partners, or others.

trust services. A set of professional attestation and advisory services performed by CPAs based on a core set of criteria that address an entity's objectives related to security, availability, processing integrity, confidentiality, or privacy.

unauthorized access. Access to information or system components that (*a*) has not been approved by a person designated to do so by management and (*b*) compromises segregation of duties, confidentiality commitments, or otherwise increases risks to the information or system components beyond the levels approved by management (that is, access is inappropriate).

vendor. An individual or business (and its employees) that is engaged to provide goods or services to the entity. Depending on the services a vendor provides (for example, if it operates certain controls on behalf of the entity that are necessary to achieve the entity's cybersecurity objectives), it might also be a service provider.

Appendix I

Overview of Statements on Quality Control Standards

This appendix is nonauthoritative and is included for informational purposes only.

This appendix is a partial reproduction of chapter 1 of the AICPA practice aid *Establishing and Maintaining a System of Quality Control for a CPA Firm's Accounting and Auditing Practice*, available at www.aicpa.org/interestareas/frc/pages/enhancingauditqualitypracticeaid.aspx.

This appendix highlights certain aspects of the quality control standards issued by the AICPA. If appropriate, readers should also refer to the quality control standards issued by the PCAOB, available at www.pcaobus.org/Standards/QC/Pages/default.aspx.

1.01 The objectives of a system of quality control are to provide a CPA firm with reasonable assurance[1] that the firm and its personnel comply with professional standards and applicable regulatory and legal requirements, and that the firm or engagement partners issue reports that are appropriate in the circumstances. QC section 10, *A Firm's System of Quality Control* (AICPA, *Professional Standards*), addresses a CPA firm's responsibilities for its system of quality control for its accounting and auditing practice. That section is to be read in conjunction with the AICPA Code of Professional Conduct and other relevant ethical requirements.

1.02 A system of quality control consists of policies designed to achieve the objectives of the system and the procedures necessary to implement and monitor compliance with those policies. The nature, extent, and formality of a firm's quality control policies and procedures will depend on various factors such as the firm's size; the number and operating characteristics of its offices; the degree of authority allowed to, and the knowledge and experience possessed by, firm personnel; and the nature and complexity of the firm's practice.

Communication of Quality Control Policies and Procedures

1.03 The firm should communicate its quality control policies and procedures to its personnel. Most firms will find it appropriate to communicate their policies and procedures in writing and distribute them, or make them available electronically, to all professional personnel. Effective communication includes the following:

- A description of quality control policies and procedures and the objectives they are designed to achieve

[1] The term *reasonable assurance*, which is defined as a high, but not absolute, level of assurance, is used because absolute assurance cannot be attained. Paragraph .53 of QC section 10, *A Firm's System of Quality Control* (AICPA, *Professional Standards*), states, "Any system of quality control has inherent limitations that can reduce its effectiveness."

Guide: Reporting on an Entity's Cybersecurity Risk Management Program and Controls, 2nd Edition. AICPA.

- The message that each individual has a personal responsibility for quality
- A requirement for each individual to be familiar with and to comply with these policies and procedures

Effective communication also includes procedures for personnel to communicate their views or concerns on quality control matters to the firm's management.

Elements of a System of Quality Control

1.04 A firm must establish and maintain a system of quality control. The firm's system of quality control should include policies and procedures that address each of the following elements of quality control identified in paragraph .17 of QC section 10:

- Leadership responsibilities for quality within the firm (the "tone at the top")
- Relevant ethical requirements
- Acceptance and continuance of client relationships and specific engagements
- Human resources
- Engagement performance
- Monitoring

1.05 The elements of quality control are interrelated. For example, a firm continually assesses client relationships to comply with relevant ethical requirements, including independence, integrity, and objectivity, and policies and procedures related to the acceptance and continuance of client relationships and specific engagements. Similarly, the human resources element of quality control encompasses criteria related to professional development, hiring, advancement, and assignment of firm personnel to engagements, all of which affect policies and procedures related to engagement performance. In addition, policies and procedures related to the monitoring element of quality control enable a firm to evaluate whether its policies and procedures for each of the other five elements of quality control are suitably designed and effectively applied.

1.06 Policies and procedures established by the firm related to each element are designed to achieve reasonable assurance with respect to the purpose of that element. Deficiencies in policies and procedures for an element may result in not achieving reasonable assurance with respect to the purpose of that element; however, the system of quality control, as a whole, may still be effective in providing the firm with reasonable assurance that the firm and its personnel comply with professional standards and applicable regulatory and legal requirements and that the firm or engagement partners issue reports that are appropriate in the circumstances.

1.07 If a firm merges, acquires, sells, or otherwise changes a portion of its practice, the surviving firm evaluates and, as necessary, revises, implements, and maintains firm-wide quality control policies and procedures that are appropriate for the changed circumstances.

Leadership Responsibilities for Quality Within the Firm (the "Tone at the Top")

1.08 The purpose of the leadership responsibilities element of a system of quality control is to promote an internal culture based on the recognition that quality is essential in performing engagements. The firm should establish and maintain the following policies and procedures to achieve this purpose:

- Require the firm's leadership (managing partner, board of managing partners, CEO, or equivalent) to assume ultimate responsibility for the firm's system of quality control.
- Provide the firm with reasonable assurance that personnel assigned operational responsibility for the firm's quality control system have sufficient and appropriate experience and ability to identify and understand quality control issues and develop appropriate policies and procedures, as well as the necessary authority to implement those policies and procedures.

1.09 Establishing and maintaining the following policies and procedures assists firms in recognizing that the firm's business strategy is subject to the overarching requirement for the firm to achieve the objectives of the system of quality control in all the engagements that the firm performs:

- Assign management responsibilities so that commercial considerations do not override the quality of the work performed.
- Design policies and procedures addressing performance evaluation, compensation, and advancement (including incentive systems) with regard to personnel to demonstrate the firm's overarching commitment to the objectives of the system of quality control.
- Devote sufficient and appropriate resources for the development, communication, and support of its quality control policies and procedures.

Relevant Ethical Requirements

1.10 The purpose of the relevant ethical requirements element of a system of quality control is to provide the firm with reasonable assurance that the firm and its personnel comply with relevant ethical requirements when discharging professional responsibilities. Relevant ethical requirements include independence, integrity, and objectivity. Establishing and maintaining policies such as the following assist the firm in obtaining this assurance:

- Require that personnel adhere to relevant ethical requirements such as those in regulations, interpretations, and rules of the AICPA, state CPA societies, state boards of accountancy, state statutes, the U.S. Government Accountability Office, and any other applicable regulators.
- Establish procedures to communicate independence requirements to firm personnel and, where applicable, others subject to them.
- Establish procedures to identify and evaluate possible threats to independence and objectivity, including the familiarity threat that may be created by using the same senior personnel on an audit

or attest engagement over a long period of time, and to take appropriate action to eliminate those threats or reduce them to an acceptable level by applying safeguards.

- Require that the firm withdraw from the engagement if effective safeguards to reduce threats to independence to an acceptable level cannot be applied.
- Require written confirmation, at least annually, of compliance with the firm's policies and procedures on independence from all firm personnel required to be independent by relevant requirements.
- Establish procedures for confirming the independence of another firm or firm personnel in associated member firms who perform part of the engagement. This would apply to national firm personnel, foreign firm personnel, and foreign-associated firms.[2]
- Require the rotation of personnel for audit or attest engagements where regulatory or other authorities require such rotation after a specified period.

Acceptance and Continuance of Client Relationships and Specific Engagements

1.11 The purpose of the quality control element that addresses acceptance and continuance of client relationships and specific engagements is to establish criteria for deciding whether to accept or continue a client relationship and whether to perform a specific engagement for a client. A firm's client acceptance and continuance policies represent a key element in mitigating litigation and business risk. Accordingly, it is important that a firm be aware that the integrity and reputation of a client's management could reflect the reliability of the client's accounting records and financial representations and, therefore, affect the firm's reputation or involvement in litigation. A firm's policies and procedures related to the acceptance and continuance of client relationships and specific engagements should provide the firm with reasonable assurance that it will undertake or continue relationships and engagements only where it

- is competent to perform the engagement and has the capabilities, including the time and resources, to do so;
- can comply with legal and relevant ethical requirements;
- has considered the client's integrity and does not have information that would lead it to conclude that the client lacks integrity; and
- has reached an understanding with the client regarding the services to be performed.

1.12 This assurance should be obtained before accepting an engagement with a new client, when deciding whether to continue an existing engagement, and when considering acceptance of a new engagement with an existing client. Establishing and maintaining policies such as the following assist the firm in obtaining this assurance:

---

[2] A *foreign-associated firm* is a firm domiciled outside of the United States and its territories that is a member of, correspondent with, or similarly associated with an international firm or international association of firms.

- Evaluate factors that have a bearing on management's integrity and consider the risk associated with providing professional services in particular circumstances.[3]
- Evaluate whether the engagement can be completed with professional competence; undertake only those engagements for which the firm has the capabilities, resources, and professional competence to complete; and evaluate, at the end of specific periods or upon occurrence of certain events, whether the relationship should be continued.
- Obtain an understanding, preferably in writing, with the client regarding the services to be performed.
- Establish procedures on continuing an engagement and the client relationship, including procedures for dealing with information that would have caused the firm to decline an engagement if the information had been available earlier.
- Require documentation of how issues relating to acceptance or continuance of client relationships and specific engagements were resolved.

Human Resources

1.13 The purpose of the human resources element of a system of quality control is to provide the firm with reasonable assurance that it has sufficient personnel with the capabilities, competence, and commitment to ethical principles necessary (*a*) to perform its engagements in accordance with professional standards and regulatory and legal requirements, and (*b*) to enable the firm to issue reports that are appropriate in the circumstances. Establishing and maintaining policies such as the following assist the firm in obtaining this assurance:

- Recruit and hire personnel of integrity who possess the characteristics that enable them to perform competently.
- Determine capabilities and competencies required for an engagement, especially for the engagement partner, based on the characteristics of the particular client, industry, and kind of service being performed. Specific competencies necessary for an engagement partner are discussed in paragraph .A27 of QC section 10.
- Determine the capabilities and competencies possessed by personnel.
- Assign the responsibility for each engagement to an engagement partner.

---

[3] Such considerations would include the risk of providing professional services to significant clients or to other clients for which the practitioner's objectivity or the appearance of independence may be impaired. In broad terms, the significance of a client to a member or a firm refers to relationships that could diminish a practitioner's objectivity and independence in performing attest services. Examples of factors to consider in determining the significance of a client to an engagement partner, office, or practice unit include (*a*) the amount of time the partner, office, or practice unit devotes to the engagement, (*b*) the effect on the partner's stature within the firm as a result of his or her service to the client, (*c*) the manner in which the partner, office, or practice unit is compensated, or (*d*) the effect that losing the client would have on the partner, office, or practice unit.

- Assign personnel based on the knowledge, skills, and abilities required in the circumstances and the nature and extent of supervision needed.
- Have personnel participate in general and industry-specific continuing professional education and professional development activities that enable them to accomplish assigned responsibilities and satisfy applicable continuing professional education requirements of the AICPA, state boards of accountancy, and other regulators.
- Select for advancement only those individuals who have the qualifications necessary to fulfill the responsibilities they will be called on to assume.

Engagement Performance

1.14 The purpose of the engagement performance element of quality control is to provide the firm with reasonable assurance (*a*) that engagements are consistently performed in accordance with applicable professional standards and regulatory and legal requirements, and (*b*) that the firm or the engagement partner issues reports that are appropriate in the circumstances. Policies and procedures for engagement performance should address all phases of the design and execution of the engagement, including engagement performance, supervision responsibilities, and review responsibilities. Policies and procedures also should require that consultation takes place when appropriate. In addition, a policy should establish criteria against which all engagements are to be evaluated to determine whether an engagement quality control review should be performed.

1.15 Establishing and maintaining policies such as the following assist the firm in obtaining the assurance required relating to the engagement performance element of quality control:

- Plan all engagements to meet professional, regulatory, and the firm's requirements.
- Perform work and issue reports and other communications that meet professional, regulatory, and the firm's requirements.
- Require that work performed by other team members be reviewed by qualified engagement team members, which may include the engagement partner, on a timely basis.
- Require the engagement team to complete the assembly of final engagement files on a timely basis.
- Establish procedures to maintain the confidentiality, safe custody, integrity, accessibility, and retrievability of engagement documentation.
- Require the retention of engagement documentation for a period of time sufficient to meet the needs of the firm, professional standards, laws, and regulations.
- Require that
  - consultation take place when appropriate (for example, when dealing with complex, unusual, unfamiliar, difficult, or contentious issues);

- sufficient and appropriate resources be available to enable appropriate consultation to take place;
- all the relevant facts known to the engagement team be provided to those consulted;
- the nature, scope, and conclusions of such consultations be documented; and
- the conclusions resulting from such consultations be implemented.

- Require that
  - differences of opinion be dealt with and resolved;
  - conclusions reached are documented and implemented; and
  - the report not be released until the matter is resolved.
- Require that
  - all engagements be evaluated against the criteria for determining whether an engagement quality control review should be performed;
  - an engagement quality control review be performed for all engagements that meet the criteria; and
  - the review be completed before the report is released.
- Establish procedures addressing the nature, timing, extent, and documentation of the engagement quality control review.
- Establish criteria for the eligibility of engagement quality control reviewers.

Monitoring

1.16 The purpose of the monitoring element of a system of quality control is to provide the firm and its engagement partners with reasonable assurance that the policies and procedures related to the system of quality control are relevant, adequate, operating effectively, and complied with in practice. Monitoring involves an ongoing consideration and evaluation of the appropriateness of the design, the effectiveness of the operation of a firm's quality control system, and a firm's compliance with its quality control policies and procedures. The purpose of monitoring compliance with quality control policies and procedures is to provide an evaluation of the following:

- Adherence to professional standards and regulatory and legal requirements
- Whether the quality control system has been appropriately designed and effectively implemented
- Whether the firm's quality control policies and procedures have been operating effectively so that reports issued by the firm are appropriate in the circumstances

1.17 Establishing and maintaining policies such as the following assist the firm in obtaining the assurance required relating to the monitoring element of quality control:

- Assign responsibility for the monitoring process to a partner or partners or other persons with sufficient and appropriate experience and authority in the firm to assume that responsibility.
- Assign performance of the monitoring process to competent individuals.
- Require the performance of monitoring procedures that are sufficiently comprehensive to enable the firm to assess compliance with all applicable professional standards and the firm's quality control policies and procedures. Monitoring procedures consist of the following:
  - Review of selected administrative and personnel records pertaining to the quality control elements.
  - Review of engagement documentation, reports, and clients' financial statements.
  - Summarization of the findings from the monitoring procedures, at least annually, and consideration of the systemic causes of findings that indicate that improvements are needed.
  - Determination of any corrective actions to be taken or improvements to be made with respect to the specific engagements reviewed or the firm's quality control policies and procedures.
  - Communication of the identified findings to appropriate firm management personnel.
  - Consideration of findings by appropriate firm management personnel who should also determine that any actions necessary, including necessary modifications to the quality control system, are taken on a timely basis.
  - Assessment of
    - the appropriateness of the firm's guidance materials and any practice aids;
    - new developments in professional standards and regulatory and legal requirements and how they are reflected in the firm's policies and procedures where appropriate;
    - compliance with policies and procedures on independence;
    - the effectiveness of continuing professional development, including training;
    - decisions related to acceptance and continuance of client relationships and specific engagements; and
    - firm personnel's understanding of the firm's quality control policies and procedures and implementation thereof.
- Communicate at least annually, to relevant engagement partners and other appropriate personnel, deficiencies noted as a result of

the monitoring process and recommendations for appropriate remedial action.

- Communicate the results of the monitoring of its quality control system process to relevant firm personnel at least annually.
- Establish procedures designed to provide the firm with reasonable assurance that it deals appropriately with the following:
  - — Complaints and allegations that the work performed by the firm fails to comply with professional standards and regulatory and legal requirements.
  - — Allegations of noncompliance with the firm's system of quality control.
  - — Deficiencies in the design or operation of the firm's quality control policies and procedures, or noncompliance with the firm's system of quality control by an individual or individuals, as identified during the investigations into complaints and allegations.

  This includes establishing clearly defined channels for firm personnel to raise any concerns in a manner that enables them to come forward without fear of reprisal and documenting complaints and allegations and the responses to them.
- Require appropriate documentation to provide evidence of the operation of each element of its system of quality control. The form and content of documentation evidencing the operation of each of the elements of the system of quality control is a matter of judgment and depends on a number of factors, including the following, for example:
  - — The size of the firm and the number of offices.
  - — The nature and complexity of the firm's practice and organization.
- Require retention of documentation providing evidence of the operation of the system of quality control for a period of time sufficient to permit those performing monitoring procedures and peer review to evaluate the firm's compliance with its system of quality control, or for a longer period if required by law or regulation.

1.18 Some of the monitoring procedures discussed in the previous list may be accomplished through the performance of the following:

- Engagement quality control review
- Review of engagement documentation, reports, and clients' financial statements for selected engagements after the report release date
- Inspection[4] procedures

---

[4] *Inspection* is a retrospective evaluation of the adequacy of the firm's quality control policies and procedures, its personnel's understanding of those policies and procedures, and the extent of the firm's compliance with them. Although monitoring procedures are meant to be ongoing, they may include inspection procedures performed at a fixed point in time. Monitoring is a broad concept; inspection is one specific type of monitoring procedure.

Documentation of Quality Control Policies and Procedures

1.19 The firm should document each element of its system of quality control. The extent of the documentation will depend on the size, structure, and nature of the firm's practice. Documentation may be as simple as a checklist of the firm's policies and procedures or as extensive as practice manuals.

Applying the Quality Control Standards to Four Hypothetical Firms

1.20 Subsequent chapters in this practice aid present four different hypothetical firms and the quality control policies and procedures each firm implements to address each of the quality control elements. Following is a description of those firms and their characteristics:

- Multioffice CPA Firm has 10 offices in 3 states and is centrally managed. It has approximately 15 partners and 100 professionals. Its accounting and auditing practice has a concentration of financial institution clients for which it performs audit and attest services. Multioffice CPA Firm has no issuer clients. (Chapter 2, "System of Quality Control for a CPA Firm's Accounting and Auditing Practice—Firm With Multiple Offices")
- Singleoffice CPA Firm has 1 office, 3 partners, and 10 professionals. Its accounting and auditing practice has a concentration of employee benefit plan audits. Singleoffice CPA Firm has no issuer clients. (Chapter 3, "System of Quality Control for a CPA Firm's Accounting and Auditing Practice—Firm With a Single Office")
- Sole Practitioner, CPA, is a sole owner who has no professional staff and occasionally hires per diem professionals. Her accounting practice consists only of engagements subject to Statements on Standards for Accounting and Review Services. (Chapter 4, "System of Quality Control for a CPA Firm's Accounting and Auditing Practice—Sole Practitioner") (Note: Sole practitioners who perform audit and attest engagements should refer to chapter 3)
- Closely Aligned CPA Firm and Non-CPA-Owned Entity are organized in an *alternative practice structure*, which is a nontraditional structure in the practice of public accounting consisting of an attest and a nonattest portion of the practice. The attest portion is conducted through a firm, Closely Aligned CPA Firm, owned and controlled by CPAs. The nonattest portion is conducted through a separate entity, Non-CPA-owned Entity, owned and controlled by individuals who are not CPAs. (Chapter 5, "System of Quality Control for an Alternative Practice Structure")

1.21 The policies and procedures described in each chapter are those that a firm of a similar size and type may consider establishing and maintaining. The policies and procedures used by an actual firm need not necessarily include nor be limited to all those used by the illustrative firms.

