April 2017

Association
of International
Certified Professional
Accountants®

Information for entity management

Note to readers:

The purpose of this document 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 document 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.

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

[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 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,

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 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* 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

protected health information, customers' credit card information, and the systems that process, transmit, and store such information.

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

[3]

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.
- *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.

Association
of International
Certified Professional
Accountants®