DESCRIPTION CRITERIA FOR MANAGEMENT'S DESCRIPTION OF THE ENTITY'S CYBERSECURITY RISK MANAGEMENT PROGRAM

April 15, 2017

Issued by the AICPA Assurance Services Executive Committee (ASEC)
Prepared by ASEC's Cybersecurity Working Group

1 2 3 4 5 6 7 8 9 0 BRAAS 1 9 8 7

Notice to Readers

Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program presents criteria established by the Assurance Services Executive Committee (ASEC) of the AICPA for use by (*a*) management, when preparing a description of an entity's cybersecurity risk management program, and (*b*) practitioners when evaluating that description, in connection with services performed on an entity's cybersecurity risk management program. ASEC, in establishing and developing these criteria, followed due process procedures, including exposure of the proposed description criteria for public comment. Under BL section 360, *Committees* (AICPA, *Professional Standards*), ASEC has been designated as a senior committee and has been given authority to make public statements and publish measurement criteria without clearance from AICPA Council or the board of directors.

Table of Contents

Description Criteria for Management's Description of the Entity's Cybersecurity Risk Management Program

Background

.01 The AICPA ASEC, through its Cybersecurity Working Group, has developed a set of benchmarks, known as *description criteria*, to be used when preparing and evaluating the presentation of a *description of the entity's cybersecurity risk management program* (description). An entity's *cybersecurity risk management program* is the set of policies, processes, and controls designed to protect information [fn 1] and systems [fn 2] from security events [fn 3] that could compromise [fn 4] the achievement of the entity's cybersecurity objectives [fn 5] and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented. This document presents the description criteria.

.02 Applying the description criteria in actual situations requires judgment. Therefore, in addition to the description criteria, this document also 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.

[fn 1] As used here, the term *information and systems* refers to information in electronic form (electronic information) during its use, processing, transmission, and storage and the systems that use, process, transmit or transfer, and store such electronic information.

[fn 2] A *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. Systems that have cybersecurity risks include, but are not limited to (*a*) manufacturing and production systems that are automated and partially automated (including the industrial control systems components of those systems), (*b*) inventory management and distribution systems and (*c*) treasury and funds management and other types of back office systems.

[fn 3] 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.

[fn 4] *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.

[fn 5] *Cybersecurity objectives* are those that address the cybersecurity risks that could affect the achievement of the entity's overall business objectives (including compliance, reporting, and operational objectives).

Applicability and Use of Description Criteria

Examination of an Entity’s Cybersecurity Risk Management Program

.03 The description criteria presented in this document were developed in conjunction with the cybersecurity risk management examination described in AICPA Guide *Reporting on an Entity’s Cybersecurity Risk Management Program and Controls* (the cybersecurity guide). That 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*). The cybersecurity risk management examination is predicated on the concept that, because management is ultimately responsible for developing, implementing, and operating the entity’s cybersecurity risk management program, management is responsible for the following:

- Developing and presenting a description of the entity’s cybersecurity risk management program
- Making an assertion about whether the description is presented in accordance with the description criteria
- Making an assertion about the effectiveness of the controls within the program based on a set of control criteria

The CPA (known as a *practitioner*) expresses an opinion on whether the description is presented in accordance with the description criteria and on the effectiveness of controls. [fn 6]

.04 For the cybersecurity risk management examination described in the cybersecurity guide, these description criteria are intended to serve as a set of suitable criteria for management’s description. Management uses the description criteria when preparing the description of the entity’s cybersecurity risk management program; the practitioner uses the description criteria when evaluating whether the presentation is presented in accordance with the description criteria.

Consulting Services

.05 The description criteria in this document may be used by management and the practitioner in connection with nonattest services on an entity’s cybersecurity risk management program in accordance with CS section 100, *Consulting Services: Definitions and Standards* (AICPA, *Professional Standards*). A nonattest (non-assurance) consulting engagement may provide information and recommendations to management and often precedes an attestation engagement. In such circumstances, management and practitioners may find the description criteria in this document useful.

.06 If the practitioner is engaged to provide nonattest services to management (for example, if the practitioner is engaged to assist management with the development of the description of the entity’s

[fn 6] As discussed, the description is one of two separate but complementary subject matters in the cybersecurity risk management examination; the other is the effectiveness of the controls within that program to achieve the entity’s cybersecurity objectives based on the control criteria. This document does not, however, present the control criteria against which to measure and evaluate the effectiveness of controls within an entity’s cybersecurity risk management program. Management is responsible for selecting the control criteria to be used in the cybersecurity risk management examination and may select any control criteria, as long as it is considered suitable and available criteria for the engagement in accordance with the attestation standards.

cybersecurity risk management program), threats to the practitioner's independence may exist when that practitioner also provides attest services to the entity. The "Nonattest Services" interpretations (AICPA, *Professional Standards*, ET sec. 1.295) provide special independence requirements for practitioners who provide nonattest services for an attest client. In addition, the "Conceptual Framework Approach" interpretation (AICPA, *Professional Standards*, ET sec. 1.210) discusses threats to independence not specifically detailed elsewhere.

Suitability and Availability of the Description Criteria

.07 According to the attestation standards, the attributes of suitable criteria are as follows: [fn 7]

- *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 matter prepared in accordance with them does not omit relevant factors that could reasonably be expected to affect users' decisions made on the basis of that subject matter.

.08 In addition to being suitable, AT-C section 105 [fn 8] indicates that the criteria used in an attestation engagement should be available to report users. The publication of the description criteria makes the criteria available to report users. Accordingly, ASEC has concluded that the description criteria are suitable criteria in accordance with the attestation standards.

Categories of Description Criteria

.09 The description criteria included in this document 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.

[fn 7] Paragraph .A42 of AT-C section 105, *Concepts Common to All Attestation Engagements* (AICPA, *Professional Standards*).

[fn 8] Paragraph .25*b* of AT-C section 105.

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, use of 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 [fn 9] requiring a response, remediation, or both.

h. *Monitoring of the Cybersecurity Risk Management Program*. Disclosures Information 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

[fn 9] A *security incident* is a security event that requires action on the part of an entity in order to protect information assets and resources.

iii. the key security policies and processes implemented and operated to address the entity's cybersecurity risks.

Preparing and Evaluating the Presentation of Management's Description of the Entity's Cybersecurity Risk Management Program in Accordance With the Description Criteria

.10 Management's description of the entity's cybersecurity risk management program is intended to provide 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.

.11 Ordinarily, a description of an entity's cybersecurity risk management program 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 of the description criterion presented in paragraph .21; and
- does not omit or distort information that is likely to be relevant to users' decisions.

.12 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 disclosures in the description. In addition, the degree of detail to be included in the description generally is 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.

.13 Consideration of the implementation guidance presented for each criterion 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.

.14 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 affect the decisions of report users. Additional disclosures may include the following, for example:

- Significant interpretations made in applying the description criteria in the specific engagement circumstances (for example, what constitutes a security event or incident).
- Subsequent events, depending on their nature and significance.

- When reporting on only a portion of the entity-wide cybersecurity risk management program, a significant security incident that occurred in another portion of the program.

Materiality Considerations When Preparing and Evaluating the Presentation of the Description in Accordance With the Description Criteria

.15 As discussed in paragraph .02, 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.

.16 Qualitative factors to be considered include matters such as these:

- Whether the description is prepared at a level of detail likely to be meaningful to users
- Whether each of the description criteria in paragraph .21 has been addressed without using language that omits or distorts the information
- Whether the characteristics of the presentation are appropriate, as variations in presentation may occur

.17 For example, a description would not be presented in accordance with the description criteria if any of the following are true:

- It omits information involving one or more significant business units or segments, when the engagement addresses the entity-wide cybersecurity risk management program.
- It 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).
- It 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).
- It omits or distorts significant information related to any of the description criterion in a manner that might affect users' decisions.

.18 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 it is unlikely to be significant (in other words, immaterial) to report users' decisions.

Using the Description Criteria when Preparing and Evaluating a Description About Only a Portion of an Entity’s Cybersecurity Risk Management Program

.19 Though the description criteria were designed to permit management to describe an entity-wide cybersecurity risk management program, they also may be used when preparing and evaluating a description that is limited to only a portion of the entity. For example, they may be used when preparing and evaluating a description about 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, 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

.20 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 Program Description Criteria and Related Implementation Guidance

.21

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*

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.*

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*[fn 10] *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*

[fn 10] 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 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*
• *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*

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*

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*

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*

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*
• *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*

Effective Date

.22 The description criteria are effective upon issuance.

Appendix — Glossary

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 need to 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 or board of 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).

commitments. Declarations made by management to customers regarding the performance of one or more systems. 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
- The hours a system will be available
- Published password standards
- Encryption standards used to encrypt stored customer data

compromise. Refers to a loss of confidentiality, integrity, or availability of information, including any resulting 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.

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 within 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 AICPA attestation standards and the AICPA cybersecurity guide.

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.

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*.

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 elements 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. Refers to activities that apply across the entity—most commonly in relation to entity-wide controls.

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.

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 elements.

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.

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.

policies. 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 bases for procedures.

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 is restricted in accordance with paragraph .64 of AT-C section 205.

retention. A phase of the data life cycle that pertains to how 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 response. The decision to accept, avoid, reduce, or share a risk.

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 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.

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 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.

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 also might be a service provider.