EXPOSURE DRAFT

PROPOSED DESCRIPTION CRITERIA FOR MANAGEMENT'S DESCRIPTION OF AN ENTITY'S CYBERSECURITY RISK MANAGEMENT PROGRAM

September 15, 2016

Comments are requested by December 5, 2016.

Prepared by the AICPA Assurance Services Executive Committee Cybersecurity Working Group

CONTENTS

Page

Explanatory Memorandum

Exposure Draft

Explanatory Memorandum

Introduction

In response to growing market demand for information about the effectiveness of an entity's cybersecurity risk management program, the auditing profession, through the AICPA, is developing a new engagement that CPAs can use to assist boards of directors, senior management, and other pertinent stakeholders as they evaluate the effectiveness of an entity's cybersecurity risk management program. Because of the profession's commitment to continuous improvement, public service, and increasing investor confidence, this engagement (referred to as a *cybersecurity examination*) will be voluntary, flexible, and comprehensive. As cybersecurity risk management evolves, the AICPA will adapt and advance the engagement, incorporating feedback from users and addressing opportunities to enhance efficiency and reduce compliance burdens. To provide practitioners with performance and reporting guidance for the engagement, the AICPA's Auditing Standards Board (ASB) is working in conjunction with the Assurance Services Executive Committee (ASEC) to develop an attestation guide (referred to as the *cybersecurity attestation guide*).

The cybersecurity examination to be described in the cybersecurity attestation guide will be performed in accordance with the attestation standards. Under those standards, an attestation engagement is predicated on the concept that a party other than the practitioner[1] makes an assertion about whether the *subject matter* is measured or evaluated in accordance with suitable criteria. The attestation standards state that, in an examination engagement, the responsible party (generally, that is *management* in a cybersecurity examination engagement) takes responsibility for the subject matter.

In the cybersecurity examination, management makes an assertion about whether the subject matter is measured or evaluated in accordance with suitable criteria. The subject matter of the cybersecurity examination includes the following:

- A description of the entity's cybersecurity risk management program in accordance with the *description criteria.*

- An assessment of the effectiveness of the controls within that program to achieve the entity's cybersecurity objectives based on the *control criteria*.

[1] Under those standards, the CPA performing an attest engagement is known as a *practitioner*.

Because management is ultimately responsible for the entity's cybersecurity risk management program and the operation of the controls within that program, it is management's responsibility to develop and present, in the cybersecurity report, a description of the entity's cybersecurity risk management program. Management also is responsible for selecting both the description criteria and the control criteria to be used in the engagement. This document presents only the *description criteria* for use when preparing the description of the entity's cybersecurity risk management program.[2] In addition to the description criteria, this document also presents points of focus that represent important characteristics of the description criteria. Management may determine that some of these points of focus are not suitable or relevant and may identify and consider other characteristics based on specific circumstances of the entity. *Points of focus* assist management in determining the matters to be addressed in the presentation. However, use of the criteria does not require management to address every point of focus in its description.

In establishing and developing these criteria, ASEC follows due process procedures, including exposure of criteria for public comment. BL section 360R, *Implementing Resolutions under Section 3.6 Committees* (AICPA, *Professional Standards*), designates ASEC as a senior technical committee with authority to make public statements and publish measurement criteria without clearance from AICPA council or the board of directors. Accordingly, ASEC will conclude whether the description criteria are suitable criteria for preparing, and evaluating the presentation of, the description of the entity's cybersecurity risk management program in the cybersecurity examination described in the cybersecurity attestation guide.

Although the description criteria proposed in this document are for use when preparing, or evaluating the presentation of, the description of an entity's cybersecurity risk management program, such criteria also may be used when the practitioner is engaged to provide other nonattest or advisory services to a client in connection with the entity's cybersecurity risk management program. For instance, a practitioner may use such criteria when engaged to assist management with the development of its description of the entity's cybersecurity risk management program for use in internal reporting.

As previously noted, this document does not present the control criteria against which to measure and evaluate the effectiveness of controls within an entity's cybersecurity risk management program. Management may select any control criteria as long as it is considered suitable criteria for the engagement in accordance with the attestation standards.

[2] At the time of issuance, there were no other description criteria for use when preparing the description of an entity's cybersecurity risk management program.

Background

High profile cybersecurity attacks on major organizations have resulted in an increased focus on cybersecurity by an entity's directors, management, customers, and business partners. Regulators, analysts, and investors also have begun to focus on an entity's cybersecurity measures. Each of these user groups has expressed a desire for information about an entity's cybersecurity risk management program that would enable them to make informed decisions. Examples follow:

- Board members and directors need information about the entity's cybersecurity risk management program to help them fulfill their oversight responsibilities by understanding the cyber risks faced by the entity. They also want information from an independent third-party evaluator that will help them evaluate management's performance in managing cybersecurity risks.
- Business partners may benefit from information about controls the entity has in place to deal with threats to and vulnerabilities in systems used by the entity to produce or provide particular goods or services. This information is likely to be valuable to them when evaluating the entity's ability to provide those goods and services in the event of a disruption to its IT systems.
- Analysts and investors may benefit from information about an entity's cybersecurity risk management program that will help them understand the entity's cybersecurity risks that could threaten the achievement of the entity's operational, financial, legal, and regulatory objectives, all of which could have an adverse impact on the business's value and stock price.
- Some industry regulators may benefit from information about an entity's cybersecurity risk management program to support their oversight role.

Useful Information Included in Management's Description

Management's description of the entity's cybersecurity risk management program is designed to provide users with information about the environment in which the entity operates and the process used to develop its cybersecurity objectives, identify its sensitive information and systems, and manage the risks that threaten them. The description also provides users with a summarized description of the controls within the cybersecurity risk management program that have been designed and implemented to respond to those risks. It does not, however, provide a detailed description of such controls or a description of the procedures performed by the practitioner and results of those tests. Absent such information, the description provides the context necessary for users to understand the conclusions, expressed by management in its assertion and by the CPA in his or her report, about the effectiveness of the controls within the entity's cybersecurity risk management program.

As previously stated, management is responsible for preparing the description of the entity's cybersecurity risk management program. The description criteria in this document are used to prepare the description. When developing the description criteria, the AICPA considered the nature, type, and extent of cybersecurity information published by industry experts and requested by regulators and other potential report users. Examples of the information considered include the following:

- National Institute of Standards and Technology Framework for Improving Critical Infrastructure (NIST Cybersecurity Framework or NIST CSF)
- International Organization for Standardization (ISO)/IEC 27001/27002 and related standards
- U.S. Department of Homeland Security requirements for annual FISMA reporting
- FFIEC questionnaires
- COBIT 5
- COSO's *Internal Control—Integrated Framework* (COSO 2013 framework)
- HIPAA Security Rule
- PCI DSS 3.1
- NIST Special Publication 800 series
- HITRUST CSF

However, the AICPA did not believe that any individual source alone addressed all the elements of cybersecurity that might be useful to a variety of users when making informed decisions. Therefore, the description criteria presented in this document is derived from a variety of sources.

When developing the description criteria, the AICPA recognized the risk that users' need for useful information might result in disclosures that could be used by hostile parties to identify and exploit vulnerabilities in an entity's cybersecurity risk management program. Therefore, the AICPA considered those risks that could arise when developing the disclosures and attempted to balance those disclosures with the need to protect the entity's information and systems.

Guide for Respondents

ASEC is seeking comments specifically on the nature and extent of information and disclosures contained in the proposed description criteria. Specifically, respondents are asked to respond to the following questions:

1. Are there any unnecessary or otherwise not relevant description criteria or points of focus? Please provide a list.

2. Are there any missing description criteria or points of focus? Please provide a list.

3. Are there any description criteria or points of focus that would result in disclosure of information that would increase the risk of a security event? Please provide a list.

4. Do you have any concerns about the measurability of any of the description criteria or points of focus? Please provide a list.

5. The AICPA developed the description criteria and related points of focus using an approach similar to the one used by COSO when developing its *Integrated Framework—Internal Control*. Similar to the COSO approach, a description of the entity's cybersecurity risk management program prepared in accordance with the description criteria would include information about each of the criteria in this document. The points of focus related to the criteria are important characteristics of the criteria. Consistent with the COSO approach, management may determine that some of the points of focus are not suitable or relevant and may identify and consider other characteristics based on specific circumstances of the entity. *Points of focus* assist management in determining the matters to be addressed in the presentation. However, use of the criteria does not require management to address every point of focus in its description. Do you believe this approach is appropriate? If not, please describe the approach you would recommend.

Comments are most helpful when they refer to specific paragraphs or criteria numbers, include the reasons for the comments, and, when appropriate, make specific suggestions for any proposed changes to wording. When a respondent agrees with proposals in the exposure draft, it will be helpful for the working group to be made aware of this view, as well.

Written comments on the exposure draft should be sent to Mimi Blanco-Best at mblancobest@aicpa.org and received by December 5, 2016.

Comment Period

The comment period for this exposure draft ends December 5, 2016.

Assurance Services Executive Committee (2015–2016)

Robert Dohrer, *Chair*
Bradley Ames
Christine M. Anderson
Dorsey Baskin
Brad Beasley
Greg Bedard
Nancy Bumgarner
Mary Grace Davenport
Chris Halterman
Don Kluthe
Michael Ptasienski
Beth A. Schneider
Miklos Vasarhelyi
Deetra B. Watson

ASEC Cybersecurity Working Group

Chris Halterman,*Chair*
Efrim Boritz
Mark Burnette
Andrés Castañeda
Brian DePersiis
Sandy Herrygers
Eddie Holt
Kevin Knight
Guarav Kumar
Dave Palmer
Adam Ross
Rod Smith
Shahryar Shaghaghi
Jeff Trent
Jeff Ward
David Wood

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

Introduction

.01 The AICPA Assurance Services Executive Committee (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). The description criteria presented in this document are for use when preparing the description in the cybersecurity examination described in the cybersecurity attestation guide;[1] however, they also may be used when preparing, and evaluating the presentation of, a description in other types of engagements, such as those discussed in paragraph .13.

.02 The cybersecurity examination described in the cybersecurity attestation guide will be performed in accordance with the AICPA *Statements on Standards for Attestation Engagements*. Under those standards, an attestation engagement is predicated on the concept that a party other than the practitioner makes an assertion about whether the subject matter is measured or evaluated in accordance with suitable criteria. The attestation standards state that, in an examination engagement, the responsible party (generally, that is management in a cybersecurity examination engagement) takes responsibility for the subject matter.

.03 The *subject matter* of the cybersecurity examination includes the following:

- A description of the entity's cybersecurity risk management program in accordance with the description criteria.[2]

- An assessment of the effectiveness of the controls within that program to achieve the

[1] As of the date of publication, the cybersecurity attestation guide is under development. The guide will provide application and performance guidance for practitioners engaged to perform the cybersecurity examination developed by the AICPA. However, practitioners may be able to perform other types of examination engagements in accordance with the attestation standards. Although the guide will not address such examinations, practitioners may find the guidance useful in such situations.

[2] Because the description of the entity's cybersecurity risk management program is part of the subject matter in a cybersecurity examination, there is a risk that a cybersecurity report that does not contain a description could be misunderstood by users. For this reason, practitioners should consider carefully whether to perform an attestation engagement related to an entity's cybersecurity risk management program when the engagement does not include a description of the entity's cybersecurity risk management program prepared in accordance with the description criteria.

entity’s cybersecurity objectives based on the control criteria.

.04 Because management is ultimately responsible for the entity’s cybersecurity risk management program and the operation of the controls within that program, it is management’s responsibility to develop and present, in the cybersecurity report, a description of the entity’s cybersecurity risk management program. An entity’s *cybersecurity risk management program* is the set of policies, processes, and controls designed to protect information[3] and systems[4] from security events[5] that could compromise[6] 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.

.05 Management uses the description criteria when preparing the description of the entity’s cybersecurity risk management program (description); the practitioner uses the description criteria when evaluating whether the presentation is presented in accordance with the description criteria.

.06 Management is responsible for selecting the description criteria to be used in the cybersecurity examination. This document presents the description criteria for use when preparing the description of the entity’s cybersecurity risk management program.[7] It also presents points of focus that represent important characteristics of the criteria.

[3] As used here, the terms *information* and *systems* refer to information in electronic form (electronic information) during its use, processing, transmission and storage, and systems that use electronic information to process, transmit or transfer, and store information.

[4] For purposes of this paper, a *system* refers to a set of components designed, implemented, and operated to work together to achieve one or more specific business objectives (for example, delivery of services, production of goods) in accordance with management-specified requirements. System components can be classified into the following: infrastructure, software, people, processes, and data. The business definition of the term *system* is used, as opposed to its common usage, which refers to the components of a system (for example, computer systems, IT systems). Systems that have cybersecurity risks include manufacturing and production systems that are automated and partially automated (including the industrial control systems components of those systems), inventory management and distribution systems, as well as systems that perform support functions within an organization.

[5] A *security event* is an occurrence, arising either internally or externally, that could pose a threat to the availability, integrity, or confidentiality of information or systems from unauthorized access, result in unauthorized disclosure or theft of information or other assets, cause damage to systems, and so on.

[6] *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.

[7] At the time of issuance, there were no other description criteria for use when preparing the description of an entity’s cybersecurity risk management program.

.07 In establishing and developing these criteria, ASEC follows due process procedures, including exposure of criteria for public comment. BL section 360R, *Implementing Resolutions under Section 3.6 Committees* (AICPA, *Professional Standards*), designates ASEC as a senior technical committee with authority to make public statements and publish measurement criteria without clearance from AICPA council or the board of directors. Accordingly, ASEC has concluded that the description criteria are suitable criteria for use in the cybersecurity examination described in the cybersecurity attestation guide.

.08 In addition to the description of the entity's cybersecurity risk management program, the report issued as a result of the cybersecurity examination (referred to as the *cybersecurity report*) also will include management's assertion and the practitioner's opinion about whether the description is presented in accordance with the description criteria and whether the controls within that program are effective to achieve the entity's cybersecurity objectives based on the control criteria. This document does not present the control criteria against which to measure and evaluate the effectiveness of controls within an entity's cybersecurity risk management program.[8]

Professional Standards That Apply to the Cybersecurity Examination

.09 The cybersecurity examination is performed in accordance with AT-C section 105, *Concepts Common to All Attestation Engagements* (AICPA, *Professional Standards*), and AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*). Under those standards, the CPA performing an attest engagement is known as a *practitioner*. In an examination engagement, the practitioner provides a report in which he or she expresses an opinion on subject matter or an assertion about the subject matter in relation to an identified set of criteria.

.10 In a cybersecurity examination engagement, the practitioner expresses an opinion on whether the description of the entity's cybersecurity risk management program is presented in accordance with the description criteria and whether the controls within that program are effective to achieve the entity's cybersecurity objectives based on the control criteria. As stated in paragraph .04, the description and conclusion about the effectiveness of controls are the subject matter of the engagement. The description criteria presented in this document are used to evaluate the presentation of the description. (The control

[8] Management also is responsible for selecting the control criteria to be used in the engagement and may select any control criteria as long as it is considered suitable criteria for the engagement in accordance with the attestation standards.

criteria, which are used to evaluate the effectiveness of the controls included within the entity's risk management program, are not addressed in this document.)

.11 According to the attestation standards, the attributes of suitable criteria are as follows: [9]

- *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 decisions of the intended users made on the basis of that subject matter.

.12 In addition to being *suitable*, AT-C section 105[10] indicates that the criteria used in an attestation engagement should be available to users. The publication of the description criteria makes the criteria available to users.

.13 The description criteria also may be used when the practitioner is engaged to provide other nonattest or advisory services to a client in connection with the entity's cybersecurity risk management program. For instance, a practitioner may use such criteria when engaged to assist management with the development of its description of the entity's cybersecurity risk management program. In this situation, however, the representations in the description remain the responsibility of management.

.14 Due to the rapidly evolving nature of cybersecurity risks and the relative immaturity of cybersecurity risk management programs to address those risks, it is expected that early use of the description criteria will be to support the performance of consulting services in connection with an entity's cybersecurity risk management program. Consulting services are performed in accordance with the guidance in CS section 100*, Consulting Services: Definitions and Standards* (AICPA, *Professional Standards*).

.15 If the practitioner assists management with the development of its description, threats to the practitioner's independence may exist. The "Nonattest Services" interpretation (AICPA, *Professional Standards*, ET sec. 1.295), provides special independence requirements for practitioners who provide nonattest services for an attest client. In addition, The

[9] Paragraph .A42 of AT-C section 105, *Concepts Common to All Attestation Engagements* (AICPA, *Professional Standards*).
[10] Paragraph .25*b* of AT-C section 105.

"Conceptual Framework Approach" interpretation (AICPA, *Professional Standards*, ET sec. 1.210), discusses threats to independence not specifically detailed elsewhere.

Categories of Description Criteria

.16 The description criteria included in this document is categorized into the following sections:

a. *Nature of Operations*. Information about the nature of the entity's operations to enable report users to better understand subsequent information and disclosures related to the entity's cybersecurity risks and the controls management has implemented and operates to mitigate those risks.

b. *Nature of Information at Risk*. Information about the types of information the entity creates, uses, and stores that is susceptible to cybersecurity risk.

c. *Cybersecurity Risk Management Program Objectives* (*Cybersecurity Objectives*). Information about the entity's cybersecurity objectives and the process of developing and maintaining them.

d. *Inherent Risks Related to the Use of Technology.* Information about the characteristics of the entity's IT environment, including the technologies, connection types, and delivery channels used by the entity, that can help report users understand the complexity of the entity's IT environment and its effect on the entity's inherent cybersecurity risk.

e. *Cybersecurity Risk Governance Structure.* Information about the entity's cybersecurity risk governance structure, including the processes for communicating integrity and ethical values, board oversight, establishing accountability, and hiring and developing qualified personnel.

f. *Cybersecurity Risk Management Process.* Information related to the entity's process to assess its cybersecurity risks, including information related to the process management uses to identify the information assets and systems at risk and the external requirements that govern the security of that information; the identification and assessment of the types, likelihood, and impact of potential cybersecurity risks to the security of that information; and the determination of how best to manage those risks.

g. *Cybersecurity Communications and the Quality of Cybersecurity Information*. Information about the process the entity uses to communicate cybersecurity objectives, expectations, responsibilities, and related matters to both internal and external users, including the communication of identified security events to appropriate parties.

h. *Monitoring of the Cybersecurity Risk Management Program*. Information related to the process the entity uses to assess the effectiveness of the entity's controls included in its cybersecurity risk management program, including information about the corrective actions taken when security events, threats, vulnerabilities, and control weaknesses are identified.

i. *Cybersecurity Control Activities*. Summary descriptions of the controls the entity has designed, implemented, and operates (i) to protect information and systems from security events[11] that could compromise the achievement of the entity's cybersecurity objectives and (ii) to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented.

.17 The criteria sections are not mutually exclusive, and there may be some overlap among the criteria presented in each section. Accordingly, management has flexibility when determining in which section to describe its controls, as long as each criteria is adequately described in the presentation (that is, all 32 description criteria must be addressed).

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

.18 Management's description of the entity's cybersecurity risk management program is intended to provide users with information about an entity that will enable them to better understand the entity's cybersecurity risk management program. For example, the 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, will allow users to better understand the design of controls within the entity's cybersecurity risk management program. As such, while some of the criteria do not directly address an entity's cybersecurity risk management program, they provide a context that enables report users' to understand the cybersecurity information and disclosures presented elsewhere in the report (including the assertion provided by management and the opinion provided by the practitioner about the

[11] A *security event* is an occurrence, arising either internally or externally, that could pose a threat to the availability, integrity, or confidentiality of information or systems from unauthorized access, result in unauthorized disclosure or theft of information or other assets, cause damage to systems, and so on.

effectiveness of controls within the program to achieve the entity's cybersecurity objectives based on the control criteria).

.19 For the description to be presented in accordance with the description criteria, all the information and disclosures called for in the description criteria should be included in the presentation. In addition, each of the relevant elements required by the criteria should be adequately described or disclosed.

.20 The description may be presented using various formats, such as narratives, flowcharts, tables, or graphics, or a combination thereof. Furthermore, unless specifically required by the description criteria, disclosures need not be quantified. The degree of detail to be included in the description generally is a matter of judgment; management is not required to describe elements in such a detailed manner that it would compromise the entity's cybersecurity controls. For example, when summary descriptions of controls are requested by a criterion, such descriptions are required only to contain sufficient information about the controls the entity has designed and implemented to enable intended users to understand whether it is likely that the entity's controls would sufficiently address the risks that threaten the achievement of the entity's cybersecurity objectives.

.21 In addition to the description criteria, this document also presents points of focus related to each criteria. Similar to the points of focus in *Internal Control—Integrated Framework* revised in 2013 by the Committee of Sponsoring Organizations of the Treadway Commission (COSO 2013 framework), the points of focus are important characteristics of the criteria. Consistent with the COSO approach, management may determine that some of these points of focus are not suitable or relevant and may identify and consider other characteristics based on specific circumstances of the entity. Points of focus assist management in determining the matters to be addressed in the presentation. However, use of the criteria does not require management to address every point of focus in its description.

Tailoring and Disclosing the Cybersecurity Objectives

.22 In the cybersecurity examination, the entity's *cybersecurity objectives* are those that could be affected by cybersecurity risks and, therefore, affect the achievement of the entity's compliance, reporting, and operations objectives. Accordingly, understanding the entity's cybersecurity objectives is integral to the assessment and evaluation of whether controls are effective based on the control criteria.

.23 The nature of an entity's cybersecurity objectives will vary depending on the environment in which the entity operates, the entity's mission and vision, the overall business objectives established by management, and other factors. For example, a telecommunication entity may have a cybersecurity objective related to the reliable functioning of those aspects of its operations that are deemed to be critical infrastructure, whereas an online dating entity is likely to regard the privacy of the personal information collected from customers to be a critical factor in achieving its operating objectives. However, most organizations generally have a number of cybersecurity objectives in common.

.24 For that reason, intended users have to understand what the entity's cybersecurity objectives are and how they affect the evaluation of whether controls are suitably designed and operating effectively to meet the control criteria to achieve those objectives. Description criterion #3 (and related points of focus) presents a listing of cybersecurity objectives that typically apply to all entities. Management is expected to tailor those objectives to reflect the nature of the entity's business and the industry in which it operates and then to disclose them in the description of the entity's cybersecurity risk management program.

Applying the Description Criteria When the Scope of the Cybersecurity Examination Is Less Than Entity Wide

.25 The description criteria are designed to be flexible and result in a presentation that meets the business and assurance needs of users and management. Accordingly, although the description criteria were developed to describe an entity-wide cybersecurity risk management program, they also may be used when preparing and evaluating a description of a more limited cybersecurity risk management program. For example, they may be used when preparing and evaluating a description for

- 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; or
- one or more specific sets of systems or particular sets of information used by the entity.

.26 In those situations, the content of management's description should be tailored to specifically address the particular business unit, segment, or type of information addressed by the cybersecurity risk management program included within the scope of the engagement. Additional information on how the criteria might be tailored in such circumstances will be provided in the cybersecurity attestation guide.

Description Criteria and Related Points of Focus

NATURE OF OPERATIONS

DC1: The nature of the entity’s operations, including the principal products or services the entity sells or provides and the methods by which they are distributed

The following points of focus highlight important characteristics relating to this criterion:

- The entity’s principal markets, including the 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 (that is, sales, revenue, and so on)
- Changes to the entity’s principal products, services, or distribution methods during the past 12 months

NATURE OF INFORMATION AT RISK

DC2: The types of information created, collected, transmitted, used, or stored by the entity to support its operations, business objectives, and mission

The following points of focus highlight important characteristics relating to this criterion:

- 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 cardholder data)
- External party (entity) information that warrants protection based on law, commitment, or reasonable expectation of confidentiality
- Entity information (for example, trade secrets, corporate strategy, and operational data) or other information, included in any of the preceding categories, whose integrity is critical to the entity

CYBERSECURITY RISK MANAGEMENT PROGRAM OBJECTIVES (*CYBERSECURITY OBJECTIVES*)

DC3: The entity’s cybersecurity risk management program objectives (cybersecurity objectives)

The following points of focus highlight important characteristics relating to this criterion:

- Matters to be considered when developing cybersecurity objectives include the following:
    1. 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, critical infrastructure, and extended supply chains
    2. 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)
    3. Commitments made as part of a certification and authorization process for government agencies and other parties
    4. 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)
    5. Other business initiatives

- The following cybersecurity objectives are tailored to reflect the nature of the entity's business and the industry in which it operates.

Availability

Ensuring timely, reliable, and continuous access to and use of information and systems 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
- 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;
- 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 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 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
- Safeguarding of life and health

DC4: The process for developing and maintaining cybersecurity objectives to support the achievement of the entity's objectives

The following points of focus highlight important characteristics relating to this criterion:

- The security management and control framework or combination thereof used by management to develop and maintain controls within the entity's cybersecurity risk management program (for example, NIST Cybersecurity Framework, ISO 27001/2, and so on)
- The process for establishing cybersecurity objectives based on the entity's objectives established by the board of directors and management

INHERENT RISKS RELATED TO THE USE OF TECHNOLOGY

DC5: Inherent cybersecurity risk characteristics arising from the technologies, connection types, and delivery channels used by the entity

The following points of focus highlight important characteristics relating to this criterion:

- Use of cloud computing and IT-hosted services (at the infrastructure level)
- Use of mobile devices, platforms, and deployment approaches
- Network architecture and strategy
- Types of application and infrastructure (that is, DB, OS types and technologies)

- Types of external party access and connectivity to environment and sensitive data, including the type and nature of outsourced service providers that store, process, and transmit or access systems
- Nature of external-facing web applications and the nature of applications developed in-house
- Dependency on strategically significant IT equipment and systems that are outdated or unsupported, or both

DC6: Organizational characteristics that could affect the entity’s inherent cybersecurity risk

The following points of focus highlight important characteristics relating to this criterion:

- IT organization size and structure (for example, centralized vs. decentralized, insourced or outsourced)
- Types of user groups (for example, employees, vendors, business partners, and so on)
- Whether the entity’s information assets exist in nations 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 and IT
- Business units with IT systems administered under a separate management structure (for example, outside of a centralized IT function)

DC7: Changes at the entity that could affect the entity’s inherent cybersecurity risk

The following points of focus highlight important characteristics relating to this criterion:

- Changes to business unit, IT, and security personnel that have, or are reasonably likely to have, a significant effect on the entity’s cybersecurity risk management program and related controls
- Significant changes to entity processes, IT architecture, and applications during the past 12 months
- Acquisitions during the past 12 months that have, or are reasonably likely to have, a significant effect on the entity’s cybersecurity risk management program and related controls, the integration or segmentation strategy used for the acquiree’s IT systems, and the current state of those activities

- Acquisitions prior to the past 12 months that have, or are reasonably likely to have, a significant effect on the entity's cybersecurity risk management program and related controls for which integration is not yet complete

- Divestures for the past 12 months that have, or are reasonably likely to have, a significant effect on the entity's cybersecurity risk management program and related controls, the ongoing service support of those systems (if any), and the current status of those activities

DC8: Information about security incidents identified within the 12-month period ended on the date of management's description in each of the following categories:

a. **Total number of incidents, including the mean time from first occurrence to detection**

b. **Total number of incidents requiring remediation and total number of incidents resulting in a loss (financial or data), including the following:**

i. Types of data or system affected

ii. Mean time from first occurrence to detection

iii. Mean time from detection to remediation

iv. Nature of event and resulting loss

The following point of focus highlights important characteristics relating to this criterion:

- Disclosure of the nature of the event and resulting loss may need to give consideration to legal and regulatory restrictions on such disclosures

CYBERSECURITY RISK GOVERNANCE STRUCTURE

DC9: The process for communicating integrity and ethical values to support the functioning of the cybersecurity risk management program

The following points of focus highlight important characteristics relating to this criterion:

- 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

DC10: The process for board oversight of the entity's cybersecurity risk management program

The following points of focus highlight important characteristics relating to this criterion:

- 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

DC11: Established cybersecurity accountability and reporting lines

The following points of focus highlight important characteristics relating to this criterion:

- 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) who reports to an appropriate member of executive management, if any
- The roles and responsibilities of entity personnel who perform cybersecurity controls and activities, including line-of-defense roles
- The process for considering external parties when establishing structures, reporting lines, authorities, and responsibilities

DC12: The process used to hire, develop, and retain competent individuals and contractors with cybersecurity control responsibilities

The following points of focus highlight important characteristics relating to this criterion:

- The process for considering the competence of qualified personnel with cybersecurity responsibilities, including the performance of background checks, assessment of educational levels, 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 addressing and communicating identified cybersecurity threats, vulnerabilities, and control weaknesses

DC13: The process for holding individuals accountable for their cybersecurity responsibilities

The following points of focus highlight important characteristics relating to this criterion:

- The process used to communicate and hold individuals accountable for the performance of their responsibilities

- The process to monitor communication and accountability mechanisms and employee compliance with their responsibilities

- 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 MANAGEMENT PROCESS

DC14: The process for identifying risks to the achievement of the entity's cybersecurity objectives and assessing risks to determine how such risks should be managed

The following points of focus highlight important characteristics relating to this criterion:

- The use of inventory management to classify the entity's information assets and systems according to its nature and sensitivity

- How the process includes the consideration of the types, likelihood, and impact of risks to information assets and systems, including manufacturing and industrial control systems, from potential threats arising from the following:

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

- Obtaining threat and vulnerability information from information-sharing forums and other sources

DC15: The process for assessing and managing the risks associated with vendors and business partners

The following points of focus highlight important characteristics relating to this criterion:

- The process for identifying external parties affecting the entity’s cybersecurity risk management and maintaining an inventory of those parties
- How the entity manages risks to its cybersecurity objectives associated with vendors and business partners, including the following:
    - i. 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
    - ii. Assessing, on a periodic basis, the risks that the vendor and its business partners represent to the achievement of the entity's objectives
    - iii. Assigning responsibility and accountability for the management of associated risks
    - iv. Establishing communication and resolution protocols for service and product issues
    - v. Establishing exception-handling procedures
    - vi. Periodically assessing the performance of vendors and their business partners
    - vii. Implementing procedures for addressing associated risks

DC16: The process for identifying and assessing changes that could significantly affect the design and operating effectiveness of the entity’s cybersecurity controls

The following points of focus highlight important characteristics relating to this criterion:

- Changes to the regulatory, economic, and physical environment in which the entity operates
- How the process addresses the impact on the entity’s cybersecurity risk management program of new business lines, dramatically altered compositions of existing business lines, changes in available resources, acquired or divested business operations, rapid growth, changing reliance on foreign geographies, and new technologies
- The process for performing ad hoc risk assessments

CYBERSECURITY COMMUNICATIONS AND QUALITY OF CYBERSECURITY INFORMATION

DC17: The process for internally communicating relevant cybersecurity information necessary to support the functioning of the entity’s cybersecurity risk management program, including (*a*) objectives and responsibilities for cybersecurity, and (*b*) thresholds for communicating identified security events that are (i) actively monitored and investigated and (ii) determined to be security incidents requiring a response or remediation, or both

The following points of focus highlight important characteristics relating to this criterion:

- Methods used to communicate to personnel information to enable them to understand and carry out their cybersecurity responsibilities (for example, through the use of
    - i. awareness programs, including training about detecting and avoiding social engineering threats and security breach reporting and response
    - ii. job descriptions
    - iii. acknowledgement of code of conduct and policies, and
    - iv. policy and procedures manuals.)

- Communications made between management and the board of directors to enable each to have information needed to fulfill their roles

- The process by which timing, audience, and nature of information are addressed when selecting the communication method to be used

- The use of separate communication channels, such as whistle-blower hotlines, to enable anonymous or confidential communication when normal channels are inoperative or ineffective

DC18: The process for communicating with external parties regarding matters affecting the functioning of the entity’s cybersecurity risk management program

The following points of focus highlight important characteristics relating to this criterion:

- Information communicated to external parties, such as shareholders, partners, owners, regulators, customers, and financial analysts and other external parties

- The existence and use of open communication channels that allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others to provide management and the board of directors with relevant information

- Communications of relevant information made by external parties, either as a result of assessments or other basis, to the board of directors

- The use of separate 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 are considered when making communications

DC19: The process for obtaining, generating, and using relevant, quality information to support the functioning of the entity’s cybersecurity risk management program

The following points of focus highlight important characteristics relating to this criterion:

- The process used to identify information required and expected to support the achievement of the entity’s cybersecurity objectives
- Key communications made to management regarding the operation of the entity’s cybersecurity risk management program
- The use of external sources of data
- The capture and use of metrics to measure the effectiveness of the cybersecurity risk management program
- The processes in place to produce cybersecurity information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained.
- The nature, quantity, and precision of information communicated to support the achievement of the entity’s objectives

MONITORING OF THE CYBERSECURITY RISK MANAGEMENT PROGRAM

DC20: The process for conducting ongoing and periodic separate evaluations to evaluate the operating effectiveness of key control activities and other components of internal control

The following points of focus highlight important characteristics relating to this criterion:

- The variety of different types of ongoing and separate evaluations used, including penetration testing, independent certificates made against established specifications (for example, HITRUST and ISO 27001), and internal audit assessments
- 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 separate evaluations, including whether (*a*) the design and current state of the entity’s cybersecurity risk management program, including the controls, is 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 varied depending on risk

DC21: The process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control weaknesses to parties responsible for taking corrective actions, including management and the board of directors, as appropriate

The following points of focus highlight important characteristics relating to this criterion:

- The process by which management and the board of directors, as appropriate, assess results of ongoing and separate evaluations, including whether the process considers the remediation of identified security threats, vulnerabilities, and control weaknesses on a timely basis
- The process for communicating identified security threats, vulnerabilities, and control weaknesses to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate

CYBERSECURITY CONTROL ACTIVITIES

DC22: The entity's IT infrastructure and its network architecture

The following point of focus highlights important characteristics relating to this criterion:

- 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

DC23: The security policies that define expected security controls and user behavior as an authoritative source for the implementation of control activities

The following points of focus highlight important characteristics relating to this criterion:

- The existence of a formal security policy established to implement the entity's cybersecurity strategy
- Key topics addressed by the security policy

DC24: The process for designing and implementing controls to protect information assets and systems and to detect, respond to, mitigate, and recover from security events based on the assessed risks

The following points of focus highlight important characteristics relating to this criterion:

- The process used to develop a risk response (risk treatment plan) based on the results of the risk assessment

- The process to ensure that controls align with risk responses needed to address and mitigate assessed cybersecurity 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 activities

- The relevant business processes that require control activities

- The process for ensuring that risk mitigation activities include a range and variety of controls (for example, manual and automated controls, preventive and detective controls, and so on) to achieve a balanced approach to the mitigation of identified cybersecurity risks

DC25: A summary description of the nature of the controls in place to prevent intentional and unintentional security events

The following point of focus highlights important characteristics relating to this criterion:

- A summary of preventive controls, including those over the following:
  i. Protection of data-at-rest
  ii. Protection of data during processing
  iii. Protection of data-in-transit within the entity and between the entity and external parties
  iv. Data loss prevention
  v. User identification, authentication, authorization, and credentials management
  vi. Physical and logical access provisioning and de-provisioning, including remote access
  vii. Privileged account management
  viii. IT asset management, including hardware and software commissioning, configuration, maintenance, and decommissioning as well as physical and logical servers and other devices
  ix. Capacity management
  x. Back up of data and software
  xi. Data destruction
  xii. Operating location and data center physical security and environmental safeguards
  xiii. Monitoring and managing changes to systems made internally or by external parties, including software acquisition, development, and maintenance and patch management
  xiv. Security training and awareness programs
  xv. Separation of incompatible functions

DC26: A summary description of the controls used to detect security events

The following points of focus highlight important characteristics relating to this criterion:

- The deployment of tools and programs, the implementation of monitoring processes and procedures, or operation of other measures to identify anomalies in information flow, access, data communications, and the operation of the system

- The process for analyzing anomalies to identify security events
- The process for users to escalate identified security events through the course of business operations and ongoing communications both within and outside the organization

DC27: A summary description of the measures to identify security incidents, develop a response to those incidents, and implement activities to mitigate and recover from identified security incidents

The following points of focus highlight important characteristics relating to this criterion:

- 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 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 recovers operations from identified security incidents
- The process by which the incident response plan is updated based on the analysis of lessons learned
- The process used to make communications to management about the security incident, including the nature of the incident, restoration actions taken, and activities required for future prevention of the event
- The process used to make communications to affected third parties about the security incident
- The process for periodically testing the incident response plan

DC28: A summary description of the controls used to monitor current processing capacity usage and enable the implementation of additional capacity

The following points of focus highlight important characteristics relating to this criterion:

- 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

DC29: A summary description of the measures to detect and mitigate environmental threat events and back-up procedures to support system availability

The following points of focus highlight important characteristics relating to this criterion:

- 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 process for backing up data to support continued availability in the event of the destruction of data within systems
- Steps taken to provide for alternate processing infrastructure in the event of normal processing infrastructure becoming unavailable

DC30: A summary description of the measures to identify confidential information when received or created, determine the retention period for that information, and retain the information for the specified period

The following points of focus highlight important characteristics relating to this criterion:

- 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 preventing the destruction of identified information during its specified retention period

DC31: A summary description of the measures to identify confidential information at the end of its specified retention period and the process for destroying that information

The following points of focus highlight important characteristics relating to this criterion:

- 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

.27 The description criteria are effective when issued.

.28

Appendix A—Glossary

access to personal information. The ability to view personal information held by an organization. This ability may be complemented by an ability to update or correct the information. Access defines the intersection of identity and data, that is, who can do what to which data. Access is one of the fair information practice principles. Individuals must be able to find out what personal information an entity has on file about them and how the information is being used. Individuals must 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 to verify 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. Governing body of an entity, which may take the form of a board of directors or supervisory board for a corporation, board of trustees for a not-for-profit organization, board of governors or commissioners for government entities, general partners for a partnership, or 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 objectives. The practitioner need only consider commitments related to the objectives addressed within the scope of the engagement. 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 examination. An examination engagement to report on whether (*a*) management's description of the entity's cybersecurity risk management program is fairly presented in accordance with the description criteria and (*b*) the controls included in that program were suitably designed and operated effectively to provide reasonable assurance that the control criteria were met to achieve the entity's cybersecurity objectives throughout the specified period. A cybersecurity examination is performed in accordance with the AICPA attestation standards and the AICPA cybersecurity attestation guide.

design. (1) Intent; as used in the definition of **internal control**, the internal control system design is intended to provide reasonable assurance of the achievement of objectives; when the intent is realized, the system can be deemed effective. (2) Plan; the way a system is supposed to work, contrasted with how it actually works.

disclosure. The release, transfer, provision of access to, or divulging 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 parts of the information system (for example, protections from fire, flood, wind, earthquake, power surge, or power outage).

entity. A legal entity or management operating model of any size established for a particular purpose. A legal entity may, for example, be a business enterprise, not-for-profit organization, government body, or academic institution. The management operating model may follow product or service lines, division, or operating unit, 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.

ethical values. Moral values that enable a decision-maker to determine an appropriate course of behavior; these values should be based on what is right, which may go beyond what is legal.

information and systems. Refers to information in electronic form (electronic information) during its use, processing, transmission and storage, and systems that use electronic information to process, transmit or transfer, and store information.

information assets. Data and the associated software and infrastructure used to process, transmit, and store it.

infrastructure. The collection of physical or virtual resources that supports an overall IT environment, including the server, storage, and network components.

inherent risk. The risk to the achievement of objectives in the absence of any actions management might take to alter either the risk likelihood or impact.

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.

organization. People, including the board of directors, senior management, and other personnel.

outsourced service providers. A vendor that the entity has engaged to perform business processes or operations that would otherwise be performed by the entity.

personal information. Information that is, or can be about or related to, an identifiable individual.

policy. Management or board member statement of what should be done to effect control. Such statements may be documented, explicitly stated in communications, or implied through actions and decisions. A policy serves as the basis for procedures.

report users (or users). Intended users of the practitioner's report in accordance with AT-C section 205, *Examination Engagements* (AICPA, *Professional Standards*). Report users may be the general public or may be restricted to specified parties in accordance with paragraph .64 of AT-C section 205. In the cybersecurity examination, the practitioner's report is included in the cybersecurity report, along with the description of the entity's cybersecurity risk management program and management's assertion.

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 either internally or externally, that could pose a threat to the availability, integrity, or confidentiality of information or systems from unauthorized access, result in unauthorized disclosure or theft of information or other assets, cause damage to systems, and so on.

security incident. A security event that requires action on the part of an entity in order to protect assets and resources.

senior management. The CEO or equivalent organizational leader and senior management team.

system. Refers to a set of components designed, implemented, and operated to work together to achieve one or more specific business objectives (for example, delivery of services, production of goods) in accordance with management-specified requirements. System components can be classified into the following: infrastructure, software, people, processes, and data. The business definition of the term *system* is used as opposed to the common usage, which refers to the components of a system (for example, computer systems, IT systems).

third party. A person or organization other than the entity and its employees or the user of the report. Third parties may be customers, business partners, government agency personnel, vendors, 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.