SOC 2 Trust Services Criteria

The following tables present the trust services criteria and the related points of focus.

In the table, criteria and related points of focus that come directly from the COSO framework are presented using a normal font.

In contrast, supplemental criteria and points of focus that apply to engagements using the trust services criteria are presented in *italics.*

Finally, criteria and points of focus that apply only when engagements using the trust services criteria are performed at a system level are presented in ***bold italics***.

This may look a bit daunting at first but take note that you will not use all of these. They are a guideline for you to select from as they fit into your business. They also serve as a guide to add controls where you may be lacking them today.

CONTROL ENVIRONMENT CC1.1

COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.

Points of focus:

- Sets the Tone at the Top — The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.
- Establishes Standards of Conduct — The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity’s standards of conduct and understood at all levels of the entity and by out sourced service providers and business partners.
- Evaluates Adherence to Standards of Conduct — Processes are in place to evaluate the performance of individuals and teams against the entity’s expected standards of conduct.
- Addresses Deviations in a Timely Manner — Deviations from the entity’s expected standards of conduct are identified and remedied in a timely and consistent manner.

Additional point of focus:

- *Considers Contractors and Vendor Employees in Demonstrating Its Commitment — Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.*

CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.

Points of focus:

- Establishes Oversight Responsibilities — The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.
- Applies Relevant Expertise — The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of senior management and take commensurate action.
- Operates Independently — The board of directors has sufficient members who are independent from management and objective in evaluations and decision making.

CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.

Points of focus:

- *Supplements Board Expertise — The board of directors supplements its expertise relevant to security, availability, processing integrity, confidentiality, and privacy, as needed, through the use of a subcommittee or consultants.*

- Considers All Structures of the Entity — Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and out sourced service providers) to support the achievement of objectives.

- Establishes Reporting Lines — Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.

- Defines, Assigns, and Limits Authorities and Responsibilities — Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.

Additional points of focus:

- *Addresses Specific Requirements When Defining Authorities and Responsibilities — Management and the board of directors consider requirements relevant to security, availability, processing integrity, confidentiality, and privacy when defining authorities and responsibilities.*

- *Considers Interactions With External Parties When Establishing Structures, Report- ing Lines, Authorities, and Responsibilities — Management and the board of direc- tors consider the need for the entity to interact with and monitor the activities of ex- ternal parties when establishing structures, reporting lines, authorities, and respon- sibilities.*

CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain com- petent individuals in alignment with objectives.

Points of focus:

- Establishes Policies and Practices — Policies and practices reflect expectations of competence necessary to support the achievement of objectives.

- Evaluates Competence and Addresses Shortcomings — The board of directors and management evaluate competence across the entity and in out sourced service providers in relation to established policies and practices and act as necessary to ad- dress shortcomings.

- Attracts, Develops, and Retains Individuals — The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and out sourced service providers to support the achievement of objectives.

- Plans and Prepares for Succession — Senior management and the board of directors develop contingency plans for assignments of responsibility important for internal control.

Additional point of focus::

- *Considers the Background of Individuals — The entity considers the background of potential and existing personnel, contractors, and vendor employees when deter- mining whether to employ and retain the individuals.*

- *Considers the Technical Competency of Individuals — The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.*

- *Provides Training to Maintain Technical Competencies — The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.*

CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsi- bilities in the pursuit of objectives.

The following points of focus:

- Enforces Accountability Through Structures, Authorities, and Responsibilities — Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.

- Establishes Performance Measures, Incentives, and Rewards — Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.

- Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance — Management and the board of directors align incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.

- Considers Excessive Pressures — Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.

- Evaluates Performance and Rewards or Disciplines Individuals — Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and

COMMUNICATION AND INFORMATION

CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.

The following points of focus:

- Identifies Information Requirements — A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.

- Captures Internal and External Sources of Data — Information systems capture internal and external sources of data.

- Processes Relevant Data Into Information — Information systems process and transform relevant data into information.

- Maintains Quality Throughout Processing — Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.

CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.

The following points of focus:

- Communicates Internal Control Information — A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.

- Communicates With the Board of Directors — Communication exists between management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.

- Provides Separate Communication Lines — Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.

- Selects Relevant Method of Communication — The method of communication considers the timing, audience, and nature of the information.

Additional points of focus:

- *Communicates Responsibilities — Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.*

- *Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters — Entity personnel are provided with information on how to* *report systems failures, incidents, concerns, and other complaints to personnel.*

• *Communicates Objectives and Changes to Objectives — The entity communicates its objectives and changes to those objectives to personnel in a timely manner.*

• *Communicates Information to Improve Security Knowledge and Awareness — The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.*

Additional points of focus:

• ***Communicates Information About System Operation and Boundaries — The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to under- stand their role in the system and the results of system operation.***

• ***Communicates System Objectives — The entity communicates its objectives to personnel to enable them to carry out their responsibilities.***

CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

The following points of focus:

• ***Communicates System Changes — System changes that affect responsibilities or the achievement of the entity's objectives are communicated in a timely manner.***

• Communicates to External Parties — Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.

• Enables Inbound Communications — Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing management and the board of directors with relevant in- formation.

• Communicates With the Board of Directors — Relevant information resulting from assessments conducted by external parties is communicated to the board of directors.

• Provides Separate Communication Lines — Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.

• Selects Relevant Method of Communication — The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.

Additional point of focus:

- *Communicates Objectives Related to Confidentiality and Changes to Objectives — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives and changes to objectives related to confidentiality.*
- *Communicates Objectives Related to Privacy and Changes to Objectives — The entity communicates, to external users, vendors, business partners, and others whose products and services are part of the system, objectives related to privacy and changes to those objectives.*

- ***Communicates Information About System Operation and Boundaries — The en- tity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation.***
- ***Communicates System Objectives — The entity communicates its system objectives to appropriate external users.***
- ***Communicates System Responsibilities — External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive communications about their responsibilities and have the in- formation necessary to carry out those responsibilities.***
- ***Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters — External users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.***

RISK ASSESSMENT

CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identifica- tion and assessment of risks relating to objectives.

The following points of focus:

- Reflects Management's Choices — Operations objectives reflect management's choices about structure, industry considerations, and performance of the entity.

- Considers Tolerances for Risk — Management considers the acceptable levels of variation relative to the achievement of operations objectives.

- Includes Operations and Financial Performance Goals — The organization reflects the desired level of operations and financial performance for the entity within operations objectives.

- Forms a Basis for Committing of Resources — Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.

External Financial Reporting Objectives

- Complies With Applicable Accounting Standards — Financial reporting objectives are consistent with accounting principles suitable and available for that entity. The accounting principles selected are appropriate in the circumstances.

- Considers Materiality — Management considers materiality in financial statement presentation.

- Reflects Entity Activities — External reporting reflects the underlying transactions and events to show qualitative characteristics and assertions.

External Nonfinancial Reporting Objectives

- Complies With Externally Established Frameworks — Management establishes objectives consistent with laws and regulations or standards and frameworks of recognized external organizations.

- Considers the Required Level of Precision — Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.

- Reflects Entity Activities — External reporting reflects the underlying transactions and events within a range of acceptable limits.

Internal Reporting Objectives

- Reflects Management's Choices — Internal reporting provides management with accurate and complete information regarding management's choices and information

- Considers the Required Level of Precision — Management reflects the required level of precision and accuracy suitable for user needs in nonfinancial reporting objectives and materiality within financial reporting objectives.

- Reflects Entity Activities — Internal reporting reflects the underlying transactions and events within a range of acceptable limits.

Compliance Objectives

- Reflects External Laws and Regulations — Laws and regulations establish mini- mum standards of conduct, which the entity integrates into compliance objectives.

- Considers Tolerances for Risk — Management considers the acceptable levels of variation relative to the achievement of operations objectives.

Additional point of focus:

- *Establishes Sub-objectives to Support Objectives — Management identifies sub- objectives related to security, availability, processing integrity, confidentiality, and privacy to support the achievement of the entity's objectives related to reporting, operations, and compliance.*

CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the enti- ty and analyzes risks as a basis for determining how the risks should be managed.

The following points of focus:

- Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels — The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.

- Analyzes Internal and External Factors — Risk identification considers both internal and external factors and their impact on the achievement of objectives.

- Estimates Significance of Risks Identified — Identified risks are analyzed through a process that includes estimating the potential significance of the risk.

- Determines How to Respond to Risks — Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.

Additional points of focus:

- *Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities — The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.*

- *Analyzes Threats and Vulnerabilities From Vendors, Business Partners, and Other Parties — The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and* *vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.*

• *Considers the Significance of the Risk — The entity's consideration of the potential significance of the identified risks includes (1) determining the criticality of identi- fied assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticali- ty, threat impact, and likelihood.*

CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.

Points of focus:

• Assesses Incentives and Pressures — The assessment of fraud risks considers incen- tives and pressures.

• Assesses Opportunities — The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts.

• Assesses Attitudes and Rationalizations — The assessment of fraud risk considers how management and other personnel might engage in or justify inappropriate ac- tions.

• *Considers the Risks Related to the Use of IT and Access to Information — The assessment of fraud risks includes consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information.*

• Assesses Changes in the External Environment — The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.

• Assesses Changes in the Business Model — The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.

• Assesses Changes in Leadership — The entity considers changes in management and respective attitudes and philosophies on the system of internal control.

Additional point of focus:

• *Assesses Changes in Systems and Technology — The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.*

• *Assesses Changes in Vendor and Business Partner Relationships — The risk identification process* *considers changes in vendor and business partner relationships.*

MONITORING ACTIVITIES

CC4.1 COSO Principle 16*:* The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

The following points of focus:

- Considers a Mix of Ongoing and Separate Evaluations — Management includes a balance of ongoing and separate evaluations.

- Considers Rate of Change — Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.

- Establishes Baseline Understanding — The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.

- Uses Knowledgeable Personnel — Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.

- Integrates With Business Processes — Ongoing evaluations are built into the business processes and adjust to changing conditions.

- Adjusts Scope and Frequency — Management varies the scope and frequency of separate evaluations depending on risk.

Additional point of focus:

- Objectively Evaluates — Separate evaluations are performed periodically to provide objective feedback.

- *Considers Different Types of Ongoing and Separate Evaluations — Management uses a variety of different types of ongoing and separate evaluations, including pen- etration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.*

CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

The following points of focus:

- Assesses Results — Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.

- Communicates Deficiencies — Deficiencies are communicated to parties responsible for taking corrective action and to senior management and the board of directors, as appropriate.

- Monitors Corrective Action — Management tracks whether deficiencies are remedied on a timely basis.

CONTROL ACTIVITIES

CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mit- igation of risks to the achievement of objectives to acceptable levels.

The following points of focus:

- Integrates With Risk Assessment — Control activities help ensure that risk responses that address and mitigate risks are carried out.
- Considers Entity-Specific Factors — Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.
- Determines Relevant Business Processes — Management determines which relevant business processes require control activities.
- Evaluates a Mix of Control Activity Types — Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.
- Considers at What Level Activities Are Applied — Management considers control activities at various levels in the entity.
- Addresses Segregation of Duties — Management segregates incompatible duties and, where such segregation is not practical, management selects and develops alternative control activities.

CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.

The following points of focus:

- Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls — Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.
- Establishes Relevant Technology Infrastructure Control Activities — Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.
- Establishes Relevant Security Management Process Controls Activities — Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity’s assets from external threats.
- Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities — Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management’s objectives.

CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

The following points of focus:

- Establishes Policies and Procedures to Support Deployment of Management's Directives — Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.

- Establishes Responsibility and Accountability for Executing Policies and Procedures — Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or func- tion in which the relevant risks reside.

- Performs in a Timely Manner — Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.

- Takes Corrective Action — Responsible personnel investigate and act on matters identified as a result of executing control activities.

- Performs Using Competent Personnel — Competent personnel with sufficient authority perform control activities with diligence and continuing focus.

- Reassesses Policies and Procedures — Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.

Logical and Physical Access Controls

CC6.1 ***The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.***

The following points of focus:

- *Restricts Logical Access — Logical access to information assets, including hard- ware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.*

- *Identifies and Authenticates Users — Persons, infrastructure, and software are identified and authenticated prior to accessing information assets, whether locally or remotely.*

- *Considers Network Segmentation — Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.*

- *Manages Points of Access — Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.*

- *Restricts Access to Information Assets — Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access-control rules for information assets.*

- *Manages Identification and Authentication — Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure, and software.*

- *Manages Credentials for Infrastructure and Software — New internal and external infrastructure and software are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required or the infrastructure and software are no longer in use.*

- *Uses Encryption to Protect Data — The entity uses encryption to supplement other measures used to protect data at rest, when such protections are deemed appropriate based on assessed risk.*

- *Protects Encryption Keys — Processes are in place to protect encryption keys during generation, storage, use, and destruction.*

CC6.2 ***Prior to issuing system credentials and granting system access, the entity registers and authorizes*** Page

The following points of focus:

- ***new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.***

- *Controls Access Credentials to Protected Assets — Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.*

- *Removes Access to Protected Assets When Appropriate — Processes are in place to remove credential access when an individual no longer requires such access.*

- *Reviews Appropriateness of Access Credentials — The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.*

CC6.3 ***The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving con- sideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.***

The following points of focus:

- *Creates or Modifies Access to Protected Information Assets — Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.*

- *Removes Access to Protected Information Assets — Processes are in place to remove access to protected information assets when an individual no longer requires access.*

- *Uses Role-Based Access Controls — Role-based access control is utilized to sup- port segregation of incompatible functions.*

- *Reviews Access Roles and Rules — The appropriateness of access roles and access rules is reviewed on a periodic basis for unnecessary and inappropriate individuals with access and access rules are modified as appropriate.*

CC6.4 ***The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.***

The following points of focus:

- *Creates or Modifies Physical Access — Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on authorization from the system's asset owner.*
- *Removes Physical Access — Processes are in place to remove access to physical resources when an individual no longer requires access.*
- *Reviews Physical Access — Processes are in place to periodically review physical access to ensure consistency with job responsibilities.*

CC6.5 ***The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.***

The following points of focus:

- *Identifies Data and Software for Disposal — Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.*
- *Removes Data and Software From Entity Control — Procedures are in place to re- move data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.*

CC6.6 ***The entity implements logical access security measures to protect against threats from sources out- side its system boundaries.***

The following points of focus:

- *Restricts Access — The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.*
- *Protects Identification and Authentication Credentials — Identification and authentication credentials are protected during transmission outside its system boundaries.*
- *Requires Additional Authentication or Credentials — Additional authentication in- formation or credentials are required when accessing the system from outside its boundaries.*
- *Implements Boundary Protection Systems — Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.*

CC6.7 ***The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.***

The following points of focus:

- *Restricts the Ability to Perform Transmission — Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement, and removal of information.*
- *Uses Encryption Technologies or Secure Communication Channels to Protect Data — Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.*
- *Protects Removal Media — Encryption technologies and physical asset protections are used for removable media (such as USB drives and backup tapes), as appropriate.*
- *Protects Mobile Devices — Processes are in place to protect mobile devices (such as laptops, smart phones, and tablets) that serve as information assets.*

CC6.8 ***The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.***

The following points of focus:

- *Restricts Application and Software Installation — The ability to install applications and software is restricted to authorized individuals.*
- *Detects Unauthorized Changes to Software and Configuration Parameters — Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.*
- *Uses a Defined Change Control Process — A management-defined change control process is used for the implementation of software.*
- *Uses Antivirus and Anti-Malware Software — Antivirus and anti-malware software is implemented and maintained to provide for the interception or detection and re- mediation of malware.*
- *Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software — Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the net- work.*

System Operations

CC7.1 *To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.*

The following points of focus:

- *Uses Defined Configuration Standards — Management has defined configuration standards.*
- *Monitors Infrastructure and Software — The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.*
- *Implements Change-Detection Mechanisms — The IT system includes a change- detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.*
- *Detects Unknown or Unauthorized Components — Procedures are in place to detect the introduction of unknown or unauthorized components.*

CC7.2 *The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.*

The following points of focus:

- *Conducts Vulnerability Scans — The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.*
- *Implements Detection Policies, Procedures, and Tools — Detection policies and procedures are defined and implemented and detection tools are implemented on infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.*
- *Designs Detection Measures — Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.*
- *Implements Filters to Analyze Anomalies — Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.*

- *Monitors Detection Tools for Effective Operation — Management has implemented processes to monitor the effectiveness of detection tools.*

CC7.3 ***The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.***

The following points of focus:

- *Responds to Security Incidents — Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.*

- *Communicates and Reviews Detected Security Events — Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.*

- *Develops and Implements Procedures to Analyze Security Incidents — Procedures are in place to analyze security incidents and determine system impact.*

Additional points of focus that apply only in an engagement using the trust services criteria for privacy:

- *Assesses the Impact on Personal Information — Detected security events are evaluated to determine whether they could or did result in the unauthorized disclosure or use of personal information and whether there has been a failure to comply with applicable laws or regulations.*

- *Determines Personal Information Used or Disclosed — When an unauthorized use or disclosure of personal information has occurred, the affected information is identified.*

CC7.4 ***The entity responds to identified security incidents by executing a defined incident-response pro- gram to understand, contain, remediate, and communicate security incidents, as appropriate.***

The following points of focus:

- *Assigns Roles and Responsibilities — Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are as- signed, including the use of external resources when necessary.*

- *Contains Security Incidents — Procedures are in place to contain security incidents that actively threaten entity objectives.*

- *Mitigates Ongoing Security Incidents — Procedures are in place to mitigate the effects of ongoing security incidents.*

- *Ends Threats Posed by Security Incidents — Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.*

- *Restores Operations — Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.*

- *Develops and Implements Communication Protocols for Security Incidents — Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.*

- *Obtains Understanding of Nature of Incident and Determines Containment Strategy — An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.*

- *Remediates Identified Vulnerabilities — Identified vulnerabilities are remediated through the development and execution of remediation activities.*

- *Communicates Remediation Activities — Remediation activities are documented and communicated in accordance with the incident-response program.*

- *Evaluates the Effectiveness of Incident Response — The design of incident-response activities is evaluated for effectiveness on a periodic basis.*

- *Periodically Evaluates Incidents — Periodically, management reviews incidents related to security, availability, processing integrity, confidentiality, and privacy and identifies the need for system changes based on incident patterns and root causes.*

Additional points of focus that apply only in an engagement using the trust services criteria for privacy:

- *Communicates Unauthorized Use and Disclosure — Events that resulted in unauthorized use or disclosure of personal information are communicated to the data subjects, legal and regulatory authorities, and others as required.*

- *Application of Sanctions — The conduct of individuals and organizations operating under the authority of the entity and involved in the unauthorized use or disclosure of personal information is evaluated and, if appropriate, sanctioned in accordance with entity policies and legal and regulatory requirements.*

CC7.5 ***The entity identifies, develops, and implements activities to recover from identified security inci- dents.***

The following points of focus:

- *Restores the Affected Environment — The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.*

- *Communicates Information About the Event — Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and external).*

- *Determines Root Cause of the Event — The root cause of the event is determined.*

- *Implements Changes to Prevent and Detect Recurrences — Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.*

- *Improves Response and Recovery Procedures — Lessons learned are analyzed and the incident-response plan and recovery procedures are improved.*

- *Implements Incident-Recovery Plan Testing — Incident-recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.*

Change Management

CC8.1 ***The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.***

The following points of focus:

- *Manages Changes Throughout the System Life Cycle — A process for managing system changes throughout the life cycle of the system and its components (infrastructure, data, software, and procedures) is used to support system availability and processing integrity.*

- *Authorizes Changes — A process is in place to authorize system changes prior to development.*

- *Designs and Develops Changes — A process is in place to design and develop sys- tem changes.*

- *Documents Changes — A process is in place to document system changes to sup- port ongoing maintenance of the system and to support system users in performing their responsibilities.*

- *Tracks System Changes — A process is in place to track system changes prior to implementation.*

- *Configures Software — A process is in place to select and implement the configuration parameters used to control the functionality of software.*

- *Tests System Changes — A process is in place to test system changes prior to implementation.*

- *Approves System Changes — A process is in place to approve system changes prior to implementation.*

- *Deploys System Changes — A process is in place to implement system changes.*

- *Identifies and Evaluates System Changes — Objectives affected by system changes are identified and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.*

- *Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents — Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified and the change process is initiated upon identification.*

- *Creates Baseline Configuration of IT Technology — A baseline configuration of IT and control systems is created and maintained.*

Risk Mitigation

CC9.1 ***The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.***

The following points of focus:

- *Provides for Changes Necessary in Emergency Situations — A process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent time frame).*

- *Protects Confidential Information — The entity protects confidential information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to confidentiality.*

- *Protects Personal Information — The entity protects personal information during system design, development, testing, implementation, and change processes to meet the entity's objectives related to privacy.*

- *Considers Mitigation of Risks of Business Disruption — Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes, information, and communications to meet the entity's objectives during response, mitigation, and recovery efforts.*

- *Considers the Use of Insurance to Mitigate Financial Impact Risks — The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives with vendors and partners.*

- *Establishes Requirements for Vendor and Business Partner Engagements — The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.*

- *Assesses Vendor and Business Partner Risks — The entity assesses, on a periodic basis, the risks that vendors and business partners (and those entities' vendors and business partners) represent to the achievement of the entity's objectives.*

- *Assigns Responsibility and Accountability for Managing Vendors and Business Partners — The entity assigns responsibility and accountability for the management of risks associated with vendors and business partners.*

- *Establishes Communication Protocols for Vendors and Business Partners — The entity establishes* *communication and resolution protocols for service or product is- sues related to vendors and business partners.*

- *Establishes Exception Handling Procedures From Vendors and Business Partners — The entity establishes exception handling procedures for service or product issues related to vendors and business partners.*

- *Assesses Vendor and Business Partner Performance — The entity periodically assesses the performance of vendors and business partners.*

- *Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments — The entity implements procedures for addressing is- sues identified with vendor and business partner relationships.*

- *Implements Procedures for Terminating Vendor and Business Partner Relationships — The entity implements procedures for terminating vendor and business partner relationships.*

Additional points of focus:

- *Obtains Confidentiality Commitments from Vendors and Business Partners — The entity obtains confidentiality commitments that are consistent with the entity's confidentiality commitments and requirements from vendors and business partners who have access to confidential information.*

- *Assesses Compliance With Confidentiality Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's confidentiality commitments and requirements.*

Additional points of focus that apply only to an engagement using the trust services criteria for privacy:

- *Obtains Privacy Commitments from Vendors and Business Partners — The entity obtains privacy commitments, consistent with the entity's privacy commitments and requirements, from vendors and business partners who have access to personal information.*

- *Assesses Compliance with Privacy Commitments of Vendors and Business Partners — On a periodic and as-needed basis, the entity assesses compliance by vendors and business partners with the entity's privacy commitments and requirements and takes corrective action as necessary.*

ADDITIONAL CRITERIA FOR AVAILABILITY

A1.1 ***The entity maintains, monitors, and evaluates current processing capacity and use of system com- ponents (infrastructure, data, and software) to manage capacity demand and to enable the imple- mentation of additional capacity to help meet its objectives.***

The following points of focus:

- *Measures Current Usage — The use of the system components is measured to estab- lish a baseline for capacity management and to use when evaluating the risk of im- paired availability due to capacity constraints.*
- *Forecasts Capacity — The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.*