AICPA

Illustrative SOC for Supply Chain Report

Appendix E

Illustrative SOC for Supply Chain Report (Including Entity Management's Assertion, Accountant's Report, and Illustrative Description of the System)

This appendix is nonauthoritative and is included for informational purposes only.

Note to Readers: *In the following illustrative SOC for Supply Chain report, Company X has engaged the practitioner to examine and report on the description of the system that manufactures and distributes widgets and the effectiveness of controls therein, which are necessary to provide reasonable assurance that the company's principal system objectives were achieved based on the applicable trust services criteria relevant to security and availability.*

This illustrative report assumes that, as discussed in the description in section 3, the components received from Company Y are a critical part of Company X's manufacture of its widgets. Company X management has decided to use the carve-out method for Company Y, and the assertion and report include certain disclosures related to Company Y and the complementary supplier controls that it is expected to have in place.

Report on Company X's Description of Its Widget Manufacturing and Distribution System and on the Effectiveness of Its Controls Relevant to Security and Availability Throughout the Period January 1, 20X1, to December 31, 20X1

CONTENTS

Section 1 — Assertion of Company X's Management

[*Company X's Letterhead*]

Assertion of Company X Management

We have prepared the accompanying description of Company X's widget manufacturing and distribution system (system) in section 3 titled "Company X's Description of Its Widget Manufacturing System Throughout the Period January 1, 20XX, to December 31, 20XX," (description) based on the criteria for a description of a company's system in DC section 300, *2020 Description Criteria for a Description of an Entity's Production, Manufacturing, or Distribution System in a SOC for Supply Chain Report,* in AICPA *Description Criteria* (description criteria). The description is intended to provide report users with information about the system, including the effectiveness of controls stated therein, that may be helpful when assessing their risks arising from Company X's manufacture and distribution of widgets.

We have also evaluated whether the controls stated in the description, which are necessary to provide reasonable assurance that Company X achieved its principal system objectives, were effective throughout the period [*date*] to [*date*] based on the trust services criteria relevant to security and availability and whether the controls stated in the description, which are necessary to provide reasonable assurance that Company X achieved its principal system objectives, were effective throughout the period January 1, 20XX, to December 31, 20XX, based on the trust services criteria relevant to security and availability (applicable trust criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria*.

We assert that:

- The description presents Company X's system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.
- Based on the evaluation described in the preceding paragraph, the controls stated in the description, which are necessary to provide reasonable assurance that Company X achieved its principal system objectives, were effective throughout the period January 1, 20XX, to December 31, 20XX, based on the applicable trust services criteria.

Section 2 — Independent Accountant's Report

Independent Accountant's Report

To: Company X

Scope

We have examined:

- Company X's accompanying description of its widget manufacturing and distribution system (system) titled "Company X's Description of Its Widget Manufacturing System Throughout the Period January 1, 20XX, to December 31, 20XX," (description) based on the criteria for a description of a company's system in DC section 300, *2020 Description Criteria for a Description of an Entity's Production, Manufacturing, or Distribution System in a SOC for*

Supply Chain Report, in AICPA *Description Criteria* (description criteria), and

- The effectiveness of controls stated in the description, which are necessary to provide reasonable assurance that ABC Entity's principal system objectives were achieved throughout the period [*date*] to [*date*] based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria*.

Entity Management's Responsibilities

Company X is responsible for establishing the system objectives; identifying the risks that threaten the achievement of the system objectives; and designing, implementing, and operating effective controls within the system to provide reasonable assurance that Company X's principal system objectives are achieved. Company X is also responsible for selecting the applicable trust services category or categories, preparing the description, and stating the controls in the description. Company X has provided the accompanying assertion titled "Assertion of Company X Management" (assertion) about the description and the effectiveness of controls stated therein.

Accountant's Responsibilities

Our responsibility is to express an opinion on the description and on the effectiveness of controls stated in the description, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein, which are necessary to provide reasonable assurance that the company achieved its principal system objectives, were effective based on the applicable trust services criteria.

An examination of the description of a company's system and effectiveness of controls involves the following:

- Obtaining an understanding of the system and the company's principal system objectives
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not effective
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description, which are necessary to provide reasonable assurance that the company achieved its principal system objectives, were effective based on the applicable trust services criteria
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination did not involve performing procedures to obtain evidence about the quality of the goods produced by the system to determine whether those goods met product performance specifications, nor did it involve performing procedures to obtain evidence about whether other system objectives were achieved. Therefore, the opinion expressed below relates only to the effectiveness of controls necessary to provide reasonable assurance that the company achieved its principal system objectives and should not be considered a warranty or guarantee that the goods meet those specifications. Furthermore, we do not express an opinion on the fitness for purpose or the commercial viability of the goods.

Inherent Limitations

The description is prepared to meet the common needs of intended users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always be effective to provide reasonable assurance that the company's principal system objectives are achieved. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the Company's policies or procedures may deteriorate.

Furthermore, the goods produced, manufactured, or distributed may be subject to rates of failure that have been deemed acceptable based on the principal system objectives. For those reasons, such goods may not always be free of defects.

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of those tests, are listed in section 4, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," in columns 2, 3 and 4, respectively.

Opinion

In our opinion, in all material respects,

a. the description presents Company X's system that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.

b. the controls stated in the description, which are necessary to provide reasonable assurance that Company X achieved its principal system objectives, were effective throughout the period January 1, 20XX, to December 31, 20XX, based on the applicable trust services criteria.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of Company X, its business customers and business partners, accountants providing services to such business customers and business partners, and prospective business customers and business partners, who have sufficient knowledge and understanding of the following:

- The nature of the goods produced, manufactured, or distributed by the company

- Internal control and its inherent limitations
- The applicable trust services criteria
- The risks that may threaten the achievement of the company's principal system objectives and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

[*Accountant's signature*]
[*Accountant's city and state*]
[*Date of accountant's report*]

Section 3 — Company X's Description of Its Widget Manufacturing and Distribution System

Note to Readers: *The following illustrative system description is for illustrative purposes only and is not meant to be prescriptive. For illustrative purposes, the description is organized by description criteria; however, there is no prescribed format for the description of a system. For brevity, the description does not include everything that might be included in the description of the entity's system. It also does not include a complete discussion of the processes and controls Company X designs, implements, and operates to achieve its principal system objectives for availability. Ellipses (...) or notes to readers indicate places where detail has been omitted from the illustration.*

Widget Manufacturing and Distribution

Company X (Company X or the Company), located in Weehawken, NJ, is a manufacturer of widgets. Company X's widgets are an integral component of autonomous vehicles manufactured by various automobile and truck original equipment manufacturers (OEMs). Widgets are provided to the OEMs for use in manufacturing and replacement parts. The Company currently does not provide widgets to the aftermarket parts industry. The widgets are the only product manufactured by the Company, and all widgets are made within the Weehawken facility.

Company X's widgets are built to meet or exceed the physical and functional specifications for the widgets described in the Company's technical specifications, which are available to OEM customers through the customer web portal. The widgets comprise both a physical device and embedded software, which is configured during the manufacturing process. The source code for the software used in the widgets is supplied by Company Y Software and then customized and configured for purpose during the manufacturing process by Company X employees. Supplies of other raw materials used in the manufacturing process come from various sources throughout the world.

The Company maintains controls throughout the manufacturing process to help ensure its availability commitments are met and performs periodic testing on a sample of outputs to ensure that its widgets meet the published specifications related to security and processing integrity.

The Company provides its customers with a limited warranty over product functionality, which includes a statement that the widgets are free from known software defects or intentionally embedded malicious code. Each widget model is designed to meet the laws and regulations of specific countries. The countries for which each model is intended are set forth in the product documentation for the model. Widgets are also designed to comply with ISO/TS16949

requirements and other industry standards listed by model in the product documentation.

Upon completion of widget manufacturing, the widgets are stored in two company-owned, on-site loading and storage facilities located in Edison, NJ, and New Brunswick, NJ. Company X has warehouse and inventory management systems in place to ensure widgets are tracked and processed completely and accurately, ensuring they are available per the Company's availability commitments. The widgets are distributed by various contracted distribution logistics companies. Company X does not own or control the distribution companies. Widgets are shipped to customers with full insurance coverage.

Principal System Objectives

Company X's ability to achieve its overall business objectives depends, in large part, on its ability to meet its commitments to customers with respect to products that achieve product performance specifications and related delivery commitments.

The technical product specifications include:

- Physical: Interface criteria, weight, durability, environmental (i.e., ability to withstand heat, dust, and humidity conditions), and power specifications
- Performance: Specific requirements regarding the digital performance of the widget for the purposes stated in product documentation
- The terms and conditions place specific limitations on the use of the product for purposes other than those for which the products were designed.

Company X warrants performance of its widgets to the specifications applicable at the time of sale, in accordance with the warranty included in the supplier contract with the OEM.

To that end, Company X has made the following commitments to its customers:

- Company X will produce widgets that meet or exceed the physical and functional specifications that are (*a*) provided as part of the ordering process or (*b*) described in the related product documentation. Programmed firmware contained within Company X's widgets is free of known software defects that would prevent the widgets from meeting product performance specifications and does not contain any intentionally embedded malicious code.
- Company X will provide firmware updates to OEMs for 15 years beyond the product release date for any software defects identified that prevent the widgets from meeting product performance specifications.
- Widget models are designed to comply with local and national regulations as set forth in product documentation. Company X's widgets are designed to comply with industry standards as listed in the terms and conditions of sale, including ISO/TS16949 requirements.
- Company X recognizes that fulfilling manufacturing and distribution requirements is critical to customers' ability to fulfill their own commitments. To that end, Company X's sales orders contain

financial incentives for meeting delivery commitments and contractual penalties for failure to meet agreed-upon quantities and delivery deadlines.

- Company X recognizes that the timely provision of widgets to customers includes the secure storage, distribution, and delivery of products. Company X commits to maintain distribution contracts in each of the applicable service areas and includes controls to monitor timeliness and quality of distribution. Storage and distribution facilities are protected against physical loss or theft of products that might affect the achievement of the Company's security and/or availability commitments.
- As part of Company X's customer-specific design and production processes, the Company regularly receives information from customers that is considered customer proprietary and sensitive. Company X has established internal data-handling processes to safeguard proprietary customer data from intentional and/or unintentional disclosure, including protection of:
  - Customer trade secrets (e.g., electronic specifications, manufacturing plans, semiconductors, distribution arrangements)
  - Customer purchase quantities and delivery criteria
  - Other proprietary elements as identified by customers at the time of sale
- In the ordinary course of business, Company X does not receive personally identifiable information regarding the end-users of derivative products (e.g., autonomous vehicles). In limited circumstances, the company may receive widgets that have been removed from end-user vehicles in order to perform diagnostic testing and quality analysis. Such information is treated as confidential information of the OEM in accordance with terms of the contract between Company X and the OEM.
- Company X has established specific manufacturing system objectives that are reviewed at each Board of Directors (Board) meeting (e.g., Improving Quality, Managing Cybersecurity Risk, Reducing Costs, Increasing Flexibility, Improving Sustainability). This report addresses the controls relevant to the following principal system objectives:
  - Manufacturing of widgets in accordance with product performance specifications
  - Meeting product availability commitments
  - Managing cybersecurity risk to an acceptable level to support the production of widgets in accordance with specifications, meet product availability commitments, and protect confidential information used in the production process from unauthorized use or disclosure

Description of Company X Software Assurance Process, as Applied to Sourced Embedded Software

Company X follows a stringent set of software quality and security assurance checks with respect to its own software, as well as that of its suppliers.

Company Y software embedded onto the Widget is subject to these software quality and security assurance checks to ensure the software is safe and secure for operation. The software assurance process includes use case testing for functionality, load and stress testing to simulate peak performance conditions, and penetration and fuzz testing to remove security flaws. Company X also receives a structural quality certification of the embedded software from Company Y based on the CISQ standard and the OWASP Top-10, to minimize the risk of latent security vulnerabilities, performance degradations, and failure modes. Both the testing and certification of structural quality are performed with each major and minor release of the embedded software.

Identified System Incidents

During the period under assessment, the Company experienced an incident in which an online intruder gained access, through a previously unknown operating system vulnerability in the server used to update a supplier's software, to the server used to store and configure the embedded software used in its widgets. The intruder used the access to make unauthorized changes to the software and configuration parameters to be loaded in the widgets. The attack was detected approximately 66 hours after the unauthorized access was obtained and was remediated within 5 days of detection. Company X ceased the manufacturing of widgets during the 5-day period and recalled all widgets that were loaded with the software from the time of initial unauthorized access through the remediation of the incident. The Company reconciled serial numbers of all recalled and unshipped widgets to manufacturing records without exception. Based on this reconciliation, management believes that all widgets with the unauthorized software have been accounted for. All of these widgets were subsequently destroyed under controlled conditions.

As part of the remediation, Company X reinstalled the operating system and applications from a backup made prior to the incident and applied the software patch provided by the operating system supplier.

Production, Manufacturing, and Distribution Risks

Risks related to the production, manufacturing, and distribution system and underlying information systems, use of suppliers, and delivery channels used by the entity:

- The Company's widgets are manufactured with software supplied by Company Y, which is configured and installed in each widget during the manufacturing process. Company Y is responsible for supplying components, including the embedded software, which meet the Company's requirements. The quality of the Company's final product is dependent on receiving materials and components, including embedded software, which are free of software defects and do not contain any intentionally embedded malicious code. To that end, see the section "Description of Company X Software Assurance Process, as Applied to Sourced Embedded Software" for controls Company X deploys to test the software that Company Y supplies. The controls and processes of the various raw material and component suppliers are outside the subject of this report.
- The Company's manufacturing and distribution processes are highly automated and integrated, using various IT equipment and information systems. The failure of such equipment and information systems could result in a significant disruption to the manufacture and distribution of widgets. One of the systems Company

X uses in its manufacturing process is the AAA system. The AAA system provider recently went bankrupt. The Company's risk assessment indicates that the Company has not experienced any significant issues with this system. While the Company has the capabilities to repair this system in-house, it will be difficult to replace the AAA system. The Company is actively seeking a replacement strategy before the system becomes obsolete.

- The Company regularly receives, from customers, information that is proprietary and sensitive, including customer trade secrets, customer purchase quantities and delivery criteria, and other proprietary elements as identified by customers at the time of sale.

Risks related to physical, environmental, technological, organizational, and other changes

- As part of the Company's strategic initiatives, the Company moved its widgets manufacturing facility from Sacramento, CA, to Weehawken, NJ, at the beginning of the period. As part of this change, the Company hired a new head of production management that oversees the Weehawken, NJ, facility.
- During the year, the Company also switched the embedded software supplier from Company Z to Company Y during this location change.

Components of the System that Manufactures and Distributes the Widgets

Infrastructure. Company X manufactures widgets on its own assembly line. The manufacturing process includes the direct manufacture of certain key components from raw material, and the assembly of these components with other components sourced from suppliers located in Asia, US, and Mexico.

Customers are given a view into Company X's production and distribution system (PADS) where they can place their orders and track the status and location of the widgets they have ordered.

Components from suppliers are received in a near just-in-time (JIT) fashion based on production forecasts to control inventories; however, some component inventories are kept during peak volume season. This requires real-time tracking of all components and shipments in SAP material management module. Suppliers are given access into an interface that shows real-time status of WIP inventories and order forecasts, enabling suppliers to ship components on an as-needed basis to Company X.

The manufacture of Company X specialty components requires the use of numerous computer controls machines and tools, including injection presses, a de-burring machines, and a soldering machine. These are controlled by automated scheduling systems on the plant floor. The raw materials are delivered into one end of the manufacturing plant, where they are stored in vats and fed into the manufacturing equipment. The finished components are stored on specialized racks and taken to the assembly area by human-operated forklifts.

The assembly of components into final widgets requires a line of specialized robot arms with drilling, soldering, and compression attachments arranged in order. The assembly line is controlled by software embedded into the robots and a master control system (MCS) that operates the robot arms in proper cadence. That software can be updated to assemble the 20 models of widgets

that Company X manufactures. Each widget requires a different set of raw components and different set of operations by the robot assembly line. MCS can handle the 20 widget models and some types of customizations (e.g., including or excluding certain components off the assembly).

The IT systems running the shop floor run on a set of Microsoft Windows servers, running the Windows 10 OS. These are four-way servers housed in a small data center, in a 30x20 room in each of the manufacturing sites. They are connected to the local area networks (LAN) for these sites, which also connect to all the end-user workstations, running Microsoft Office, as well as the scanners used for checking shipments in and out, the mobile devices for shop floor staff, and the HVAC system for climate control. The servers are also connected by a wide area network (WAN) to the other sites in the Company as well as the corporate systems in Company X's secured network operations centers (NOCs). The WAN connectivity is run over T3 lines provided by ABC Communications, with a redundant loop provided by DEF Communications. Business continuity and disaster recovery (BC/DR) services are provided by GHI Corporation with a 4-hour recovery SLA.

Employees access the applications (see "Software" section below) either through their desktop on company-supplied computers or through a Citrix Access Gateway. Data communications between offices are encrypted with Cisco virtual private networking (VPN) technology using Advanced Encryption Standard 256-bit encryption to protect data and intra-company communications.

Company X's IT systems and manufacturing control systems (MCS, PADS, and others) use the Microsoft SQL Server relational database management system. These database servers and file servers are housed in Company X's secured NOCs. All data at rest in the DBMS is encrypted.

Company X uses Transport Layer Security to encrypt email exchanges with customers, suppliers, facility and service providers, and transportation providers. All sensitive data is also encrypted at rest in the DBMS.

Software. The software used in the manufacturing and distribution process falls into three main categories:

1. Embedded logic is the software or firmware that gets encoded in the widgets and robots that operate on the manufacturing floor, in the assembly process, or as part of the distribution process. This software is updated only when it is patched for security vulnerabilities, or when upgrades to the device functionality are necessary.
2. Operating and network software is the software that is in the network routers, gateways, firewalls, etc., and on the operating systems of all the devices, servers, and endpoint computers. The PCs, RDBMS, and servers have already been described. The networks are all running Cisco equipment and their latest operating software. Company X is also running security software for WAF, antivirus and intrusion detection. The HVAC systems are controlled by proprietary software from the HVAC supplier.
3. Information software includes the software that collects and processes data from the factory, distribution process, or customers (as described in the "data" section below) and is used to control the manufacturing and distribution process and customer payments, account tracking, recordkeeping, etc. Company X uses the following IT systems:

- Master Control System (MCS) — The MCS was developed in-house. Together with the Production and Distribution System and the AAA system, it is responsible for the operation of the manufacturing and assembly process, including the robotic assembly line used to assemble the 20 varieties of widgets that Company X manufactures.
- Production and Distribution System (PADS) — The PADS, also developed in house, tracks widgets manufactured and delivered. Customers can track materials through PADS interfaces (portals and APIs). PADS is the source of record for master transportation file data and transportation logs.
- Warehouse and Inventory Management System (WIMS) — WIMS, also developed in house, tracks widgets in the warehouse. Track inventory across every step of your operations from ordering to delivery, track items by lot number, serial numbers, expiration dates, and other methods, monitor asset levels in multiple locations and transfer from one to another when necessary. WIMS interfaces with PADS and WIMS is the source of record for master inventory and warehouse data.
- The AAA system is a third-party supplier software and, together with the MCS and PADS, is responsible for the operation of the manufacturing and assembly process.
- SAP — The manufacturing plants run SAP for all the time-keeping, personnel management, HR, financial reporting, and materials management, including WIP inventories and component orders to ensure raw materials and components are delivered on time for production while minimizing WIP. This system is customized for Company X using configurations and some RICEF code.
- Quality Assurance System (QAS) — The is an in-house developed system that tracks in-plant sampling tests as well as returns and defects in the field. The system is integrated into MCS and SAP to tie together manufacturing configurations and components used in specific batches for root cause analysis.
- Analytics — Company X uses a third-party commercial-off-the-shelf (COTS) analytics package for managing data and business reporting.
- Customer Information System (CIS) — The CIS keeps track of all customer data, including prior order histories and account information. The CIS interfaces into the SAP system for AR.
- Application TRK is installed to enhance the workflow and approval process in support of the policies. This application enables tracking of additions, modifications, or deletions of users; changes to data classification; changes to authority levels in access approvals; tests of new security components prior to installation; and tracking of system incidents and their resolution.

People. Company X has a staff of approximately 150 employees organized in the following functional areas:

- *Corporate.* Executives, senior production management, and senior logistics management. These individuals perform oversight responsibilities over the production and transportation processes through the performance of various monitoring controls. The controls primarily consist of measurement and analyses of key performance indicators generated through internal reports.
- *Operations.* Staff that administer the day-to-day manufacturing activities, and scheduling of transportation providers. Operation staff are divided into the following categories:
  - Design staff
  - Assemblers and assembly supervisors
  - Packaging staff
  - Computer control programmers and operators
  - Quality control inspectors
  - Facility managers
  - Safety coordinators
  - Warehouse workers
  - Transportation coordinators
  - Reports managers

Data. Data within the production system constitutes production requisitions created based on customer orders, production data related to batches, components, raw materials, WIP inventory, and production and quality control logs and reports. Data within the transportation system constitutes master transportation file data and transportation logs. Data within WIMS constitutes master inventory and warehouse data.

These reports are used by management for performing analyses and assessing the effectiveness of controls. They are generated internally within the production and transportation systems and are available in electronic PDF and comma-delimited value file exports. They are not transmitted directly from the production and transportation systems to external parties.

Materials. Company X purchases raw materials and components from preapproved suppliers, selected through a strict vetting and bidding process. Suppliers are responsible for the quality of materials and components; however, Company X has instituted a system of spot checks over certain significant raw materials.

Materials and components that are not being used within the manufacturing system are stored within facilities and secured by physical controls. Inventory controls are employed to ensure production at capacity that would enable the Company to meet its distribution commitments.

Processes and Procedures. The Company's portfolio of security and availability controls is based on specifications set forth in the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) standards. The CRO is responsible for creating, updating, communicating, and monitoring procedures and control activities based on these standards. Procedures and related controls address the following areas within the manufacturing areas:

- Authorized access to the manufacturing management and transportation scheduling systems
- Authorized access to reporting system
- Malware protection
- Filtering of network traffic
- Compartmentalization of manufacturing and transportation systems from office networks
- Change management over SDLC
- Necessary backup and offline storage
- Physical access to production and warehouse facilities
- Environmental monitoring in production and warehouse facilities
- Disaster recovery programs

A description of procedures and controls is provided below.

This section provides information about the five interrelated components of internal control at Company X, including:

- Control Environment,
- Risk Assessment Process,
- Monitoring Activities,
- Information and Communication, and
- Control Activities

Control Environment

Company X's control environment exists under the organization's governance structure and bodies which is led by the Board of Directors (Board). The Board oversees and monitors Company X's control environment with the assistance of its subcommittees including the Audit Committee, which provides general direction and oversight on matters related to the financial statement preparation, external audits and internal control assessment and reporting, and the Technology Committee, which oversees the entity's IT and operations, especially as it relates to manufacturing, engineering and production. The role of these governance bodies as it relates to promoting the integrity of Company X's control environment and are referenced, as warranted in under the subheadings of this section.

Code of Conduct

A sound control environment is established through a commitment to integrity and ethical conduct throughout all levels of the organization. Company X promotes a culture of integrity through an organizational culture and philosophy that prioritizes standards and ethical conduct. To this end, Company X has developed a Code of Conduct policy that has been mandated and approved by the Board. The Code of Conduct provides detailed guidance on proper behavior and outlines sanctions for a breach of conduct up to and including termination. Human Resources is given responsibility for monitoring adherence to the code of conduct and those in a supervisory capacity are trained and instructed to report violations. In addition, an anonymous ethics hotline has been established to facilitate the reporting of dubious conduct and provides a method of reporting which is intended to shield the whistleblower from reprisals. All reported incidents are assigned a case number and investigated. Record of these reports and investigations are summarized and reported to the Board to provide proper

visibility and oversight. The Code of Conduct applies to suppliers and critical third parties that meet certain predefined characteristics and profiles. All employees and contract laborers under Company X's management are required to read and evidence their commitment to acknowledge the Code of Conduct by signature at the time of hire and confirm their acknowledgement annually thereafter.

Company X has anonymous third-party administered whistleblower hotlines available to internal and external users. The CRO monitors customer and workforce complaints reported vie the hotlines.

Control Assessment, Oversight, and Reporting

Board members are appointed to act on behalf of the shareholders. Roles and responsibilities of Board members as outlined in the Board of Directors' Charter are segregated from the roles and responsibilities of management. The Board, by charter, comprises at least 50% independent board members and bears ultimate responsibility for the Company X's control environment and the system of internal control. The Board, depending upon the subject matter on the docket, also assesses the need to supplement board membership with individuals that, for example, possess expertise related to supply chain and third-party risk management. Specifically, the need for special expertise is evaluated prior to each board meeting, based on the meeting agenda. If warranted, the Board will procure the needed experts or consultants, as needed.

Quarterly and annually, senior management and the Board receive information and training needed to fulfill their roles with respect to the achievement of Company X's service commitments and system requirements.

Responsibility for oversight of internal control is delegated to the Audit Committee, with at least 50% of its membership drawn from independent members of the Board. The Audit Committee meets at least quarterly. The Audit Committee comprises individuals who possess requisite expertise related to financial reporting, internal control, operations and logistics, and cybersecurity. In addition, other expertise disciplines will be summons on ex officio basis to address specific topics, as required. Internal Audit, who reports directly to the chair of the Audit Committee, is responsible for assessing Company X's control environment, and planning, executing and issuing audit reports to the responsible management (for the subject matter examined) and the Audit Committee.

The Technology Committee comprises designated representatives of the Board, the Chief Technology Officer (CTO), the Chief Risk Officer (CRO), Chief Information Security Officer (CISO) and the General Managers of Company X's business units. Various internal and external business analysts and system analysts also participate in meetings of the committee, as warranted, to provide subject expertise. The purpose of the Technology Committee is to ensure that Company's technology direction and capability, including information technology, engineering and production can support Company X's current operations, its strategy and future growth. An important mandate of the Technology Committee is to provide design governance to the entity, ensuring the important technology components and application systems under consideration for acquisition and implementation in will support Company X's business strategy, will integrate well into the existing application and technology infrastructure and will scale well throughout the enterprise and support the intended user population(s), as needed.

Organizational Design, Span of Authority, and Reporting Lines

Company X has one primary business unit with a number of operating units and geographic locations. To simplify operations and reporting relationships, the organization and reporting relationships are, however, defined functionally rather than geographically by operating center. Company X assesses its organizational structure, reporting lines, authorities, and responsibilities as part of its ongoing risk assessment and management process, which is summarized and approved by the Board annually. Reporting relationships and organizational structures are reviewed periodically (and at least annually) by senior management and revised when necessary to reflect current organizational structure. A reviewed and updated (if necessary) risk assessment and organization charts that details reporting lines are included as part of a Board package along with other policies that is reviewed and approved by the board, annually.

Roles and responsibilities are documented in written job descriptions which are specified for each position classification. Job descriptions are reviewed by Company X management on an annual basis for needed changes and where job duty changes are required necessary changes to these job descriptions are also made to enable execution of authorities and responsibilities and flow of information to manage the activities of Company X.

Employee roles and responsibilities whose execution affect the achievement of objectives are communicated as part of the hiring or transfer process. Human resources personnel screen internal and external job applicant qualifications based on the defined requirements within the job description. Transcripts are obtained to evidence educational attainment, and job references are checked to validate experience. Prior to extension of a job offer, job candidates are subject to a background check by a third-party provider that conducts a multi-jurisdictional database search of criminal records and credit reporting agencies:

Management is committed to continually developing its workforce and attracting and retaining competent personnel to ensure continued achievement of objectives. To that end Company X provides continued internal and external trainings based on the employees' responsibilities. In addition, annual security, privacy, and safety trainings are mandatory for all employees, contractors, and supplier employee. New hires whether an employee, contractor, or supplier employee, are provided the same training during the onboarding process. The training includes communication of policies for accessing and using systems and sanctions for violating the information security policy. In the training, employees are also instructed to report potential security incidents to the help desk. Management monitors compliance with training requirements.

Company X believes in continuous monitoring and improvement of its environment, processes, technology and people. As it relates to its people, Company X management and the Board perform annual performance evaluations to communicate and hold individuals accountable for performance of internal control responsibilities. The performance evaluation is signed by the manager and employee. The evaluation process may result in corrective actions, including training or sanctions, as necessary.

Management and the Board establish measurable goals and performance evaluation criteria, including incentives, other rewards, and sanctions appropriate for responsibilities at all levels of Company X, that are in alignment with Company's short-term and longer-term objectives. Established short-term and longer-term Company X goals and performance evaluation, reward and

sanctions criteria for Company X executives are reviewed and approved annually by the Compensation Committee to ensure the goals and rewards consider pressures associated with the achievement of objectives. For example, Company X personnel with internal control responsibility are not rewarded based on number of exceptions noted or lack thereof by the external auditor.

Management and the Board evaluate performance of internal control responsibilities, providing rewards and sanctions appropriate for responsibilities, considering the achievement of both short-term and longer-term objectives.

During its ongoing and periodic business planning, business continuity planning and budgeting process, management and the Board evaluate the need for additional tools and resources to achieve business objectives including contingency plans for assignments of responsibility important for internal control.

Risk Assessment Process *[not illustrated]*

Information and Communication

A key step in the design of Company X's processes and controls is the identification of the information needed to operate, monitor and control the system and the definition of the requirements for it. The identified information is included in the system design specifications at the functional and detailed design levels. The subsequent testing of system changes includes procedures to evaluate the completeness and accuracy of the specified information.

Security availability objectives of the system are detailed through various policies, procedures and manuals. These documents are available to internal personnel through an intranet site. The policies and procedures are reviewed by senior management and approved annually by the CRO. As part of senior management's annual review, they identify information required and expected to support the achievement of Company X's service commitments and system requirements.

Company X's security, availability and processing policies and procedures address employee's responsibility for production quality and performance specifications, delivery requirements, operational failures, incidents, system problems, concerns and complaints. The documented policies and procedures include internal controls for producing timely, accurate and complete products. The policies, procedures, and manuals include, but are not limited to, the following:

- Logical and Physical Security
- Change Management
- Incident Response and Monitoring
- Assembly Manuals
- ISO Compliance Procedures
- QAS Procedures

The policies and procedures help ensure that employees understand their individual roles and enable them to carry out their responsibilities and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems. Employees also received updates via staff meetings and monthly newsletters. The documented Incident Response and Monitoring Policy includes procedures regarding an

escalation plan based on the nature and severity of the incident to senior management and the Board, as necessary.

Company X's security and availability commitments are communicated to customers through documented contracts while product specifications are set forth in product documentation. Agreements are established with service providers, including Company Y, that include clearly defined terms, conditions, and responsibilities. Company X's website includes information regarding terms and responsibilities. Any changes to the commitments and requirements are communicated to internal personnel, customers, and third parties on a timely basis.

Monitoring Activities *[not illustrated] ...*

Control Activities *[for brevity, only control activities that address CC5.1–5.3 and CC6. 1–2 have been illustrated. The control activities that address the availability criteria have not been illustrated.]*

Control Design and Implementation

Company X follows a defined process for selecting, developing, and implementing controls when the need for an additional control is identified, whether as a result of a change in risk assessment, the monitoring of controls, or other activities. Once the risk has been identified, a manager from the department responsible for the process is assigned responsibility for developing the new control with the assistance of a team comprising personnel from the controller's office, internal audit, information technology, engineering, and other departments, as necessary. The team identifies the detailed characteristics of the risk and identifies potential controls that would address the risks. Potential controls are evaluated and one or more controls are selected for implementation. As part of the control selection process, the need for monitoring is evaluated and, if needed, appropriate monitoring activities are selected.

The design and implementation of controls is considered a process change and follows the change management process described below.

Security Policies

As a manufacturing organization, Company X treats all third-party information in its custody and all intellectual property as confidential information. Nonpublic information is also regarded as confidential, and as such, afforded all the same protections and safeguards documented all confidential information through the implementation policies, procedures, and controls. The Information Security Policy which defines protection requirements, access rights, and access restrictions, as well as retention and destruction requirements for confidential data. The Information Security Policy also defines assessing risks on a periodic basis, preventing unauthorized access, adding new users, modifying access levels of existing users, and removing users who no longer need access. The functional organization design and on-going assessment facilitates effective lines of reporting, enables execution of authority and responsibilities and the flow of information to manage the activities of the Company.

The following security policies and related processes are in place for the MCS:

- Data classification and business impact assessment
- Selection, documentation, and implementation of security controls
- Assessment of security controls
- User access authorization and provisioning
- Removal of user access

- Monitoring of security controls
- Security management

Asset Management

Company X has an asset management (AM) application to track information assets, including hardware, all stages of data (at-rest, during processing, or in transmission), all three types of software described above (IT software, software on-board manufacturing equipment, and software that's engineered into the product), mobile devices, and offline system components. This inventory is kept up to date by the CTO's office and reviewed by management at least once per annum to certify correctness. These reviews and certifications by management are also tracked by the AM application.

Network Structure

Company X uses network segmentation to help limit access. The network segment in user are:

- Manufacturing — used for IT systems that control the manufacture of widgets, including SCM systems
- Code injection — used for the server and client that configure install embedded software in widgets
- Engineering — used for product design, development, and analysis
- Corporate — used for all other functions
- IT test — used by IT to test changes to software and hardware
- External — used to control access with outsides networks

Virtual firewall technology is used to control access between segments while access to the manufacturing and code injection segment is controlled through dedicated jump servers.

Physical and virtual IT device specification and configuration standards exist for each type of IT device. Operating system, database, and middleware configuration standards are also defined. Variances from standards for a particular use case must be documented and approved by the CISO and CIO. Configurations standards are reviewed and revised on an annual basis. Implementation of configuration changes required by changes to standards are made via the patch management process.

Unique user identification numbers, names, and passwords are required to authenticate users to production systems and all data assets, as well as to the facility services, transportation provider, member services, and client reporting websites. Users are identified and authenticated to the corporate network through a single sign-on tool. This tool is then used to identify and authenticate users to IT components on all but the manufacturing and code injection segments. Access to the manufacturing and code injection segments generally requires separate validation of credentials at dedicated workstations on those segments.

Inbound external traffic terminates at a DMZ that's separated via firewall from the internal network. External users, whether employees or approved third party personnel, are permitted access to company systems via VPN over SSL networks and an access control system that uses two-factor authentication.

Access to applications, servers and other resources is based on role-based security enforced by access control software. In-scope production systems are

configured to limit access to personnel based on the rule sets implemented by the access control system.

Password parameters consist of the following:

- Passwords contain a minimum of eight characters, including one non-alphanumeric character, and are complexity-enabled.
- Passwords expire every 90 days for non-privileged accounts and 60 days for privileged accounts.
- Log-on sessions are terminated after three failed log-on attempts.

Users cannot reuse the last three passwords (five passwords for privileged accounts).

New software, hardware, and devices that are implemented in the company network undergo a change management process, as documented in this report. This process includes the configuration of access credentials to network and information assets for the new software or hardware to function properly. Software and hardware assets are reviewed quarterly and any credentials are removed for any decommissioned assets.

Employees are granted logical and physical access to in-scope systems based on documented approvals. All personnel with external access are documented and access is reviewed by management at least once every six months by appropriate management personnel. Company X's transportation providers, subassembly providers, treating facilities, and component providers (subcontractors) are approved for access by an authorized user. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel. User access is reviewed quarterly to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts. Accounts that are no longer needed are removed from the authorized user list in the access control system.

Administrative access to Active Directory, Unix, SCM systems and system servers and databases is restricted to authorized employees.

The human resources department provides IT personnel with an employee termination report every two weeks. IT reconciles the termination report with current access privileges to determine if access has been appropriately removed or disabled. Customer service and supply chain management teams also provide monthly updates to lists of third-party personnel who can have access to specific Company X systems. Dormant network accounts are disabled after 90 days of inactivity, and dormant MCS accounts are disabled after 45 days of inactivity.

Internal data-handling processes have been established to make sure that confidential customer information is adequately safeguarded. The Company encrypts all e-mail exchanges with customers, suppliers, facility and service providers, and transportation providers with Transport Layer Security. Additionally, the Company encrypts all sensitive data at rest in the DBMS. All internal data transmissions between Company offices are encrypted. Encryption keys are managed and protected using a COTS key vault product across the enterprise.

Change Management... [not illustrated]

Business Continuity and Recovery

The Company monitors its manufacturing plant equipment, systems and personnel schedules, and inventory to ensure adequate system capacity is maintained; equipment is maintained, replaced or upgraded timely; personnel are

available as per manufacturing plans; and inventory of raw materials, WIP, and finished goods are maintained at forecasted levels. The Facilities Team maintains HVAC and other environmental systems, such as UPS, backup generators, sprinklers, fire extinguishers as part of its daily activities and a third party is contracted to test the backup generators and inspect fire extinguishers annually. The Plant Equipment Maintenance Team monitors plant equipment as part of the team's daily activities with routine maintenance performed during scheduled weekly maintenance windows. The Assembly Supervisors plan and monitor personnel schedule and attendance, including penalties for repeat tardiness, which may include employment termination. The NOC Team monitors the network and plant systems for capacity and any potential availability issues. The Assembly Supervisors and Managers, Sales Managers, and Warehouse Managers meet monthly to discuss inventory including planning for future as well as managing current inventory levels.

The Company has contracted with GHI Corporation for its business continuity and disaster recovery with a 4-hour recovery SLA based on its business impact analysis. The Company works with GHI Corporation to test the plans annually.

The Computer Operators performs incremental backup of manufacturing data daily and full backups weekly. Backups are monitored daily and re-run if failed. Backup tapes are shipped off weekly and stored at the GHI Corporation backup storage facility.

Quality Management

As part of the Company X's Quality Assurance System (QAS), the entity remains cognizant of applicable laws and regulations regarding the manufacture, distribution, and export of widgets and their components. The QAS includes quarterly reviews for changes to organizational policy, processes, specifications, and results. Performance results are reviewed with key personnel to ensure that available improvements are implemented and that quality control shortcomings related to customer specifications, commitments, and delivery are adequately addressed on a timely basis.

Company X's widgets are produced using materials and parts from external sources. As part of Company X's ISO 9000-based quality controls, the Company provides both material specifications and software quality requirements (where applicable) to suppliers from whom materials are purchased.

As a function of QAS, products and materials received are inspected for adherence to the Company's specifications and suitability for use in its manufacturing processes. While reasonable measures are instituted to verify the suitability of materials and logical components, the controls and processes of Company X's suppliers are not included in this description nor tested by the practitioner.

Section 4 — Trust Services Categories, Criteria, Related Controls, and Tests of Controls

***Note to Readers*:** *Although the applicable trust services criteria, related controls, and management responses to deviations, if any, would be presented in this section, they are an integral part of Company X's description of its widget manufacturing and distribution system throughout the period January 31, 20X1, to December 31, 20X1. Company X's controls relevant to security and the practitioner's test of controls presented in this section are for illustrative purposes. For brevity, the table does not include the controls Company X designs, implements, and operates to achieve its principal system objectives relevant to*

availability and processing integrity. Only selected controls, tests of controls, and results thereof are illustrated in the table. Accordingly, the table is incomplete.

Applicable Trust Services Criteria Relevant to the Security and Availability Categories

Information Produced by the Entity

For tests of controls requiring the use of Information Produced by the Entity (IPE), including Electronic Audit Evidence (EAE) (e.g., controls requiring system-generated populations for sample-based testing), the practitioner performed a combination of the following procedures to address the completeness, accuracy, and data integrity of the data or reports used:

- Inspected the source of the IPE,
- Inspected the query, script, or parameters used to generate the IPE,
- Tied data between the IPE and the source, and/or
- Inspected the IPE for anomalous gaps in sequence or timing to determine the data is complete, accurate, and maintains its integrity.

For tests of controls requiring management's use of IPE in the execution of the controls (e.g., agreeing the general ledger to the sub-ledger), the practitioner inspected entity management's procedures, as applicable, to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports.

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
Control Environment			
CC1.1 The entity demonstrates a commitment to integrity and ethical values.	Company X has documented the code of business conduct and ethical standards which are reviewed, updated if applicable, and approved by the board of directors and senior management annually.	Inspected the code of business conduct and ethical standards of Company X noting the conduct and standards outlines the Company's commitments to integrity and ethical values and that the conduct and standards were updated and approved by the board of directors and senior management within the examination period.	No exceptions noted.
	Personnel, including contractors, are required to read and accept the code of business conduct and ethical standards upon their hire and formally reaffirm them annually thereafter. Agreements are established with suppliers, vendors, and critical third parties (Company Y, GHI Corporation and other critical third parties) that include clearly defined terms, conditions, and responsibilities for suppliers, vendors, and critical third parties.	For a selection of new hires including contract hires, inspected the code of business conduct and ethical standards signed and determined that the conduct and the standards were acknowledged by each hire selected. For a selection of current personnel, including contractors, inspected the code of business conduct and ethical standards signed and determined that the conduct and the standards were acknowledged annually by each person selected. For a selection of agreements with the suppliers, vendors, and critical third parties, inspected the agreements and determined that the agreement outlined Company X's requirements, including terms, conditions, and responsibilities for the suppliers, vendors, and critical third parties.	Two of 45 new hires selected, did not sign the conduct and standards acknowledgement.

(continued)

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	Management monitors personnel compliance with the code of business conduct and ethical standards through monitoring of customer and workforce member complaints and the use of an anonymous third-party administered ethics hotline. Company X's code of business conduct includes a sanctions policy for personnel who violate the code of business conduct. The sanctions policy is applied to personnel who violate the code of business conduct.	Inspected Company X's website and test dialed the hotline number provided and determined that an anonymous third-party administered hotline is available. Inspected Company X's code of business conduct and determined that it included a sanctions policy for personnel who violate the code of business conduct. For a selection of customer and workforce member complaints logged via the third-party administered hotline, inspected the related documentation and determined that personnel who violated the code of business conduct were sanctioned as per the policy.	No exceptions noted.
	Prior to employment, personnel are verified against regulatory screening databases, including at a minimum, credit, criminal, drug, and employment checks.	For a selection of new hires, inspected the background checks and determined that selected personnel successfully completed background checks including, credit, criminal, drug and employment checks prior to being hired by Company X.	No exceptions noted.
CC1.2 The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The board of directors are appointed to act on behalf of the shareholders. Roles and responsibilities of the board of directors as outlined in the Board of Directors' Charter are segregated from the roles and responsibilities of management. The board of directors understand and acknowledge the Board of Directors' Charter to accept its oversight responsibilities in relation to established requirements and expectations and ultimate responsibility for Company X's control environment. The Board oversees and monitors Company X's control environment with the assistance of its subcommittees including the Technology Committee, which oversees the entity's IT and operations, especially as it relates to manufacturing, engineering and production.	Inspected the Board of Directors' Charter and determined that the board of directors are appointed to act on behalf of the shareholders and the roles and responsibilities are segregated from the roles and responsibilities of management. Inspected the board of directors' acknowledgement of the Board of Directors' Charter to accept its oversight responsibilities in relation to established requirements and expectations. Inspected the Board of Directors' Charter and determined that the Technology Committee has been assigned the responsibility to oversee the entity's IT and operations, especially as it relates to manufacturing, engineering and production.	No exceptions noted.

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	The Board of Directors' Charter includes the minimum background and skills required of board of directors. During the annual board meeting, the background and skills of each board member is compared to the background and skills noted in the Board of Directors' Charter.	Inspected the Board of Directors' Charter and determined that the minimum background and skills required of board of directors is documented. For the annual board meeting, inspected the meeting minutes and determined that the background and skills of each board member was compared to the background and skills noted in the Board of Directors' Charter.	No exceptions noted.
	The Board of Directors meeting agendas is reviewed in advance of the meeting to determine whether subject matter on the agenda requires specific expertise that is not represented and, if warranted, will procure the needed experts or consultants, as needed.	Inspected meeting agendas and minutes for evidence that (*a*) the Board of Directors meeting agendas is reviewed in advance of the meeting to determine whether subject matter on the agenda requires specific expertise that is not represented and (*b*) that, if warranted, the board will procure the needed experts or consultants, as needed, prior to discussing the topic.	
	The board of directors consist of majority of independent members as per the Board of Directors' Charter to maintain independence from management and is composed of at least 50% independent board members,	Inspected the Board of Directors' Charter and determined that it notes the board of directors should consist of majority of independent members. Inspected the board of directors' structure and determined that the board of directors consisted of majority of independent members. Inspected the board of directors' structure and determined that at least 50% or independent of Company X.	No exceptions noted.

(continued)

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	An Audit Committee has been formed as a subcommittee of the board and is charged with evaluating the control environment, and financial reporting process. The audit committee meets quarterly and reports to the board directors and, like the board, is composed of at least 50% external (independent) members. Internal Audit reports directly to the Audit Committee and is responsible for assessing Company X's control environment. Internal Audit with the advice and approval of the Audit Committee, are responsible for planning, executing and issuing audit reports to the responsible management (for the subject matter examined) and to the Audit Committee.	Evaluated the Audit Charter to confirm that they have responsibility for overseeing the control environment and financial reporting process. Evaluated the membership and reporting structure and confirmed that the audit committee is composed of at least 50% external members. Inspected Audit Committee meeting minutes and determined that meetings occur at least quarterly and the meeting minutes are shared with the Board. Inspected the Internal Audit Charter and determined that Internal Audit reports directly to the Audit Committee. Reviewed Audit Committee Minutes and determined that Internal Audit actively reports to and is overseen by the Audit Committee. Inspected the Internal Audit Planning process and three-year audit plan to determine the completeness of the audit universe and span of review.	No exceptions noted.
	The Technology Committee comprises designated representatives of the Board, the Chief Technology Officer (CTO), the Chief Risk Officer (CRO), Chief Information Security Officer (CISO) and the General Managers of Company X's business units.	Evaluated the Technology Committee Charter and determined that the membership comprises the positions as described.	No exceptions noted.

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	The Technology Committee ensure the Company's technology direction and capability, including information technology, engineering, and production, can support its current operations, strategy, and future growth. The Technology Committee meets at least quarterly and reports to the Board.	Evaluated the Technology Committee Charter and determined that the committee has responsibility for overseeing the entity's technology direction and capability, including ensuring that the entity's information technology, engineering and production can support the Company's current and future objectives as it relates to security, availability and processing integrity. Inspected the Technology Committee meeting minutes to determine whether meetings occur at least quarterly and the meeting minutes are shared with the Board.	Exception noted. One of two quarterly Technology Committee meeting minutes was not available.
CC1.3 Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Company X management and the board of directors evaluate its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revise these when necessary to support the achievement of objectives.	Inspected the annual business planning and risk assessment documentation and determined that organizational structure, reporting lines, authorities, and responsibilities were revised.	No exceptions noted.
	Job descriptions are reviewed by Company X management on an annual basis for needed changes and where job duty changes are required necessary changes to these job descriptions are also made to enable execution of authorities and responsibilities and flow of information to manage the activities of Company X.	Inspected the annual business planning and risk assessment documentation and determined that organizational structure, reporting lines, authorities, and responsibilities were revised.	No exceptions noted.

(continued)

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	Company X has a data classification system that treats all third-party information in its custody and all intellection property as confidential information. All information resources deemed "confidential" are afforded the same high-level protections and safeguards through the implementation policies, procedures, and controls. The Information Security Policy defines protection requirements, access rights, and access restrictions, as well as retention and destruction requirements for confidential data. The security policy also defines assessing risks on a periodic basis, preventing unauthorized access, adding new users, modifying access levels of existing users, and removing users who no longer need access.	Obtained the data classification system to determine that all third-party information in the Company's custody is classified confidential. Inspected the Information Security Policy to determine whether it defines protection requirements, access rights, and access restrictions, as well as retention and destruction requirements for confidential data and that he security policy also defines assessing risks on a periodic basis, preventing unauthorized access, adding new users, modifying access levels of existing users, and removing users who no longer need access.	No exceptions noted.
	The Technology Committee comprises designated representatives of the Board, the Chief Technology Officer (CTO), the Chief Risk Officer (CRO), Chief Information Security Officer (CISO) and the General Managers of Company X's business units.	Evaluated the Technology Committee Charter and determined that the membership comprises the positions as described.	No exceptions noted.
	The Technology Committee ensures that the Company's technology direction and capability, including information technology, engineering, and production, can support its current operations, strategy, and future growth. The Technology Committee meets at least quarterly and reports to the Board.	Evaluated the Technology Committee Charter and determined that the committee has responsibility for overseeing the entity's technology direction and capability, including ensuring that the entity's information technology, engineering and production can support the Company's current and future objectives as it relates to security, availability and processing integrity. Inspected the Technology Committee meeting minutes to determine whether meetings occur at least quarterly and the meeting minutes are shared with the Board.	Exception noted. One of two quarterly Technology Committee meeting minutes was not available.

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
CC1.4 The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Job requirements and requisite skill sets for all candidates (employees and contractors) are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring or transfer evaluation process to support the achievement of objectives. The experience and training of candidates, whether an employee, internal transfer, contractor, or employee, are evaluated before they assume the responsibilities of their position to support the achievement of objectives. Existing personnel are evaluated at least annually.	For a selection of new hires, whether an employee, contractor, or employee, and transfers, inspected the personnel file and determined that job requirements and requisite skillsets were documented in the job descriptions. For a selection of new hires, whether an employee, internal transfer, contractor, or employee, inspected the personnel file and determined that offer letter and management notes were maintained evidencing that the selected personnel were evaluated before they assume the responsibilities of their position. For a selection of personnel, whether an employee, contractor, or employee, inspected the personnel file and determined that annual performance evaluations were performed including action items for any shortcomings or decision to terminate the employment.	No exceptions noted.
	Company X evaluates outsourced service providers against established policies and practices as part of the annual evaluation process or when new outsourced service provider relationships are established to support the achievement of Company X's service commitments and system requirements. Any shortcomings noted during the evaluation are addressed with action items and reevaluated in the following year's evaluation process or sooner.	For a selection of outsourced service providers, including existing and new providers, inspected the annual service provider risk assessments performed and determined that external service provider performance and risks were assessed, including action items for any shortcomings as well as follow-up on prior year's action items as necessary.	No exceptions noted.

(continued)

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	Management provides continued internal and external training based on employees' responsibilities. In addition, annual security, privacy, and safety trainings are mandatory for all employees, contractors, and employee. New hires whether an employee, contractor, or employee, are provided the same trainings during the onboarding process. Management monitors compliance with training requirements.	Obtained the dates of and attendance sheets for the annual security training and determined that attendees had signed the attendance sheet for training sessions. For a selection of personnel, obtained the dates of and attendance sheets for role specific trainings and determined that the employee, contractor, or employee selected, had signed the attendance sheet for training sessions. For a selection of new hires, obtained the dates of and attendance sheets and determined that the employee, contractor, or employee selected, had signed the attendance sheet for training sessions. For a selection of personnel not present during the training dates, inspected management's training related documentation and determined that the selected personnel were required to take the training subsequently within the examination period.	No exceptions noted.
	During its ongoing and periodic business planning, business continuity planning and budgeting process, management and the board of directors evaluate the need for additional tools and resources to achieve business objectives including contingency plans for assignments of responsibility important for internal control.	Inspected Company X's annual business planning, business continuity planning and budgeting related documentation and determined that Company X continually evaluated its need for additional tools and resources as well as contingency plans for assignments of responsibility important for internal control.	No exceptions noted.

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	Prior to employment, personnel, including contractors and employees, are verified against regulatory screening databases, including at a minimum, credit, criminal, drug, and employment checks. For personnel with access to customer and company confidential information, such background checks are re-performed every two years.	For a selection of new hires, including contractors and employees, inspected the background checks and determined that selected personnel successfully completed background checks including, credit, criminal, drug and employment checks prior to being hired by Company X. For a selection of personnel with access to customer and company confidential information, inspected the background checks and determined that selected personnel successfully completed background checks including, credit, criminal, drug and employment checks every two years.	No exceptions noted.
CC1.5 The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Company X management and the board of directors perform annual performance evaluations to communicate and hold individuals accountable for performance of internal control responsibilities. The performance evaluation is signed by the manager and employee. Corrective actions, including training or sanctions, as necessary. Each Company X department, such as Operations, Quality Assurance, Software Development, Information Security, Infrastructure, Human Resources, Legal, Compliance, Internal Audit, Finance, Customer Support, hold periodic (weekly) meetings to monitor and manage respective department's progress or lack thereof as it relates to their achievement of department's responsibilities.	For a selection of personnel, whether an employee, contractor, or employee, inspected the personnel file and determined that annual performance evaluations were performed including action items for any shortcomings or decision to terminate the employment, and that evaluations were signed by the manager and the employee. For a selection of weekly department meetings inspected the meeting minutes and determined that department's progress is monitored and measured by respective department heads, including escalation or corrective action as necessary.	No exceptions noted.

(continued)

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	Management and the board of directors establish measurable goals and performance evaluation criteria, including, incentives, other rewards, and sanctions appropriate for responsibilities at all levels of Company X, that are in alignment with Company's short-term and longer-term objectives. Established short-term and longer-term Company X goals and performance evaluation, reward and sanctions criteria for Company X executives are reviewed and approved annually by the Compensation Committee to ensure the goals and rewards consider pressures associated with the achievement of objectives.	For a selection of roles, inspected Company X's documented goals, performance evaluation criteria and compensation matrix including incentives and rewards and determined that a formal process has been implemented for performance measures, incentives and rewards and that the goals documented for selected roles included both short-term and longer-term goals that aligned with Company X's short-term and longer-term goals. Inspected the annual Total Executive Compensation Package and determined that the Compensation Committee approved the package.	No exceptions noted.
	Established short-term and longer-term Company X goals and performance evaluation, reward and sanctions criteria for Company X executives are reviewed and approved annually by the Compensation Committee to ensure the goals and rewards consider pressures associated with the achievement of objectives.	For a selection of roles, inspected the annual Total Executive Compensation Package approved by the Compensation Committee which included Company X's documented goals, performance evaluation criteria and compensation matrix including incentives and rewards and determined that a formal process has been implemented for performance measures, incentives and rewards and that the goals documented for selected roles considers excessive pressures or conflicting goals and evaluation criteria.	No exceptions noted.

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	Management and the board of directors evaluate performance of internal control responsibilities, providing rewards and sanctions appropriate for responsibilities, considering the achievement of both short-term and longer-term objectives.	For a selection of personnel, inspected the personnel file and determined that annual performance evaluations were performed including action items for any shortcomings and that rewards or disciplines documented were consistent with the goals and performance evaluation criteria approved by the Compensation Committee.	No exceptions noted.
Information and Communication			
CC2.1 The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Company X performs assessment at least annually to identify the information required and expected to support the internal control and the achievement of Company X's system objectives. Company X's most valuable and sensitive intellectual property, critical designs, trade secrets, manufacturing dependencies, data and mission-critical systems, "crown jewels" are identified during the assessment, including internal and external sources of data.	Inspected Company X's annual assessment and determined that it identifies the information required to support internal controls and the achievement of Company X's system objectives, including identification of most valuable and sensitive intellectual property, critical designs, trade secrets, manufacturing dependencies, data and mission critical systems, i.e., "crown jewels" whether those are internal or external to Company X.	No exceptions noted.
	Company X has implemented various processes and procedures relevant to security and availability to manufacture widgets in a timely, accurate and complete manner consistent with the Company's objectives. Company X has logical and physical security, change management, incident monitoring, and data classification, integrity, and retention controls, as necessary, with checks and balances woven into each applicable process to ensure quality of processing.	Inspected Company X's documented policies and procedures as it relates to security and availability of its manufacturing process and determined that those document Company X's internal controls for manufacturing widgets that help achieve the Company's commitments and system requirements in a timely, accurate and complete manner.	No exceptions noted.

(continued)

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
CC2.2 The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security of the system, is provided to personnel to carry out their responsibilities.	Inspected Company X's intranet and determined that documented policies and procedures as it relates to security of most valuable data and mission critical systems is available to internal personnel on the intranet.	No exceptions noted.
	Company X management and the board of directors meet quarterly and annually to communicate information needed to fulfill their roles with respect to the achievement of Company X's service commitments and system requirements. Company X has Incident Response policies and procedures in place that includes an escalation plan based on the nature and severity of the incident to senior management and the board of directors as necessary.	For a selection of quarters and the year, inspected the quarterly and annual board meeting minutes and determined that those minutes documented discussion of key items with respect to the achievement of Company X's system objectives, including progress, delays, risks, and challenges related to those key items as applicable. Inspected Company X's documented Incident Response policies and procedures and determined that they include escalation tree and communication plans depending on the nature of the incident, including escalation to the Board, as necessary.	No exceptions noted.
	Company X has anonymous third-party administered whistleblower hotlines available to internal and external users. Management monitors customer and workforce member complaints reported via the hotlines.	Inspected Company X's website and test dialed the hotline number provided and determined that an anonymous third-party administered hotline is available. For a selection of customer and workforce member complaints logged via the third-party administered hotline, inspected the related documentation and determined that personnel who violated the code of business conduct were sanctioned as per the policy.	No exceptions noted.

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	Company X holds quarterly and annual Board meetings. In addition, for communication of an unforeseen event, Incident Response policies and procedures are in place that includes escalation plan based on the nature and severity of the incident to senior management and the board of directors as necessary.	For a selection of quarters and the year, inspected the quarterly and annual board meeting minutes and determined that those documented discussion of key items with respect to the achievement of Company X's system objectives, including progress, delays, risks, challenges related to those key items as applicable. Inspected Company X's documented Incident Response policies and procedures and determined that it includes escalation tree and communication plans depending on the nature of the incident, including escalation to the Board, as necessary.	No exceptions noted.
	Company X's security commitments are communicated to external users (Company Y, GHI Corporation and other critical third parties), as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities. The responsibilities of internal users whose roles affect system operation are communicated to those parties. Responsibilities and policies and procedures posted on Company X's intranet are updated as necessary.	Inspected Company X 's intranet, customer portal, and websites and determined that documented responsibilities, policies and procedures as they relate to security commitments and responsibilities are available to internal personnel on the intranet and external personnel on Company X's websites and customer portals as applicable. For a selection of responsibilities, policies and procedures posted on the intranet, inspected the documents and determined that history of changes with the date of change was documented.	No exceptions noted.
	Internal and external users have been provided with information on how to report security failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected Company X's documented Incident Response policies and procedures and determined that it includes escalation tree and communication plans depending on the nature of the incident, including escalation to the Board, as necessary.	No exceptions noted.

(continued)

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	Changes to Company X's principal system objectives are communicated to internal and external users, vendors, and other third parties (Company Y, GHI Corporation and other critical third parties) whose products and services are part of the system.	Inspected Company X's intranet, customer portal, and websites and determined that documented responsibilities, policies and procedures as it relates to security commitments and responsibilities are available to internal personnel on the intranet and external personnel on Company X's websites and customer portals as applicable, and that those responsibilities, policies and procedures documented history of changes with the date of change. For a selection of agreements with the suppliers, vendors, and critical third parties, inspected the agreements and determined that the agreement outlined Company X's requirements, including terms, conditions, and responsibilities for the suppliers, vendors, and critical third parties and that signed addendum to agreements were also maintained when changes to commitments and requirements occurred, as necessary.	No exceptions noted.
	Management provides continued training about its security commitments and requirements for personnel to support the achievement of objectives. Management monitors compliance with security training requirements. Company X also provides user guides, security alerts and known issues on its websites and customer portal with information to improve security knowledge and awareness.	Obtained the dates of and attendance sheets for the annual security training, as well as the quarterly security compliance updates for employees and determined that employees had signed the attendance sheet for training sessions and updates on the specified dates. For a selection of personnel not present during the training dates, inspected management's training related documentation and determined that the selected personnel were required to take the training subsequently within the examination period. Inspected Company X's customer portal and websites and determined that user guides and history of security alerts and known issues with information to improve security knowledge and awareness was available.	No exceptions noted.

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	Company X posts a description of its system, system boundaries, and system processes that include infrastructure, software, people, processes and procedures, data, and raw materials on its intranet for internal users and on the Internet for external users.	Inspected Company X's intranet and Internet descriptions of Company X's system, system boundaries, and system processes and determined that the description addressed infrastructure, software, people, processes and procedures, data, and raw materials for the in-scope technology and locations.	No exceptions noted.
	Agreements are established with suppliers and business partners (Company Y, GHI Corporation and other critical third parties) that include clearly defined terms, conditions, and responsibilities for suppliers, vendors, and critical third parties.	For a selection of agreements with the suppliers, vendors, and critical third parties, inspected the agreements and determined that the agreement outlined Company X's requirements, including terms, conditions, and responsibilities for the suppliers, vendors, and critical third parties.	No exceptions noted.
	Planned changes to system components are reviewed, scheduled, and communicated to management as part of the weekly IT maintenance process. Planned changes to system components are communicated to external users (Company Y, GHI Corporation and other critical third parties) via the Company X's website.	For a selection of weeks, inspected weekly IT maintenance schedules and communications and determined that planned system changes were included and had been reviewed and signed off by IT management. Inspected Company X's customer portal and determined that it published a calendar of upcoming system changes existed and that it communicated upcoming changes and their impact on users, if any.	No exceptions noted.
Control Activities			
CC5.1 The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	As part of its annual risk assessment, management linked the identified risks to controls that have been designed and operated to address them. When the need for new controls is identified, management develops the requirements for the new controls and uses the change management process to implement them.	Obtained and inspected the annual risk assessment documentation to determine that new controls were implemented for any risks not adequately addressed by existing controls. Inspected a sample of system change requests to determine that the change management process was followed.	No exceptions noted.

(continued)

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	As part of the risk assessment, management assessed the environment, complexity, nature and scope of its operations when developing control activities to mitigate the risks.	Obtained and inspected the risk assessment documentation to determine whether management assessed the environment, complexity, nature and scope of its operations when developing control activities to mitigate the risks	No exceptions noted.
	When management identifies the need for new controls, management considers a mix of control activities, including both manual and automated controls and preventive and detective controls.	Obtained and inspected the risk assessment documentation to determine whether management considered a mix of control activities to mitigate the identified risks.	No exceptions noted.
	Company X has designed application-enforced segregation of duties to define what privileges are assigned to users within the MCS.	Inspected the access control policy to determine whether application controls were designed to enforce segregation of duties to users within the MCS.	No exceptions noted.
CC5.2 The entity also selects and develops general control activities over technology to support the achievement of objectives.	As part of the IT strategic plan, strategic IT risks affecting the organization and recommended courses of action are identified and discussed. The plan is developed annually by the CIO and approved by senior management and the Security Steering Committee.	Inspected the annual IT strategic plan documentation to determine whether IT risk affecting the organization and recommended courses of action were identified and discussed and whether the plan was approved by senior management and the Security Steering Committee.	No exceptions noted.
	Management developed a list of control activities to manage the technology infrastructure risks identified during the annual risk assessment process.	Inspected the risk assessment, internal audit plan and audit program for the calendar year to determine whether management developed and implemented control activities over the technology infrastructure.	No exceptions noted.
	Management developed a list of control activities to manage the security access management risks identified during the annual risk assessment process.	Inspected the risk assessment, internal audit plan and audit program for the calendar year to determine whether management developed and implemented control activities designed to restrict technology access rights to authorized users commensurate with their job responsibilities and protect corporate assets from external threats.	No exceptions noted.

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	Company X employs organization-defined tailored acquisition strategies and procurement methods for the purchase, development, and maintenance of information systems, system components, or information system services from technology suppliers.	Inspected the procurement policy manual to determine whether management employed acquisition strategies and procurement methods for the purchase, development, and maintenance of information systems, system components, or information system services from technology suppliers.	No exceptions noted.
	Company X has a formalized security and systems development methodology that includes project planning, design, testing, implementation, maintenance, and disposal or decommissioning.	Inspected the systems development methodology document to determine whether it included project planning, design, testing, implementation, maintenance, and disposal or decommissioning.	No exceptions noted.
	Company X uses a standardized server build checklist to help secure its servers.	For a selection of servers, inspected the associated server build checklist to determine whether standardized checklists were used to help secure servers.	No exceptions noted.
	Patches are applied regularly applied in accordance with Company X's patch management procedures.	For a selection of patches, inspected the associated patching documentation as well as the patch management procedures to determine whether patches were applied regularly applied in accordance with Company X's patch management procedures.	No exceptions noted.
	Company X utilizes firewalls, an intrusion detection system (IDS), an intrusion prevention system (IPS), and operating system event logs to protect its environment. Alerts are configured around the utilities to notify the security administration team of potential security threats or incidents.	Observed the firewall configurations, the intrusion detection system, the intrusion prevention system, and operating system event logs to determine whether system monitoring utilities were in place to protect the environment. Observed the alert settings for the firewalls, the IDS, the IPS, and the operating system event logs to determine whether alerts were in place to notify the security administration team of potential security threats or incidents.	No exceptions noted.

(continued)

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	On a daily basis, the security administration team reviews the following security incident and event monitoring (SIEM) reports: • failed object level access; • daily IDS or IPS attacks; • critical IDS or IPS alerts; • devices not reporting in the past 24 hours; • failed login detail; • firewall configuration changes; • Windows policy changes; • Windows system shutdowns and restarts; and security events requiring further investigation are tracked using a help desk ticket and monitored until resolved.	For a selection of days, inspected the SIEM reports and verified that the security administration team reviewed the SIEM reports on a daily basis.	No exceptions noted.
CC5.3 The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Company X's policy and procedure manuals address controls related to the MCS. Policy sections include *a.* data classification and business impact assessment; *b.* selection, documentation, and implementation of security controls; *c.* assessment of security controls; *d.* user access authorization and provisioning; *e.* removal of user access; user provisioning and deprovisioning; *f.* monitoring of security controls; and *g.* security management.	Inspected the policy and procedure manuals related to the MCS to determine whether they included section headings that addressed controls over the significant aspects of system operations.	No exceptions noted.

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	Application TRK is installed to enhance the workflow and approval process in support of the policies.	Observed Application TRK to determine whether it was installed to enhance the workflow and approval process in support of the policies.	No exceptions noted.
	An information security policy is in place to help ensure that employees understand their individual roles and responsibilities concerning processing and controls.	Inspected the information security policy to determine whether the policy was in place and whether it detailed roles and responsibilities concerning processing and controls.	No exceptions noted.
	The Company's Security Steering Committee is charged with establishing, maintaining, and enforcing the overall security policies and procedures.	Inspected a sample of minutes from quarterly Security Steering Committee meetings to determine whether the committee was charged with establishing, maintaining, and enforcing the overall security policies and procedures.	No exceptions noted.
	As part of its Quality Assurance System (QAS), Company X performs quarterly reviews for changes to organizational policies, processes, specifications and results.	For a selection of quarters, inspected the quarterly review documentation as well as the updated policies and procedures and determined that Company X performed quarterly reviews for changes to organizational policies, processes, specifications and results.	No exceptions noted.
	The information security team monitors the results of vulnerability assessments on a monthly basis. The information security team uses these results to identify necessary changes to the policies and procedures.	For a selection of months, inspected the vulnerability assessments as well as the related review documentation to determine whether the results of vulnerability assessments were monitored on a monthly basis. Further, inspected the policy and procedure manuals and verified that necessary changes were made as a result of reviewing the results of the vulnerability assessments.	No exceptions noted.

(continued)

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	The Chief Risk Officer is responsible for creating, updating, communicating, and monitoring procedures and control activities based on the specifications set forth in the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) standards.	Inspected the job description for the Chief Risk Officer to determine whether the individual's responsibilities included updating, communicating, and monitoring procedures and control activities. Inspected the policy and procedure manuals as well as related review documentation to determine whether procedures and control activities were updated based on ISO and IEC standards.	No exceptions noted.
	Company X has written job descriptions specifying the responsibilities and the academic and professional requirements for key job positions. Human resources personnel screen internal and external job applicant qualifications based on the defined requirements within the job description. Transcripts are obtained to evidence educational attainment, and job references are checked to validate experience.	For a sample of key positions, inspected written job descriptions to determine whether the job descriptions included responsibilities and academic and professional requirements. For a sample of employees, inquired of the employees about their understanding of their job responsibilities, academic qualifications, and professional certifications and compared their responses for consistency to the documented responsibilities, and academic and professional requirements documented in the job description applicable to their position. For a sample of new employees and employees who have transferred internally, inspected the personnel file to determine whether transcripts were obtained, and job references were checked.	No exceptions noted.
	Company X's policy and procedure manuals are reviewed annually by the CIO, Vice President of Operations, and the Security Officer for consistency with the organization's risk mitigation strategy and updated as necessary for changes in the strategy.	Inspected the policy and procedure manuals to ascertain whether policies and procedures had been updated for changes in the risk mitigation strategy. Inspected documentation of the annual review of the policy and procedures manuals by the CIO, Vice President of Operations, and the Security Officer.	No exceptions noted.

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
Logical and Physical Access			
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 company identifies, classifies and manages an inventory of information assets through an access database. The inventory is reviewed and approved by management on an annual basis.	Inspected the access database to determine whether an inventory is maintained and information assets are classified. Inspected documentation of management's review and approval of the inventory and classification.	No exceptions noted.
	The Company monitors system components through an automated management interface to log, track, and maintain inventory components.	Inspected the automated inventory management tool to determine that the tool is in place to monitor the system components. Inspected information system inventory records from the inventory management tool to determine that the tool was providing necessary information to manage assets.	No exceptions noted.
	Logical access to information assets is restricted through use of access control software and rule sets.	Inspected information systems configuration to determine whether access control software and rule sets were used to restrict access.	No exceptions noted.
	Production systems are configured to authenticate users with a unique user account and enforce predefined user account and minimum password requirements.	Inspected the Information Security Policy to determine whether unique user accounts are required and minimum password requirements for production systems are defined.	No exceptions noted.
	Administrative access to Active Directory, Unix, SCM systems and system servers and databases is restricted to authorized employees.	Inspected information systems configuration to determine whether administrative access to Active Directory, UNIX, SCM systems, servers, and databases is restricted to authorized employees.	No exceptions noted.

(continued)

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	Company X's transportation providers, assembly providers (user entities), treating facilities, and component providers (subcontractors) are approved for access by an authorized user.	Inspected a sample of documented user entity and subcontractor requests for access to the system to determine whether they were approved for access by an authorized user. Inspected a sample of user access configurations and determined that system configurations aligned to approved requests.	No exceptions noted.
	Company X permits remote access to production systems by authorized employees only with multi-factor authentication (MFA) over encrypted virtual private network (VPN) connection	Observed a remote login session to determine that MFA VPN was required to access the production network.	No exceptions noted.
	Web servers utilize TLS certificates for encrypted web communication sessions. TLS certificates are monitored for renewal.	Inspected login portal for each of the in-scope information assets to determine whether web communication sessions were secured through TLS certificates. Inspected certificate expiration report to determine whether TLS certificates were valid and renewals were tracked.	No exceptions noted.
	In-scope system components require unique username and passwords (or authorized SSH keys) prior to authenticating users.	Inspected login attempts to determine that the in-scope system components required authentication measures for users.	No exceptions noted.
	End user and server workload network traffic is segmented to support isolation.	Inspected the network diagram and configurations to determine that customer environments and data are segmented.	No exceptions noted.

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
	Inbound internet traffic terminates at hosts in the DMZ which is separate from the LAN.	Observed firewall system configurations to determine whether inbound Internet traffic terminated at hosts in the DMZ which was separate from the LAN.	No exceptions noted.
	A data classification policy is in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the data classification policy to determine that procedures existed around classifying and protecting confidential information.	No exceptions noted.
	SSL certificates are used at the entry-point firewalls to information assets to establish access control rules.	Inspected the SSL certificates for verification, issuance, signature algorithm, and validity date.	No exceptions noted.
	Passwords for in-scope system components are configured according to the Company X's policy, which (*a*) requires eight-character minimum and 90-day password changes; (*b*) is complexity enabled; and (*c*) locks users out of the system after three invalid attempts.	Inspected in-scope system components to determine that passwords were configured according to company policy.	No exceptions noted.
	All new software and devices installed on the network or in the manufacturing facility go through a change management process, which includes establishing appropriate credentials for said software and/or devices to operate on company infrastructure.	Inspected a sample of new software and devices installed on the network to determine whether appropriate user credentials were established and user accounts settings aligned to security policies.	No exceptions noted.
	Databases housing sensitive customer data are encrypted at rest.	Inspected database configurations to determine that databases were encrypted at rest.	No exceptions noted.
	Encryption keys used by integrated services are encrypted themselves with a unique master key.	Inspected the configuration for the encryption process to determine that encryption activities use an acceptable cryptographic algorithm.	No exceptions noted.

(continued)

Trust Services Criteria for the Security and Availability Categories	*Description of Company X's Controls*	*Practitioner's Tests of Controls*	*Results of Practitioner's Tests of Controls*
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Access to in-scope system components requires a documented access request form and manager approval and authorization prior to access being provisioned.	Inspected access requests forms for a sample of new hires that received access to the in-scope system components to determine that an access provisioning request was approved prior to access being provisioned.	No exceptions noted.
	IT is notified of terminations by email from HR. Access is removed/disabled from the network, and in-scope applications timely.	Compared a system-generated list of active users to a system-generated list of terminated employees to determine whether any terminated employees had access to the in-scope applications.	No exceptions noted.
	A termination checklist is completed and access is revoked for employees within 24 hours as part of the termination process.	Inspected termination tickets for a sample of terminated employees during the review period to determine that access was revoked within 24 hours as a part of the termination process.	No exceptions noted.
	Management performs a quarterly access review for the in-scope system components to ensure that access is restricted appropriately. Tickets are created to remove access as necessary in a timely manner.	Inspected access review documentation for sample of quarters to determine that an access review was performed for in-scope system components and that tickets were created to remove inappropriate access.	No exceptions noted.

Section 5 — Other Information Provided by Company X Management That Is Not Covered by the Accountant's Report

Note to Readers: *The entity may wish to attach to the description of the manufacturer's system, or to include in a document containing the accountant's report, information in addition to its description. The following are examples of such information:*

- *Future plans for new systems.*
- *Other services provided by the organization that are not included in the scope of the engagement*
- *Qualitative information, such as marketing claims, that may not be objectively measurable*
- *Responses from management to deviations identified by the practitioner when such responses have not been subject to procedures by the practitioner*

For brevity, an example is not provided.