April 2017

Association of International Certified Professional Accountants®

Illustrative cybersecurity risk management report

Note to readers:

Although the AICPA Guide Reporting on an Entity's Cybersecurity Risk Management Program and Controls describes the components of a cybersecurity risk management report and the information to be included therein, it does not mandate specific formats for most of the information to be presented. Entity management and the practitioner may organize and present the required information in a variety of formats.

The format of the illustrative cybersecurity risk management report presented in this nonauthoritative document is included for illustrative purposes only. The illustrative cybersecurity risk management report contains all the required components of such a report, including (a) management's assertion, (b) the accountant's report, and (c) the description of the entity's cybersecurity risk management program.

CONTENTS

Section 1—Assertion of the Management of XYZ Manufacturing

Introduction

We have prepared the attached XYZ Manufacturing's Description of its Cybersecurity Risk Management Program throughout the period January 1, 20X1, to December 31, 20X1, (description) based on the criteria for a description of an entity's cybersecurity risk management program identified in the AICPA *Description Criteria for Management's Description of an Entity's Cybersecurity Risk Management Program* (description criteria). An entity's cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity's cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that are not prevented. We have established XYZ Manufacturing's cybersecurity objectives, which are presented on page XX of the description. We have also identified the risks that would prevent those objectives from being achieved and have designed, implemented, and operated controls to address those risks.

Inherent Limitations

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in an entity's cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Assertion

We assert that the description throughout the period January 1, 20X1, to December 31, 20X1, is presented in accordance with the description criteria. We have performed an evaluation of the effectiveness of the controls included within the cybersecurity risk management program throughout the period January 1, 20X1, to December 31, 20X1, using the criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) (control criteria). Based on this evaluation, we assert that the controls were effective throughout the period January 1, 20X1, to December 31, 20X1, to achieve the entity's cybersecurity objectives based on the control criteria.

Section 2—Independent Accountant ’s Report

To Management of XYZ Manufacturing:

Scope
We have examined the accompanying XYZ Manufacturing’s Description of its Cybersecurity Risk Management Program throughout the period January 1, 20X1, to December 31, 20X1, (description) based on the description criteria noted below. We have also examined the effectiveness of the controls within that program to achieve the entity’s cybersecurity objectives based on the control criteria noted below.

The criteria used to prepare the description are the AICPA’s *Description Criteria for Management’s Description of an Entity’s Cybersecurity Risk Management Program* (description criteria); the criteria used to evaluate whether the controls within the entity’s cybersecurity risk management program were effective to achieve the entity’s cybersecurity objectives are the criteria for security, availability, and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) (control criteria).

An entity’s cybersecurity risk management program is the set of policies, processes, and controls designed to protect information and systems from security events that could compromise the achievement of the entity’s cybersecurity objectives and to detect, respond to, mitigate, and recover from, on a timely basis, security events that were not prevented.

Entity’s Responsibilities

XYZ Manufacturing’s management is responsible for the following:

- Establishing the entity’s cybersecurity objectives, which are presented on page XX of the description.
- Designing, implementing, and operating the cybersecurity risk management program, including the controls within that program, to achieve the entity’s cybersecurity objectives
- Preparing the accompanying description of the entity’s cybersecurity risk management program
- Providing an assertion about whether the description of the entity’s cybersecurity risk management program is presented in accordance with the description criteria and whether controls within the cybersecurity risk management program were effective to achieve the entity’s cybersecurity objectives.

When preparing its assertion titled *Assertion of the Management of XYZ Manufacturing*, management is responsible for (*a*) selecting, and identifying in its assertion, the description criteria and the control criteria and (*b*) having a reasonable basis for its assertion about whether the controls within the entity’s cybersecurity risk management program were effective to achieve the entity’s cybersecurity objectives by performing an assessment of the effectiveness of those controls based on the control criteria. The description of the entity’s cybersecurity risk management program and management’s assertion accompany this report.

Accountant’s Responsibilities

Our responsibility is to express an opinion, based on our examination, about whether the description of the entity’s cybersecurity risk management program is presented in accordance with the description criteria and whether the controls within that program were effective to achieve the entity’s cybersecurity objectives based on the control criteria.

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 the examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls within the program were effective to achieve the entity's cybersecurity objectives based on the control criteria.

Our examination included

- obtaining an understanding of the entity's cybersecurity objectives and its cybersecurity risk management program;
- assessing the risks that the description was not presented in accordance with the description criteria and that the controls within that program were not effective; and
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria and whether the controls were effective.

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.

Inherent Limitations

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 inherent limitations in its cybersecurity risk management program, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis.

Examples of inherent limitations in a cybersecurity risk management program include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects,

- the description of XYZ Manufacturing's cybersecurity risk management program throughout the period January 1, 20X1, to December 31, 20X1, is presented in accordance with the description criteria and
- the controls within that program were effective throughout the period January 1, 20X1, to December 31, 20X1, to achieve the entity's cybersecurity objectives based on the control criteria.

Baker, Jones, and Eagle, CPAs
Athens, Georgia March 1, 20X2

Section 3—XYZ Manufacturing's Description of its Cybersecurity Risk Management Program

Note to readers: *The following illustrative description of an entity's cybersecurity risk management program, which is based on the operations of a hypothetical company, illustrates how a company might prepare and present a description of its cybersecurity risk management program in accordance with the description criteria. The description criteria have been included within the presentation for illustrative purposes.*

Nature of Business and Operations

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

XYZ Manufacturing (XYZ or the Company) is a leading manufacturer, distributor, and retailer of reproduction consumer products and objects from various historical periods, with an emphasis on classical Greece, ancient Rome, and medieval Europe. The Company's products allow consumers to emulate a non-contemporary lifestyle in one or more facets of their lives. Merchandise is provided across a broad range of categories including kitchen and dining, furniture, bedding and bath, lighting solutions, and arts, crafts, and sewing. The Company operates through three key segments: manufacturing (30 percent of revenue), online retail (40 percent of revenue), and wholesale (30 percent of revenue). XYZ's online retail and wholesale operations offer products manufactured by the Company and sourced under contract from other manufacturers. Online retail also offers products sourced from other wholesalers.

The Company serves its primary markets of North America and Europe from its headquarters in Athens, Georgia, and Rome, Italy, respectively, and has major operating facilities throughout the U.S. and Europe. Manufacturing is located in Shanghai, China. In 2015, the Company entered into a joint venture with UVW Trading of Hong Kong to expand into Asian markets, where the Company's products hold strong appeal from a novelty perspective. Distribution is provided by commercial carriers.

Nature of Information at Risk

DC2: The principal types of sensitive information created, collected, transmitted, used, or stored by the entity

The Company creates, obtains, distributes, uses, and stores a wide variety of information in its operations. In addition to information common to the operation of entities similar to XYZ, such as regulatory compliance information and personnel records, the Company uses the following information:

- Financial information, which is used for both internal and external reporting purposes. Internal financial information and external financial information, prior to publication, is considered confidential and is treated as insider information.
- Confidential sales information, including customer lists, confidential wholesale pricing information, and order information
- Payment card information used in online retail and wholesale transactions, including cardholder names and card numbers. This information may be retained for customer convenience on XYZ systems for ease of ordering
- Online retail customer profile information used to provide customers with a personalized lifestyle experience
- Confidential product information including product specifications, new design ideas, and branding strategies

- Proprietary information provided by business partners, including manufacturing data, sales and pricing information, and licensed designs
- Confidential employee information

Cybersecurity Risk Management Program Objectives (Cybersecurity Objectives)

DC3: The entity's principal cybersecurity risk management program objectives (cybersecurity objectives) related to availability, confidentiality, integrity of data, and integrity of processing

Under the direction of the XYZ board of directors, management establishes the objectives of the Company. Based on these objectives, management also establishes specific objectives for its cybersecurity risk management program. Because substantially all Company operations involve the use of IT, the Company makes no distinction between information security and cybersecurity.

XYZ Manufacturing's cybersecurity objectives are the following:

Availability

Enabling timely, reliable, and continuous access to and use of information and systems to support operations and to

- provide
  - online retail store availability 24-hours a day year-round
  - customer experiences related to system response and dropped transactions meeting benchmarks established by management
  - manufacturing system availability during scheduled shifts
  - timely information from the enterprise resource planning (ERP) system to suppliers and management to support decision making
  - wholesale online, field sales support, and customer service center systems availability as committed
  - accurate product availability and delivery information
- support the delivery of products to customers as committed
- comply with applicable laws and regulations
- safeguard assets

Confidentiality

Protecting information from unauthorized access and disclosure, including means for protecting proprietary information and personal information subject to privacy requirements, to safeguard

- employee and customer information, including credit card information, in accordance with laws, regulations, and card brand requirements
- confidential corporate data related to sales and financial reporting
- confidential business transactions related to the information of business partners and others
- the intellectual property of the Company, its business partners, and others

Integrity of Data

Guarding against improper capture, modification or destruction of information to support

- the preparation of reliable
  - financial and nonfinancial information for external reporting purposes
  - information for internal use
- nonrepudiation and authenticity of transactions from online systems
- the completeness, accuracy, and timeliness of manufacturing, delivery of goods, and information processing

- management, in holding employees, vendor and business partner employees, and customers accountable for their actions
- the storage, processing, and disclosure of information, including personal and third-party information

Integrity of Processing
Guarding against improper use, modification, or destruction of systems in order to support

- the accuracy, completeness, and reliability of product delivery and transaction processing
- the manufacture of goods to product specifications
- the efficient operation of production
- the safeguarding of the life and health of employees in production facilities

Guarding against the improper use or misuse of processing capabilities that that could be used to impair the security or operations of external parties

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

The Company's board of directors, with the support of management and outside resources engaged by the board, reviews and updates its formal business strategy annually. Based on that strategy, management and the board annually establish or update the Company's overall business objectives, including objectives over operations, compliance, and reporting. At the completion of this process, the overall objectives are approved.

Upon approval of the Company's business strategy and overall objectives, management uses a top-down approach to establish or update specific business objectives for business units and functions, including information technology, within the organization. This process includes budgeting resources and establishing metrics for the achievement of the objectives. At the completion of this process, the specific business objectives and the budget is submitted to the board for approval.

As part of the development of specific business objectives, the chief information security officer (CISO) updates the Company's cybersecurity objectives with the objectives of the business units and other functional areas. These cybersecurity objectives are then approved by the Company's executive management, including the CEO, COO, CFO, chief risk officer (CRO), general counsel (GC), and the CIO.

The Company's cybersecurity risk management program is based on specifications set forth in the National Institute of Standards and Technology "Framework for Improving Critical Infrastructure Cybersecurity" (NIST cybersecurity framework) and International Standardization Organization and International Electrotechnical Commission (ISO/IEC) standards. The Company's portfolio of security controls is based on ISO/IEC controls and, for systems containing cardholder information, the Payment Card Industry Data Security Standards.

Factors that have a Significant Effect on Inherent Cybersecurity Risks

DC5: Factors that have a significant effect on the entity's inherent cybersecurity risks, including the (1) characteristics of technologies, connection types, use of service providers, and delivery channels used by the entity; (2) organizational and user characteristics; and (3) environmental, technological, organizational and other changes during the period covered by the description at the entity and its environment

Technologies, connection types, service providers, and delivery channels. The Company uses the following technologies, connection types, service providers, and delivery channels:

- An integrated ERP system is used to manage manufacturing, wholesale, and retail operations. The ERP system is interfaced with the manufacturing, wholesale, and online retail systems to provide an integrated IT environment.
- Online retail operations are supported by a software-as-a-service (SaaS) cloud provider. The integrated solution provided permits the Company to design and maintain its retail site in an effective and efficient manner. Online wholesale operations are supported through a third-party system that interfaces with the ERP system. The system is hosted on a network of virtual servers hosted in XYZ's primary data center.
- Wholesale call center services are outsourced with the call center's systems interfaced with the ERP system to facilitate ordering and problem resolution. The interface with the call center is over a virtual network connection. Custom-developed software is used to interface the call center system to the ERP interface.
- Field sales automation is provided through the use of company-owned tablet devices running third-party software customized for the Company. Tablets access the ERP system through a virtual private network (VPN) system.
- Manufacturing is controlled through a network of midrange systems running widely used manufacturing system software. This software is modified and maintained by Company IT personnel.
- All connectivity to external users occurs through defined access points managed by routers.
- Routers are also used to segment the network within the Company.
- Transmissions to vendors and other third parties are sent through defined channels.

Organizational and user characteristics. The Company's IT function is headed by a chief information officer (CIO) and is divided into application services, technology services, and information security. The Company uses a centralized organizational model to support company applications and technology. The online retail and call center vendor relationships are managed by designated personnel in technology services reporting to the chief technology officer (CTO). The information security group is headed by the CISO and consists of security architecture and technical support, application security, and security operations center personnel. Security operations center personnel are primarily responsible for user administration, second-level security support, security event monitoring, and security incident response and management.

Users of the system primarily consist of the following:

- Consumers whose access is restricted to the online retail system provided by the vendor.
- Wholesale customers whose employees have access to catalog information, order status, order functionality, and account functionality through the internet module of the wholesale system. Customer personnel are assigned user IDs via a master customer account that is also used to administer the accounts. Customer personnel accounts are assigned defined roles established by the Company.
- UVW personnel whose access is similar to wholesale customer access.
- Call center service organization personnel, who access the wholesale system through assigned user accounts that are restricted to a defined call center role.
- All XYZ employees, who are assigned unique user IDs that grant them default company access and email access, with the exception of manufacturing line personnel in Shanghai who are not granted access.

- Product vendors, who are granted limited access to the ERP system to pick up purchase orders and inquire about the status of invoices. This access is provided through a module of the ERP system through a vendor account and password.

Although IT assets are located in all countries of operation, the Company does not deem any countries to be of higher risk than others.

Environmental, technological, organizational, and other changes during the period. In December of 20XX, the Company added manufacturing operations in Shanghai, China, through the acquisition of an established brass foundry. At the time of acquisition, the foundry ran its business operations using off-the-shelf software on a local area network. The Company completed migration of all foundry data processes to the ERP system in March of the current year.
The Company is in the process of finishing its new manufacturing facility and upgrading manufacturing and foundry equipment as part of a modernization program. As part of this program, it is modernizing foundry floor equipment, replacing existing manual equipment with new equipment that uses leading industrial control systems. These systems will be integrated with the ERP system to enhance production operations and reporting. The new facility is expected to be operational by November. The process for adding new system components related to this change is subject to the cybersecurity risk management program and controls over those components are implemented as part of the change management process.

DC6: For security incidents that (1) were identified during the 12-month period preceding the period end date of management's description and (2) resulted in a significant impairment of the entity's achievement of its cybersecurity objectives, disclosure of the following: (a) nature of the incident; (b) timing surrounding the incident; and (c) extent (or effect) of these incidents and their disposition

XYZ utilizes a number of both manual and automated security monitoring capabilities to identify security events that occur in the environment. During the period under assessment, the Company experienced an incident that resulted in a compromise of sensitive data from a SQL injection attach on a web application. The attack was detected approximately 66 hours after the event and was remediated within 5 days of detection. XYZ Manufacturing incurred costs related to the notification of and credit monitoring for affected parties (commercial customer information and personally identifiable information of retail customers), as well as fees associated with the retention of outside cybersecurity expertise to conduct forensic investigation of the affected systems and, later, an independent evaluation of security measures to ensure that remediation actions were sufficient to address the identified threats. The incident was fully resolved and remediated, and XYZ has made the necessary adjustments to its systems and processes, as well as to the affected service provider systems and processes, to reduce the likelihood that similar incidents could reoccur.

Cybersecurity Risk Governance Structure

DC7: The process for establishing, maintaining, and communicating integrity and ethical values to support the functioning of the cybersecurity risk management program

Management sets the organizational tone through policies, a code of ethics, a commitment to hiring competent employees, and the development of reward structures that promote an effective internal control and governance structure. The board of directors meets quarterly with members of executive management to review financial and operational performance, including the entity's cybersecurity risk management program.

Employees are required to sign the employee handbook upon hire, acknowledging their acceptance and adherence to the Company's policies and code of conduct. Such policies and the code of conduct have been designed to promote integrity and ethical values throughout the workplace. The information security policy includes information about the following:

- Information privacy, confidentiality, and acceptable use
- Electronic communications
- Data management
- Disclosure

DC8: The process for board oversight of the entity's cybersecurity risk management program

The XYZ board of directors includes various outside directors with industry knowledge and experience including one board member who is a former IT director of an S&P 100 company with 15 plus years of experience in IT and cybersecurity and serves as the board's subject matter expert on cybersecurity matters. Additionally, the XYZ CISO joins the quarterly board meeting to present an overview of the Company's cybersecurity risk management program, including activities of the entity's risk governance committee. Feedback and action items are provided by the board, which is actively engaged in overseeing this key business risk.

The risk governance committee was established to coordinate the risk assessment and management efforts of the entity and its units. The committee, which is chaired by the CRO and consists of the CISO, CCO, external specialists, and IT and business line personnel, ensures that (*a*) cybersecurity risks arising from both internal and external sources are identified and evaluated, (*b*) controls are properly designed and implemented to address all areas as appropriate, and (*c*) controls operate effectively to achieve the entity's cybersecurity objectives. Areas evaluated include systems development, computer operations, program changes, and access to programs and data.

As part of the CISO's quarterly presentations, the results of the XYZ information security team's program assessments are presented and discussed, as well as any corrective action needed as a result of the assessments. The presentations also include summaries of the Company's vendor and business partner oversight program. Under the program, Company personnel perform an annual review of vendor and business partner relationships to evaluate whether the Company is in compliance with industry standards and best practices.

DC9: Established cybersecurity accountability and reporting lines

Under the direction of the risk governance committee, the CISO is responsible for overseeing the cybersecurity risk management program and executing the entity's strategy and other decisions agreed upon by executive management and the board of directors. The CISO reports administratively to the CIO, with an escalation point to the CEO. The CISO presents a quarterly cybersecurity update to the board of directors to report on the state of the entity's cybersecurity risk management program.

The CISO also chairs the information security committee. The information security team, which consists of representatives from all departments in XYZ, is a centralized team of cybersecurity practitioners, subject matter experts, and IT personnel who support the information security operations of the organization (such as systems administrators, software engineers, network engineers, and security analysts). The duties, responsibilities, and hierarchy of employees on the information security team are defined in a role matrix and form the foundation of the entity's cybersecurity risk management program. The information security committee defines and approves the strategy, policies, and standards underlying the entity's cybersecurity risk management program. The results of the annual risk assessment, periodic internal audits, and quarterly external independent assessments are provided to the CISO and the information security committee throughout the year in order to continuously adapt the program to align with new and emerging threats and potential vulnerabilities. The activities of the information security committee are overseen by the risk governance committee.

Alongside the CISO is the CTO, who also reports administratively to the CIO but with an escalation point to the CEO. The CTO is responsible for managing the technology and resources that support the internal operations of the company. This includes overseeing policy and processes regarding relationships with vendors and business partners that may contribute to the cybersecurity risk management program. These

policies and processes are administered through the vendor and business partner oversight program discussed in a later section.

DC10: The process used to hire and develop competent individuals and contractors and to hold those individuals accountable for their cybersecurity responsibilities

Applicants with a role in the cybersecurity risk management program are hired based on their ability to satisfy the job duties and responsibilities of the position and fulfill the goals and expectations of the entity. They are evaluated on their level of education, the merits of their past experience, a positive performance history, and knowledge of relevant cybersecurity controls and processes. Before employment, all applicants must also pass a thorough background check.

Upon hiring, employees are required to sign the employee handbook, acknowledging their acceptance and adherence to the Company's policies and any associated confidentiality and nondisclosure agreements.

Upon hiring and annually thereafter, all employees must successfully complete training courses covering basic information security practices that support the functioning of an effective cybersecurity risk management program. Employees with job responsibilities that fall directly within the cybersecurity risk management program (such as IT personnel, IT management, and internal auditors) have minimum training and continuing education requirements each year.

Employees in the cybersecurity risk management program are encouraged to maintain an active role in relevant cybersecurity information sharing forums, special interest groups, and professional associations to stay up to date on new and emerging cybersecurity risks that may impact the entity or its operating environment.

Contractors are required to follow the same onboarding process as employees and are subject to the same background checks and security awareness training requirements as employees. Employees' and contractors' compliance with security awareness training requirements is monitored on a semiannual basis by human resources.

XYZ has established an entity-wide hierarchy and reporting structure that is codified within an organizational chart maintained on the corporate intranet by human resources. XYZ has prepared a role matrix for employees and managers who have roles within the cybersecurity risk management program. The role matrix defines key job duties and responsibilities in the context of the overall program. Additional information security responsibilities and practices for certain roles within the entity are described in the Company's information security policy and the employee handbook.

All employees go through an annual performance review cycle. At the beginning of each calendar year, employees and their immediate supervisors establish goals and expectations for their job performance over the upcoming year based on the job duties and responsibilities described in the role matrix. Employees then receive a mid-year and year-end performance review from their supervisors that assesses the employees' performance against the agreed-upon goals and expectations. Based on the results of their performance review, employees receive merit increases in compensation and are eligible for bonuses and promotion, respective of their seniority, experience, and position within the organization. Employees whose performance is not in alignment with established goals and expectations for job performance, or who are not fulfilling their job responsibilities, may be referred to human resources by their supervisor to develop a performance enhancement plan.

If an employee violates any statute of the employee handbook or the Company's policies, or otherwise acts in a manner deemed contrary to the mission and objectives of the Company, whether purposefully or not, the employee is subject to sanctions up to and including termination of employment.

Cybersecurity Risk Assessment Process

DC11: The process for (1) identifying cybersecurity risks and environmental, technological, organizational and other changes that could have a significant effect on the entity's cybersecurity risk management program and (2) assessing the related risks to the achievement of the entity's cybersecurity objectives

XYZ maintains a detailed inventory of all information systems, including manufacturing and industrial control systems. All such assets are assigned ownership by a designated department or team within the entity and prioritized based on the asset's business value and criticality to the organization. Information

and data assets are subject to the data management policy that defines parameters for the ownership, classification, security, storage, and retention of data. Software and hardware assets are subject to the information systems management policy that defines parameters for the acquisition, development, maintenance, security and disposal of information system assets.

On an annual basis, the information security team performs a risk assessment that identifies internal and external cyber threats and vulnerabilities to the organization. Information system assets are analyzed to identify associated threats to those assets and vulnerabilities that may be exploited. The resulting risks are then scored based on their likelihood and potential impact to the organization. The assessment includes consideration of the inherent and residual risks that may reside with external parties and the cybersecurity controls to address those risks. Specific policies and procedures are in place to assess and manage the requisition and engagement of vendors or business partners with consideration for the cyber threats and vulnerabilities such relationships may present.

Results of the risk assessment are evaluated by relevant management against criteria for risk acceptance to identify new or existing protective measures and develop or enhance information security policies and procedures.

Internal audit conducts periodic cybersecurity assessments that include working with process owners and IT support personnel to identify specific security threats and vulnerabilities and to identify how the associated risks are being addressed. Additionally, quarterly vulnerability assessments and penetration tests are performed by an external party to identify specific technical threats and vulnerabilities.

DC12: The process for identifying, assessing, and managing the risks associated with vendors and business partners

XYZ considers the inherent risk of working with vendors and business partners as part of the annual risk assessment performed by the information security team. Internal and external cyber threats and vulnerabilities are identified and assessed based on the likelihood that they could prevent the entity from achieving its cybersecurity objectives. Specific policies and procedures are in place to assess and manage the requisition and engagement of vendors. Consideration is given to the cyber threats and vulnerabilities such relationships may present and whether XYZ's controls reduce such risks to a level consistent with XYZ's cybersecurity objectives and risk acceptance.

XYZ has established a tiering system in which each vendor is assigned a tier (1–3) based upon the inherent risk of the goods and services the vendor provides, the overall operational significance of the vendor to achieving XYZ's business objectives, and the sensitivity of data that resides within the vendor's environment. Business partners are evaluated using the same tiering structure, based on the cybersecurity risk associated with each business partner.

The entity's vendor and business partner oversight program requires that all contracts with vendors or business partners clearly address (*a*) the size, scope, and nature of services being provided; (*b*) the hardware, software, and information requirements related to the provision of such services; (*c*) the responsibilities of each party; (*d*) the requirements for information security to meet XYZ's standards; (*e*)

the ability to perform independent audits of the effectiveness of internal control processes; and (*f*) the requirement to obtain and review a third-party attestation report.

Disclosure of any confidential or personally identifiable information (PII) to a vendor or business partner is provided only on an as-needed basis and only if the vendor or business partner has enacted appropriate information security and privacy controls. All vendors and business partners with access to confidential information are subject to confidentiality and privacy agreements and other contractual confidentiality provisions, which must be signed and acknowledged before access to XYZ's systems and data is granted.

The vendor and business partner oversight team ensures that XYZ and its vendors and business partners stay current with existing contractual obligations, information security and privacy regulations, certification compliance requirements, and industry standards. The vendor and business partner oversight team performs an ongoing annual review of vendor and business partner relationships to (*a*) reevaluate the services provided and any cybersecurity threats and vulnerabilities arising from the relationship; (*b*) consider whether the assessed risks are being addressed appropriately by each party's contractual agreements, information security controls and processes; and (*c*) evaluate whether the entity's vendor and business partner oversight program complies with industry standards and best practices. The review process includes obtaining security questionnaires, conducting personnel interviews, performing walkthroughs, performing site visits, and conducting IT scanning and testing. In addition, when available, the review process may also include obtaining and reviewing third-party attestation reports.

The CISO and the information security team participate in cybersecurity information sharing forums, special interest groups, and professional associations to increase information sharing between knowledgeable parties and to stay up to date on changes in the regulatory, economic, and physical environment in which the Company operates. As an international manufacturer, XYZ Manufacturing maintains communicative relationships with relevant governing and regulatory bodies to stay abreast of changes to laws and regulations that impact the organization as they arise.

Internally, consideration of the entity's cybersecurity risk management program is an integral part of proposed changes to existing business lines or operations, the development or acquisition of new business lines or operations, decisions about doing business in new geographies or markets, and the adoption of new technologies or processes throughout the business. The information security team, led by the CISO, is involved in the decision-making process related to changes that could impact the size, scope, or operational nature of the business. In this capacity, the team may perform ad hoc, focused risk assessments to identify new risks to the organization and associated impacts to be considered during the decision-making process; the team may also reevaluate the design of controls to ensure continued protection.

Additionally, on an annual basis, the information security team performs a full risk assessment that identifies internal and external cyber threats and vulnerabilities to the organization. During the annual risk assessment, the team considers both internal changes to XYZ operational processes (such as new or modified lines of business, new or modified operating procedures, new geographies or markets, new technologies or services used) and external changes (such as new or changing regulatory requirements, industry standards, economic circumstances, emerging risks) that could affect the entity. New controls are designed in response to identified threats and existing controls are assessed to ensure they reflect changes to the size, scope, and operational nature of the business.

Cybersecurity Communications and Quality of Cybersecurity Information

DC13: The process for internally communicating relevant cybersecurity information necessary to support the functioning of the entity's cybersecurity risk management program, including (1) objectives and responsibilities for cybersecurity and (2) thresholds for communicating identified security events that are monitored, investigated, and determined to be security incidents requiring a response, remediation, or both

The internal communication of cybersecurity information for employees according to their role in the cybersecurity risk management program is described in the XYZ information security policy, which is available to all employees on the Company intranet. Additionally, the employee handbook identifies certain information security responsibilities and practices, depending on the employee's role within the organization. At the time of hiring, all employees must provide sign-off, acknowledging acceptance of and adherence to the Company's policies.

Upon hiring, and annually thereafter, all employees must successfully complete training courses covering basic information security practices that support the functioning of an effective cybersecurity risk management program. The training courses are designed to assist employees in identifying and responding to social engineering attacks (phishing, tailgating) and in avoiding inappropriate security practices (for example, writing down passwords or leaving sensitive material unattended). XYZ periodically assesses employees' awareness of corporate policy by attempting to tailgate into buildings, sending simulated phishing emails, and performing desk sweeps, among other tactics. If an employee is found to be violating Company policies, additional training is provided or other disciplinary actions are taken.

Employees with job responsibilities that fall directly within the cybersecurity risk management program (IT personnel, IT management, internal audit, and the like) have additional requirements to complete technical and job-specific training throughout the year. Additionally, those employees who have direct access to customer and employee data (for example, sales, customer service, human resources, IT helpdesk, and finance) will receive specific training around incident management, information handling, and data protection.

Training and other programs related to employee cybersecurity awareness incorporate materials developed internally by XYZ in collaboration with industry- and cybersecurity-focused vendors or business partners. These vendors or business partners provide expertise and tools to develop, perform, track, and test employees' compliance with cybersecurity-awareness policies and standards.

XYZ has established a cybersecurity awareness program (CAP) that periodically distributes reminders of information security practices to all employees and sends internal communications to promote security awareness and to provide the latest security news. CAP is also responsible for (*a*) monitoring cybersecurity risk associated with vendors and business partners who have access to the entity's system; (*b*) monitoring forums and news sites for information regarding potential breaches; (*c*) reviewing vendors' and business partners' cybersecurity examination reports on an annual basis; and (*d*) maintaining ongoing, direct contact with vendors and business partners to address any issues identified.

On an annual basis, XYZ updates the cybersecurity training program and CAP to incorporate changes in the threat landscape and new tactics being executed by threat actors. XYZ also evaluates lessons learned from any previous incidents and incorporates changes into the programs as necessary.

An incident hotline is available to all employees to report information security events they have been involved in or witnessed (such as phishing attacks, malware, lost or stolen devices, and inappropriate information disclosure). XYZ receives a quarterly attestation from the outsourced call center that all hotline personnel have completed XYZ's CAP and are aware of defined policies related to information protection, data handling, and incident response.

The CISO presents a quarterly update to the board of directors to report on the state of the entity's cybersecurity risk management program. During the update, the CISO presents the status of ongoing efforts to develop and maintain the program in response to (*a*) prior security events at the organization, (*b*) changes in XYZ's operational procedures, (*c*) changes to legal and regulatory requirements affecting the organization, (*d*) results of audits and testing by internal and external parties, and (*e*) new and emerging cybersecurity risks to the organization.

DC14: The process for communicating with external parties regarding matters affecting the functioning of the entity's cybersecurity risk management program

XYZ has a disclosure policy defining when, by whom, and to what extent external parties are informed of matters relevant to the functioning of XYZ's cybersecurity risk management program. All disclosures to external parties are made in accordance with applicable laws and regulations at the state and federal level. Any such legal requirements are considered in the development and maintenance of the disclosure policy during annual review. Employees are educated on the policies and procedures for reporting and disclosing cybersecurity incidents or events through the XYZ information security policy and XYZ Employee Handbook.

XYZ may become aware of matters affecting the functioning of the entity's cybersecurity risk management program via its existing monitoring processes, as well as via notification by third parties or law enforcement. When such matters arise, they are immediately reviewed by the XYZ risk governance committee to determine relevance and applicability. Where necessary or appropriate, the matter may be treated as a security incident and handled via XYZ's security incident response process, as described later.

As is typical business practice by most organizations, XYZ restricts communication of matters related to the functioning of XYZ's cybersecurity program to only those stakeholders and business partners who have a need to know such information. This information may be communicated via mediums appropriate to the nature of the information and the urgency of the situation, and may include conference calls, electronic mail, memoranda, or in-person meetings. In the rare instance when public disclosure of such matters would be necessary or appropriate, XYZ's legal counsel and corporate communications representative are responsible for jointly distributing and communicating such disclosure.

Monitoring of the Cybersecurity Risk Management Program

DC15: The process for conducting ongoing and periodic evaluations of the operating effectiveness of key control activities and other components of internal control related to cybersecurity

XYZ uses several mechanisms to assess the ongoing effectiveness of internal controls designed to mitigate cybersecurity risks. Assessment and monitoring of the program are designed to meet the requirements of the NIST cybersecurity framework and ISO 27001.

Internal audit conducts periodic cybersecurity assessments and tests of internal controls that include (*a*) working with process owners and IT support personnel to identify specific security threats and vulnerabilities and how the associated risk is being addressed and (*b*) tests of the design, implementation, and operating effectiveness of internal controls that address cybersecurity risks. Members of the internal audit team have the requisite knowledge of and experience with cybersecurity risks and controls.

XYZ also uses external parties to independently evaluate the state of the cybersecurity risk management program. Quarterly vulnerability assessments and annual penetration tests are performed by an external service provider to identify specific technical threats and vulnerabilities and to benchmark the environment against leading cybersecurity practices. In addition, the entity obtains for its SaaS vendor an annual web application security assessment report. Every two years, XYZ engages a service provider to perform an independent assessment of the cybersecurity risk management program to evaluate alignment with leading industry practices and consistency with Company policies in order to identify gaps and potential opportunities for improvement.

Both internal and external evaluations are made using a risk-based approach that may vary the nature, timing, and extent of testing. The criteria for such evaluations, including the nature and frequency of such evaluations, are reviewed during the annual risk assessment and modified as needed, with consideration for changes to XYZ's operational processes, including changes to the size, scope, and operational nature of the business, recent security threats or incidents, new or emerging risks, and changes in industry standards.

DC16: The process used to evaluate and communicate, in a timely manner, identified security threats, vulnerabilities, and control deficiencies to parties responsible for taking corrective actions, including management and the board of directors, as appropriate

On a quarterly basis, the information security team performs a risk assessment update that identifies changes to internal and external cyber threats and vulnerabilities to the organization. Results are

evaluated by the risk governance committee, to identify whether new protective measures or enhanced information security policies and procedures are needed. The risk governance committee is also tasked with monitoring vulnerabilities, allocating resources to address them, and reprioritizing remediation initiatives, as necessary. Key performance indicators related to average closure time have also been defined and are monitored by the committee on a monthly basis.

The results of all monitoring activities, regardless of source, are entered into a vulnerability tracking system for evaluation and identification of remediation activities that may be needed. Identified vulnerabilities are assessed with regard to the likelihood and magnitude of exploitation. All vulnerabilities evaluated are identified for remediation or additional monitoring. Responsibilities for corrective action plans are assigned and completion dates determined. The information security committee reviews the list of open vulnerabilities on a monthly basis to monitor progress toward resolution and to identify trends and responses. On a quarterly basis, the risk governance committee and executive management receive summary reports of vulnerability management activities. In addition, the CISO presents cybersecurity risk management program results, including vulnerability management activities, to the board of directors during each of its regularly scheduled meetings.

Cybersecurity Control Activities

DC17: The process for developing a response to assessed risks, including the design and implementation of control processes

A risk governance committee was established by XYZ to coordinate the risk assessment and management efforts of the entity and its units. The committee, which is chaired by the CRO and consists of the CISO, CCO, external specialists, and IT and business line personnel, ensures that risks are evaluated and that controls are designed, implemented, and operated to address all areas, as appropriate, to detect, respond to, mitigate, and recover from security events based on the assessed risks. Areas for evaluation include systems development, computer operations, program changes, and access to programs and data. Implemented controls include preventive and detective controls, such as manual, automated, or IT-dependent controls based on the environment in which the entity operates; the nature and scope of the entity's operations and its specific characteristics.

Business processes are documented in standard operating manuals; however, the risk governance committee also has business operations liaisons in each business area that are responsible for the ownership and documentation of key risk areas for the business operations. In 2014, the risk governance committee enhanced their key risk considerations for business areas to include specific consideration of cybersecurity risks.

The risk governance committee business liaisons annually revisit the risk assessments and validate the existence of controls to mitigate identified risks. The controls are captured in the Company's controls repository (CR), which is an inventory of the operations, risks, and controls associated with each business area. The CR is used to conduct quarterly self-assessments of controls and also serves as an input into the Company's annual controls maturity assessment, which is conducted by internal audit and reported to the risk governance committee.

The Company contracts for insurance coverage, including business disruptions, for risks which cannot be cost effectively mitigated through other techniques.

DC18: A summary of the entity's IT infrastructure and its network architectural characteristics

XYZ employs both internally hosted and cloud-based applications to support its manufacturing, retail, and wholesale operations. Cloud-based applications are provided through an arrangement with ABC Cloud under a service contract whereby XYZ retains the responsibility for specific server configuration and operating system change management, and ABC Cloud provides server support and maintenance. Company applications run primarily on Unix family operating systems and use industry standard database management systems. The manufacturing system uses a proprietary midrange operating system supplied

by a leading IT manufacturer. The application was developed in house using the integrated operating system database. Field sales application tablets use an industry standard operating system.

XYZ has segmented its ERP financial reporting systems from its externally facing retail, wholesale, and call center interfaces through the use of Cisco ASA firewalls, which are configured, managed, and supported by XYZ IT personnel. The firewall configurations and rules follow standards created by XYZ IT management under the direction of the CISO. All connectivity to external users occurs through defined access points protected by a redundant firewall complex. Firewalls are also used to segment the network within the Company.

Wholesale call center services are outsourced, with the call center's systems interfaced with the ERP system to facilitate ordering and problem resolution. The interface with the call center is over a virtual network connection. Custom-developed software is used to interface the call center system to the ERP interface.

The call center service provider facilities are reviewed annually by XYZ through their previously defined vendor and business partner oversight program. These vendor and business partner assessments focus on areas specific to the security configurations of the hosted applications, as well as to the network architecture related to XYZ's interfaces to the vendors.

ABC Cloud's SaaS is also reviewed annually through XYZ's vendor and business partner oversight program; however, given the nature of the responsibilities defined within the cloud agreement, XYZ configures its server settings in line with XYZ's corporate standards. XYZ has defined a standard build for cloud-based server configurations and uses that as the baseline from which servers are configured to support the SaaS environment. Also, monitoring of the configurations for adherence and compliance with defined standards is conducted by XYZ IT support personnel, as well as through the corporate internal audit and risk management teams.

Field sales automation is provided through the use of Company-owned tablet devices running third-party software customized for the Company. Tablets access the ERP system through a cellular-based VPN system that uses two-factor, token-based authentication.

DC19: The key security policies and processes implemented and operated to address the entity's cybersecurity risks, including those addressing the following:

- **a*. Prevention of intentional and unintentional security events***
- **b*. Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents***
- **c*. Management of processing capacity to provide for continued operations during security, operational, and environmental events***
- **d*. Detection, mitigation, and recovery from environmental events and the use of backup procedures to support system availability***
- **e*. Identification of confidential information when received or created, determination of the retention period for that information, retention of the information for the specified period, and destruction of the information at the of the retention period***

XYZ has defined a set of information security standards and policies that are under the direction and ownership of the CIO and implemented through the CISO. The standards and policies address the management and implementation of security controls, ranging from the physical security of facilities and equipment to the logical security at the data element layer. The information security policies and standards are designed to provide information to employees, contractors, and vendors that is aligned to their job or functional responsibilities, while also contemplating segregation of functions that may otherwise create a segregation of duties conflict.

Security policies are published on the Company's intranet, included in onboarding packages, and reiterated through annual training that all employees are required to take and acknowledge. Security

policies related to relationships with vendors and business partners are enforced through contractual commitments and related service-level agreements (SLAs) and, where possible, are monitored for adherence through XYZ's vendor and business partner oversight program.
The key components of the XYZ information security policy are discussed in the following paragraphs.

Prevention of intentional and unintentional security events. The Company has the following processes in place to prevent intentional and unintentional security events:
Physical and Logical Access Provisioning, De-provisioning, and Transfers (Including Remote Access). XYZ employees are granted network access only after completing security-awareness training. Users are granted access to XYZ systems and data based on their job role. Access requests are approved by the user's manager prior to access being granted. Upon termination, human resources sends a notification through the ticketing system, which is routed to the user administration team to remove user account access for the terminated user. Human resources provides a weekly list of terminations, which is then cross-referenced against the user account list to identify any user accounts that have not been properly terminated. User accounts that are inactive for 60 days are automatically disabled. For access modifications, the user's manager is required to submit and approve an access request ticket via the ticketing system, which is routed to the user administration team for processing.
Authentication. Users are required to authenticate using a unique user ID and password before being granted access to the network. The network domain password policy is configured to include password minimum length, expiration intervals, complexity, history, and an invalid password account-lockout threshold. A new user's account password is set to pre-expire so that the password must be reset the first time a user logs in to the network.

Credentials Management. Access is granted based on role-based security profiles that provide segregation of duties and limit transaction access. XYZ application and data owners review access rights on a semiannual basis. On an annual basis, the roles and the transactions assigned to the roles must be reviewed.

Privileged User Management. Access to privileged user or superuser accounts is authorized by management. Users with privileged user accounts are provided with a standard (nonprivileged) user account for use on a daily basis (for email and personal productivity software), and are only permitted to use their superuser accounts when performing administrative tasks. All superuser account access is logged and monitored. On a quarterly basis, the user administration team performs an access review of privileged access.

*Database Security***.** Database administrators are the only individuals that can access XYZ databases. All database access and activity are logged. Database account access is reviewed twice a year for continued appropriateness. Direct data changes require approval, which should be documented within the Company's ticketing system and handled via the change management process.

Data Loss Prevention (DLP). The Company has a DLP solution that monitors and provides alerts about (and can take action regarding) the transmission or removal of confidential data outside of the Company or on noncompany-owned devices. The DLP solution is configured to encrypt external storage devices and prevent the saving of sensitive data to removable media. Hard drives of all servers, workstations, and laptops are encrypted. XYZ Manufacturing and its vendors utilize transport layer security for encryption of transmissions across the Internet to XYZ web servers and the email system. A VPN requiring multifactor authentication is used for all remote access to XYZ's internal network, ensuring that data is encrypted in transit when sent across the Internet from a Company computer system. Site-to-site VPNs are also utilized with certain XYZ vendors to provide encrypted channels for communication between locations.
Data Destruction. Data that exceeds its retention period is removed from systems and all backup media. Data that is labeled as confidential is erased using secure deletion techniques approved by the U.S. government (multi-pass overwrite). All computer hard drives are required to be securely deleted before disposal, and a certificate of destruction is obtained from the third-party organization that disposes of all computer equipment for XYZ.

Data Backup. Nightly incremental backups of all production servers and daily backups of production databases are conducted. Every month end, the Company is required to perform a full backup of the production servers. Backup tapes are encrypted and sent to a third-party vendor for storage. An automated backup system is implemented to monitor the completion of scheduled backups. When a backup job is not completed successfully, operations personnel create an incident ticket and assign personnel to resolve the failure.
Virus Detection and Prevention. Antivirus software is required to be installed on all XYZ servers, desktops, laptops, and email infrastructure and is centrally managed to ensure timely delivery of signature updates. The antivirus software settings are preconfigured for automatic updates and locked to prevent any user tampering or disabling. Email filtering software is in place to restrict and reject emails that contain certain malicious file types, including executable files. The Company's antivirus administrator is required to perform a quarterly inventory reconciliation against a system inventory list.
Firewalls and Perimeter Security. XYZ Manufacturing deploys enterprise firewalls at the perimeter of the network and in other strategic locations throughout the network in an active failover configuration. Only a minimal number of ports and services are allowed into the XYZ environment. All firewalls are managed using a centralized console, and XYZ installs monitoring software on the firewalls to provide alerts when changes occur at the administrative level. Firewall rulesets are reviewed twice a year to ensure that they are appropriately configured.
Secure System Configuration. Configuration specifications are installed on all systems before they are implemented into production. Monthly vulnerability and configuration scans to validate that all systems remain configured in accordance with XYZ's security hardening standards are performed. When updates to existing standards are made, the changes are implemented on production systems.

Intrusion Prevention. A threat intelligence database is regularly updated. Packets identified by the threat intelligence database that meet a certain risk threshold or exhibit certain characteristics are automatically dropped and prevented from entering the XYZ network.

Change Management. A change approval board (CAB) that consists of representation from all IT departments within XYZ is in place. On a weekly basis, the CAB meets to review upcoming system and application changes, which are requested via the Company's online ticketing software. All changes are required to have a documented back-out plan. All changes are required to have a documented test plan. All members of the CAB approve a change before it can be implemented. In the weekly CAB meeting, the previous week's changes are reviewed. A root cause analysis report is completed for any changes that did not go as planned before they can be reconsidered.
Application Changes. Change requestors submit a change request within the Company's ticketing system. An application analyst reviews the change request and develop a project change budget estimate. On a monthly basis, application change requests and associated budgets are reviewed and categorized by IT and the business owners and ranked according to priority. Development occurs in a development environment that is separate from the production environment, using test data. Once development is completed, user acceptance testing takes place. Once user acceptance testing is completed, the business owner who sponsored the change and the applicable application analyst are required to approve the change within the ticket. The IT operations team migrates changes into production after they have been approved by the CAB. Emergency changes are required to be documented and logged in the ticketing system after changes are completed, and the CAB conducts an after-action review to approve the changes retroactively.

Patch Management. When new patches are released, they are reviewed by a group of IT personnel, including a representative from the information security team. The team assigns a priority level to each patch. Patches that are assigned a rating of "critical" are applied to all affected systems within 7 days. Patches that are assigned a rating of "high" are applied to all affected systems within 30 days. Patches that are assigned a rating of "medium" are applied within 60 days. All other patches are applied in regular system updates that typically occur quarterly. Once assigned a patch criticality rating, a patch is assigned to the appropriate IT system administrator for evaluation and testing in the XYZ test lab. When testing is completed, a change ticket is entered in the ticketing system, and the patch is reviewed and approved by the CAB. Monthly, the information security team is required to conduct vulnerability scanning of all

systems to ensure that patches are properly in place. Any missing patches are immediately ticketed and a resolution is required within 5 business days.

Detection of security events, identification of security incidents, development of a response to those incidents, and implementation activities to mitigate and recover from identified security incidents. Due to the pervasive use of IT to conduct business operations and deliver products and services to customers, the ability to detect a security event in a timely manner is of significant importance. Accordingly, XYZ Manufacturing has defined formal key security policies and processes focused on identifying cybersecurity issues to detect security events. These policies and processes are focused on the following:

- Utilizing continuous security monitoring tools and programs to assist in identifying anomalies within the network and supporting infrastructure environment—inclusive of security event information relevant to third-party vendors
- Implementing security monitoring processes and procedures and other measures to identify anomalies in information flow, access, data communications, and the operation of business-critical systems
- Analyzing anomalies to identify security events and to detect abnormal events or data movement using historical baseline or behavioral analytics data to determine what is considered to be abnormal
- Escalating identified security events that occur through the course of business operations and ongoing communications, both within and outside of the organization

*Detection of Security Event*s. A dedicated security team is available 24/7. Administrative activity and supporting infrastructure components are monitored through manual analysis and automated alerts where risk-based security monitoring, or a triage approach, is performed based on inherent risk of the anomaly or security event detected and the potential impact that said event could have on the Company's business operating environment. Security monitoring procedures are documented and consistently followed; documentation updates are made to the relevant security monitoring procedures related documentation when required or when significant procedure-related changes are made. Regular security monitoring and detection-based reporting capabilities with metrics are mapped to business drivers for security monitoring purposes. Vendor-related and custom signatures are updated regularly based on threat intelligence information gathered for security-detection purposes. Centrally stored or monitored logs are maintained, and correlation and alerting capabilities are performed on a limited basis when unusual activity is suspected based on the information gathered from the security incident and event management (SIEM) system.
Development of a Response Plan. The incident response sections of the Cybersecurity Incident Response and Recovery Plan (CIRP) includes tactical procedures to help "triage," contain, monitor, or eradicate a security incident, including procedures to do the following:

- Respond to, recover from, and restore normal business operations in a timely manner with minimal, or no, business interruption or loss of data
- Continuously improve the cybersecurity risk management program to limit the likelihood and impact of future incidents based on lessons learned from the Company's own experiences and those of others
- Communicate with employees, stakeholders, regulators, and other constituents in a structured manner about the nature of the security incident, impact to the organization and others (if applicable), and the corrective action taken to recover

The incident response sections of the CIRP have been created based on a threat scenario risk assessment performed annually as part of the review of the plan. The plan is focused on responding to those threat scenarios that have the highest impact and likelihood of occurring based on the business and markets in which the Company operates and the current technology environment. The incident response sections of the CIRP include the following key information:

- Response plan owners (those who can activate the plan), team members, and contact information for plan owners and team members
- Defined criteria required to activate the response plan
- Target business and IT performance metrics for operating in a “business as usual” environment
- Linkage to the business impact analysis and critical path recovery items within the disaster recovery (DR) and business continuity (BC) plans
- Alternate internal and external communication and operating methods to use when primary methods are unavailable
- Communication plan for notifying internal stakeholders (including legal, human resources, marketing, and investor relations), retained service providers (external counsel, forensics investigators, and the like), and external stakeholders (such as customers, vendors, regulators, and law enforcement) to manage expectations and information disclosure as part of the overall response effort. The communication plan also includes communication templates for certain formal internal and external communications, including, but not limited to, internal IT outage notifications and public press releases
- Facility recovery procedures providing linkage to the DR and BC plans regarding the hosted hot site facility located in Syracuse, NY, and the alternate call center located in Troy, MI
- Data response procedures providing linkage to the backup policies and procedures, as well as the DR plan, regarding offsite data storage and backup media
- Hardware and software access procedures enabling IT service and operations during response and recovery procedures
- Response and recovery metrics focused on the target response and recovery milestones to enable effective management, measurement, and monitoring of recovery activities
- Detailed incident response and recovery procedures to be executed based on the identification of the root cause, including operational steps to eradicate any infections, malicious code, unauthorized user accounts, and the like, and restore systems in accordance with priority and dependencies

It should also be noted that mitigating processes and controls are evaluated as part of the current CIRP-related processes and controls in place to detect and respond to security incidents and events. (These mitigation process and control factors may be directly related to the CIRP or may be part of other security monitoring related controls.)

The CIRP is reviewed annually and approved by the following members of management:

- CISO
- CIO
- CTO
- CRO
- GC
- Chief Marketing and Communications Officer
- Director, Security Operations
- Director, Crisis and Response Management

Implementation Activities to Mitigate and Recover from Identified Security Incident. The plan activation process begins when one or more of the incident response and recovery plan owners are informed of a cybersecurity event for which incident response is imminent or underway. The plan owner will ensure details about the cybersecurity event are clearly understood and documented to the extent necessary to enable future communications. This includes the identification of security monitoring or other mitigating processes and control factors which may be present and reduce the overall impact of the identified security event. Should the plan owner decide to activate the plan, he or she will convene an emergency

meeting of the CIRP leadership team (including the CIO, CISO, CRO, GC, VP of human resources, and CFO) to determine

- immediate tasks,
- departments and functions required to carry out the plan based on the cybersecurity event,
- the initial communication plan and the individual assigned to execute the plan.

Once agreement is made, the leadership team is responsible for notifying members of their teams and others, including external advisors (such as investor relations and external general counsel) about the plan activation, initial decisions made, and assigned actions.

Once activated, XYZ considers the current cybersecurity event and its effects on systems and business operations. The Company refers to the appropriate sections of the BC and DR plans, as well as the relevant and applicable data backup logs, to identify the following:

- Where the IT systems and IT infrastructure affected by the cybersecurity event reside within the asset prioritization hierarchy
- Where the business operations affected by the cybersecurity incident or event reside within the operations prioritization hierarchy
- The planned alternative IT systems (such as the failover or load-balanced servers and network devices) and business processing activities (for instance, manual sales order forms) for the effected components of the environment
- The time prior to the cybersecurity incident or event from when the Company will be able to respond to and recover from (recovery point objective [RPO]) for the affected IT systems and IT infrastructure
- The maximum length of time until IT systems, IT infrastructure, and business processes affected by the cybersecurity incident or event is returned to normal business operation, after which significant negative impact may occur (recovery time objective [RTO])

For each IT asset (hardware and software, including virtualized assets) affected by the cybersecurity event, an evaluation will be made to determine the appropriate response and recovery actions, such as the following:

- Decommission and replace
- Reconfigure with enhancements (firmware updates, vendor patches, configuration changes)
- Reconfigure with no enhancements

Recognizing that the Company may not be able to complete the chosen recovery action in a timely manner in relation to the RTO, an alternative solution will be determined to enable a return to normal processing.

Data restoration is based on the activities outlined in the backup and recovery policies and procedures. The backup procedures apply to the following:

- Network devices—such as configurations, access control lists, and firmware
- Physical and virtual servers (DNS servers, email servers, FTP servers, application servers, database servers, web servers)—operating systems, application programs, and application data
- Networked file shares
- End user computing (desktops, laptops, tablets, mobile devices) and peripherals (such as printers and copy machines)
- Telephone and voicemail systems

XYZ Manufacturing leverages a global backup management solution to manage the backup processing and monitoring of all IT assets connected to the environment. The backup solution is connected to a virtual storage area network (SAN) and supplemented by real-time disk imaging to an offsite facility for the highest-value IT assets and data. Moderate- and lower-value information and IT assets are backed up to electronic, removable media and stored at a secure offsite facility for the period of time defined by the

backup and recovery policies and procedures. Backup method and frequency is based on the volume and frequency of information processing and the importance of the data or IT asset.

Restoration of data, software, and configurations is made using the global backup management solution. Prior to restoring data, software, and configurations to the live environment, the Company will conduct tests in the security sandbox against the backup media to determine if the cybersecurity event is present. Based on results, the Company may seek to leverage an older backup or execute the eradication techniques that were successfully employed in the production environment.

Communications related to a cybersecurity event are governed by the CIRP leadership team. Throughout recovery efforts, XYZ will communicate to the extent possible, and as required, with employees, stakeholders, regulators, or law enforcement through formal written and verbal communications (email, press releases, mass voicemail) that are structured to be informative, easy to understand, and transparent and that address the following:

- Current understanding of the cybersecurity incident or event
- The known impact of the cybersecurity incident or event
- The current status of remedial action being taken in response to the cybersecurity incident or event

Communications are tailored to specific audiences (all employees, individuals of whom specific action is required, public domain), leveraging templates that have previously been created and preapproved by appropriate members of executive management and external advisors.
Within ten business days of returning to "business as usual," the CIRP requires a formal meeting of the full cybersecurity incident response and recovery team. The purpose of the meeting (which may be held via teleconference, videoconference, or in person) is to discuss lessons learned from the event and additional actions required. Defined criteria are included within the CIRP to help determine the structure of the meeting, the documentation required, and the monitoring that will be performed to ensure any new correction action agreed upon or implemented since the occurrence of the cybersecurity incident or event continues to operate over a period of time. During the meeting, at a minimum, the following are discussed:

- Identified breakdown in processes or controls, if any
- Enhancements that may need to be made to the process for identifying security monitoring or other mitigating processes and control factors which may be present in the environment and reduce the overall impact of the identified security event, prior to plan activation
- Changes required to standard configurations and the status of changes to other comparable systems that have yet to be attacked (as well as confirmation that those systems have not been compromised)
- Changes to the CIRP or the response team that would benefit incident response or recovery capabilities
- Capital investments or additional operating expenses required to more effectively prevent or detect a similar cybersecurity incident or event
- Changes to business partner relationships that may enable better response or recovery actions to be taken for future cybersecurity incidents or events
- Changes to CIRP test scenarios

The meeting minutes from the discussion are documented and appended to the CIRP.

Once per quarter, as part of the crisis management and incident response readiness activities, formal tests of response and recovery procedures are performed. Tests are based on overall-business-based scenarios that have been developed to confirm awareness of and education about the CIRP and related plans (such as the DR and BC), as well as to hone plan content in an effort to continuously improve response and recovery capabilities.

Tests performed during three of the four quarters are "tabletop" exercises in conference rooms, leveraging tele- and videoconferencing as necessary to conduct a virtual simulation with the CIRP team and other stakeholders. Tests performed during the other quarter involve a real-life simulation where a

simulated cybersecurity incident or event is triggered. Only the CIRP leadership team is initially aware of the simulation. XYZ executes the response and recovery plan in a “real life” situation until the point when communication with internal and external stakeholders would be required. The Company then completes the simulation as if it were a real event. Test results produced from this simulated event are formally discussed; ongoing updates are made to the CIRP as deemed necessary.

Management of processing capacity to provide for continued operations during security, operational, and environmental events. Policies and processes are implemented to address capacity management and include the use of the Information Technology Infrastructure Library (ITIL) IT service management framework for capacity management. Performance management and capacity monitoring tools are used to real-time information to the network operations centers. Alert levels are established based on asset priority and failover capability for the load-balanced and redundant components. Alerts may be in the form of a yellow or red color indicator on the operator console within the network operations centers. The automatic creation of a problem ticket in the service management system for investigation and resolution, or an automated text and email to the on-call IT operations lead, is acceptable.

Detection, mitigation, and recovery from environmental events and the use of backup procedures to support system availability. Policies and processes are implemented to address the detection, mitigation and recovery from environmental threats. The primary computer facility houses key IT infrastructure for the Company’s integrated ERP system and midrange platforms supporting manufacturing software. The facility has been specifically designed to mitigate the risk of environmental threats to the computer hardware operations and include protection from fire and the loss or fluctuation of power, cooling, and humidity.

Fire suppression systems, in combination with smoke detection and hand-held fire extinguishers, are installed throughout the Company’s facilities. Preventive maintenance is performed annually along with required inspections. An uninterruptible power supply (UPS) system provides continuous conditioned power through its strings of batteries to all infrastructure hardware to control unanticipated power interruptions. Maintenance for the UPS and batteries is performed at least quarterly. Emergency generator systems are required to be installed within the secure perimeter of the data center facilities. They are sized to provide 100 percent of the data center’s electrical service in the event of a utility service failure. These generators have scheduled maintenance performed at least quarterly. The temperature and humidity inside the data center is controlled by dedicated air conditioning systems for computer hardware. These units act independently of any general building air conditioning. Maintenance is performed at least tri-annually. The data center environment, temperature, humidity, power, and fire prevention systems are required to be monitored through a building management system within the command operations center. Operations personnel man the facility 24 hours a day, 7 days a week.

Physical Access. Access to the computer facility entrances and to the network operations centers (including the raised floor areas) is controlled by the badge access reader system. Building access points are required to be locked at all hours except for the main entrance, which can be unlocked during normal business hours and manned by a security guard. At each facility entrance, visitors are required to provide relevant identification, such as name, representing company, and employee contact. All visitors receive a visitor badge and sign in on the visitor log. All personnel are required to display their badge at all times while in the facility. Visitors are escorted while in restricted-access areas of the facility; when leaving, they are required to sign out on the visitor log. Video cameras are monitored 24/7 and provide surveillance over the interior and exterior of the building. All camera activity is recorded on digital video and retained for at least 60 days.

Backup Media. Data and programs are backed up in accordance with defined schedules. The backup schedule, rotation schedule, and retention period of tapes at the offsite storage facility are determined based on business need. The offsite tape storage is located approximately 30 miles from the computer facility. Backup job failures are monitored and tracked to resolution through the incident management process. Monitoring tools established in the job scheduling and monitoring process are utilized to monitor backup jobs. Job monitoring tools are in place to automatically generate an incident ticket in the incident management system for backup failures. Tape management systems are used to manage tape activities in the data center. Features of these systems include onsite media inventory, offsite media inventory, picking list for the vault, distribution list for the vault, and scratch lists.

The tape management systems produce reports to facilitate tape movement between the tape racks and drives in the data center as well as between the data center and the offsite facility. Tape rotation is monitored. Reports are reconciled daily and discrepancies are evaluated and resolved. Periodic inventories of tapes located both onsite and at the offsite facility are required to be conducted. Backup media is periodically tested. Periodic testing of backup media is coordinated by the business continuity team and performed by the appropriate technology groups.
Alternate Processing. BC plans are in place for all major business units and updated on an annual basis. DR plans are in place to support BC plans covering the critical IT infrastructure and networking equipment. The DR plan is updated annually. The main data center is physically separated from business operating units and dedicated solely to processing functions. The DR plans are reviewed annually and tested at least once a year. During a testing exercise, locations that are part of the testing exercise access the DR location through VPNs to segregate the network and prevent interruption to production services.

All business units with RTOs of less than 72 hours participate in a DR exercise once every three years. Business units with RTOs of 48 hours or less participate in the recovery testing exercise on an annual basis. The results of the tests are documented and assembled into a problem and resolution log.

Identification of confidential information when received or created, determination of the retention period for that information, retention of the information for the specified period, and destruction of the information at the of the retention period. Policies and processes are implemented to address capacity management and include the following:
Data Classification and Retention. The data classification and retention policy and relevant security and confidentiality policies describe how information is designated as confidential and ceases to be confidential. The handling, destruction, maintenance, storage, backup, and distribution and transmission of confidential information are documented in the data classification and retention policy, XYZ's general business terms, and in some cases, in customer and business partner-specific contracts and service-level agreements.
Confidential policies and processes have been implemented to limit access to logical input routines and physical input media to authorized individuals. Each type of confidential information is classified, handled, secured, retained, and disposed of. All nonpublic customer information is confidential. Data that carries a confidential classification is subject to the Company's information security policy, which defines protection requirements, access rights, and access restrictions, as well as retention and destruction requirements. Customer, vendor, and business partner information is presumed to be confidential (as a default) unless obviously not.
As part of their standard process for establishing service levels and operational protocols with vendors or business partners such as ABC Cloud and UVW Trading, XYZ will evaluate data shared between the two organizations and agree on what is confidential. XYZ also requests that business partners disclose their security, data classification, and retention policies to ensure that XYZ's data is afforded the proper retention and information protection. The CISO, with the information security team, is responsible for maintaining and updating confidentiality, system security, and related policies.
At the time of hire or affiliation, the code of conduct and confidentiality agreements that employees are required to sign prohibit any disclosures, beyond the extent authorized, of information and other data to which the employee has been granted access. Individual manufacturing contracts also define how confidential information is authorized and rescinded. Signed nondisclosure agreements are required from third parties before information designated as confidential can be shared with them. XYZ's business partners are also subject to nondisclosure agreements or other contractual confidentiality provisions, as outlined in the Business Associate Agreement. Customer contracts, service-level agreements, and vendor contracts are negotiated before performance or receipt of service and formally signed off on by management.
Logical Access. Customers, groups of individuals, or other entities are restricted from accessing confidential information, other than their own. Users, contractors, or vendors who have the ability to access confidential information are properly authorized or supervised, in line with the Company's employees. The information supervisor for a business unit determines whether users require access to confidential information to perform their specific job functions.

Data Retention. Retention periods, and policies for ensuring retention during the specified period and proper disposal of data at the end of the retention period, are also outlined in the data classification and retention policy. The retention period assigned to data is based on the (1) classification of the data, (2) regulatory requirements and legal statutes, and (3) the general requirements of the business.
During the designated retention period, XYZ ensures that backup media (whether offline or online) are stored in a protected environment for the duration of the designated document retention period. Computer backup media is included. When the retention period has ended, XYZ Manufacturing destroys the information securely. Electronic information and other information is disposed of securely by proven means.

Association
of International
Certified Professional
Accountants®