AICPA & CIMA

Together as the Association of International Certified Professional Accountants

Illustrative SOC 2® Type 2 Report

(Including Management's Assertion, Service Auditor's Report, and the Description of the System)

Note to reader:

This publication is nonauthoritative and is provided for informational purposes only.

DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022), *is not specific about format. Service organizations may organize and present the required information in a variety of formats. The format of the illustrative disclosures presented in this document is not meant to be prescriptive but, rather, illustrative. As noted in AICPA Guide* SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy, *flowcharts, matrixes, tables, graphics, context diagrams, or a combination thereof, may be used to supplement the narratives contained within the description. For brevity, the illustrative disclosures in this document do not include all disclosures that might be described in a type 2 report. Notes to readers throughout the document indicate places where detail has been omitted. These notes are to readers of the illustrative disclosures and should not be included in a SOC 2 description.*

The trust services categories being reported on, the controls specified by the service organization, and the tests performed by the service auditor and related results presented in this document are for illustrative purposes only. They are not intended to represent the categories that would be addressed in every type 2 engagement or the controls or tests of controls that would be appropriate for all service organizations. The trust services categories being reported on, the controls a service organization would include in its description, and the tests of controls a service auditor would perform for a specific type 2 examination will vary based on the specific facts and circumstances of the engagement.

In the following illustrative type 2 report, ABC Service Organization has engaged the service auditor to examine and report on the description of the service organization's processing system and its controls relevant to security, availability, and confidentiality to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. The example assumes that ABC Service Organization management has included information in section 5, "Other Information Provided by ABC Service Organization That Is Not Covered by the Service Auditor's Report," which is not a part of the description or the service auditor's examination.

Report on ABC Service Organization's Description of the ABC Processing System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality Throughout the Period January 1, 20XX, to December 31, 20XX

Contents

Section 1 — Assertion of ABC Service Organization Management

Section 2 — Independent Service Auditor's Report

Section 3 — ABC Service Organization's Description of the ABC Processing System

- Types of Services Provided
- Principal Service Commitments and System Requirements
- Components of the System Used to Provide the Services
  - Infrastructure
  - Software
  - People
  - Procedures
    - Control Environment
      - Management Philosophy
      - Information Security Management
      - Security Policies
      - Hiring and Training
      - Oversight Roles and Responsibilities
      - Issue Escalation
      - Policy Violations
    - Information and Communication
      - Data Classification and Retention
      - Data Destruction
    - Risk Management
      - Annual Risk Assessment

Significant Risks Related to the ABC Processing System
Risk Response
Monitoring Activities
Logical and Physical Access
Establishment and Modification of System Access
Security Levels
Authorization of Access
Monitoring System Access
Authentication
Password Management
Employee Access and Termination
Workstation Security
Production System Security
Transmission Security
System Operations
Malware Prevention
Intrusion Detection
Vulnerability Management
Incident Response
System Incident Identification and Evaluation
Incident Containment
Eradication
Recovery
Periodic Evaluation of Response Process
Change Management
Patch Management
Risk Mitigation
Availability and Resilience
System Capacity Monitoring
Testing of Contingency Plan
Disruption Response
Vendor Management

Data
System Incidents
Applicable Trust Services Criteria and Related Controls
Complementary User Entity Controls (CUECs)
Subservice Organizations
Specific Criteria Not Relevant to the System
Significant Changes to the System

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

Section 5 — Other Information Provided by ABC Service Organization That Is Not Covered by the Service Auditor's Report

Section 1 — Assertion of ABC Service Organization Management

Illustrative Assertion by Service Organization Management

[ABC Service Organization's Letterhead]

Assertion of ABC Service Organization Management

We have prepared the accompanying description in section 3 titled "ABC Service Organization's Description of the ABC Processing System" throughout the period January 1, 20XX, to December 31, 20XX, (description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report,* in AICPA *Description Criteria* (description criteria). [fn 1] The description is intended to provide report users with information about the ABC Processing System that may be useful when assessing the risks arising from interactions with ABC Service Organization's (ABC's) system, particularly information about system controls that ABC has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria.* [fn 2]

ABC uses a subservice organization to host the ABC Processing System. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ABC, to achieve ABC's service commitments and system requirements based on the applicable trust services criteria. The description presents ABC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ABC's controls. The description does not disclose the actual controls at the subservice organization.

[fn 1] The 2018 description criteria are codified as DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance — 2022)*, in AICPA *Description Criteria.* As implementation guidance may be updated without changes to criteria, service organization management and the service auditor should review the most current version of DC section 200 for the most up-to-date guidance.

[fn 2] The 2017 trust services criteria are codified in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus — 2022)*, in AICPA *Trust Services Criteria.* As points of focus may be updated without changes to criteria, service organization management and the service auditor should review the most current version of TSP section 100 for the most up-to-date guidance.

We confirm, to the best of our knowledge and belief, that

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

b. the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that ABC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of ABC's controls throughout the period.

c. the controls stated in the description operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that ABC's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of ABC's controls operated effectively throughout that period.

Section 2 — Independent Service Auditor's Report

Independent Service Auditor's Report on a SOC 2 Examination [fn 3]

To: Management of ABC Service Organization

Scope

We have examined ABC Service Organization's (ABC's) accompanying description in section 3 titled "ABC Service Organization's Description of the ABC Processing System" throughout the period January 1, 20XX, to December 31, 20XX (description), [fn 4] based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report,* in AICPA *Description Criteria* (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that ABC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy,* in AICPA *Trust Services Criteria*.

The information included in section 5, "Other Information Provided by ABC Service Organization That Is Not Covered by the Service Auditor's Report," is presented by ABC management to provide additional information and is not a part of the description. Information about ABC's [*describe the nature of the information, for example, planned system changes*] has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve ABC's service commitments and system requirements based on the applicable trust services criteria, and accordingly we express no opinion on it.

fn 3 The report may also be titled "Report of Independent Service Auditors."

fn 4 The title of the description of the service organization's system in the service auditor's report should be the same as the title used by service organization management in its description of the service organization's system.

ABC uses a subservice organization to host the ABC Processing System. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at ABC, to achieve ABC's service commitments and system requirements based on the applicable trust services criteria. The description presents ABC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of ABC's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

ABC is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that ABC's service commitments and system requirements were achieved. In section 1, ABC has provided its assertion titled "Assertion of ABC Service Organization Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. ABC is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

An examination of the description of a service organization's system and the suitability of the design

and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

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

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in section 4, "Trust Services Category, Criteria, Related Controls, and Tests of Controls," of this report in columns 2, 4, and 5, respectively.

Opinion

In our opinion, in all material respects,

a. the description presents the ABC Processing System that was designed and implemented throughout the period January 1, 20XX, to December 31, 20XX, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that ABC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of ABC's controls throughout the period.

c. the controls stated in the description operated effectively throughout the period January 1, 20XX, to December 31, 20XX, to provide reasonable assurance that ABC's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of ABC's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of ABC; user entities of the ABC Processing System during some or all of the period January 1, 20XX, to December 31, 20XX; business partners of ABC subject to risks arising from interactions with the ABC Processing System; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations

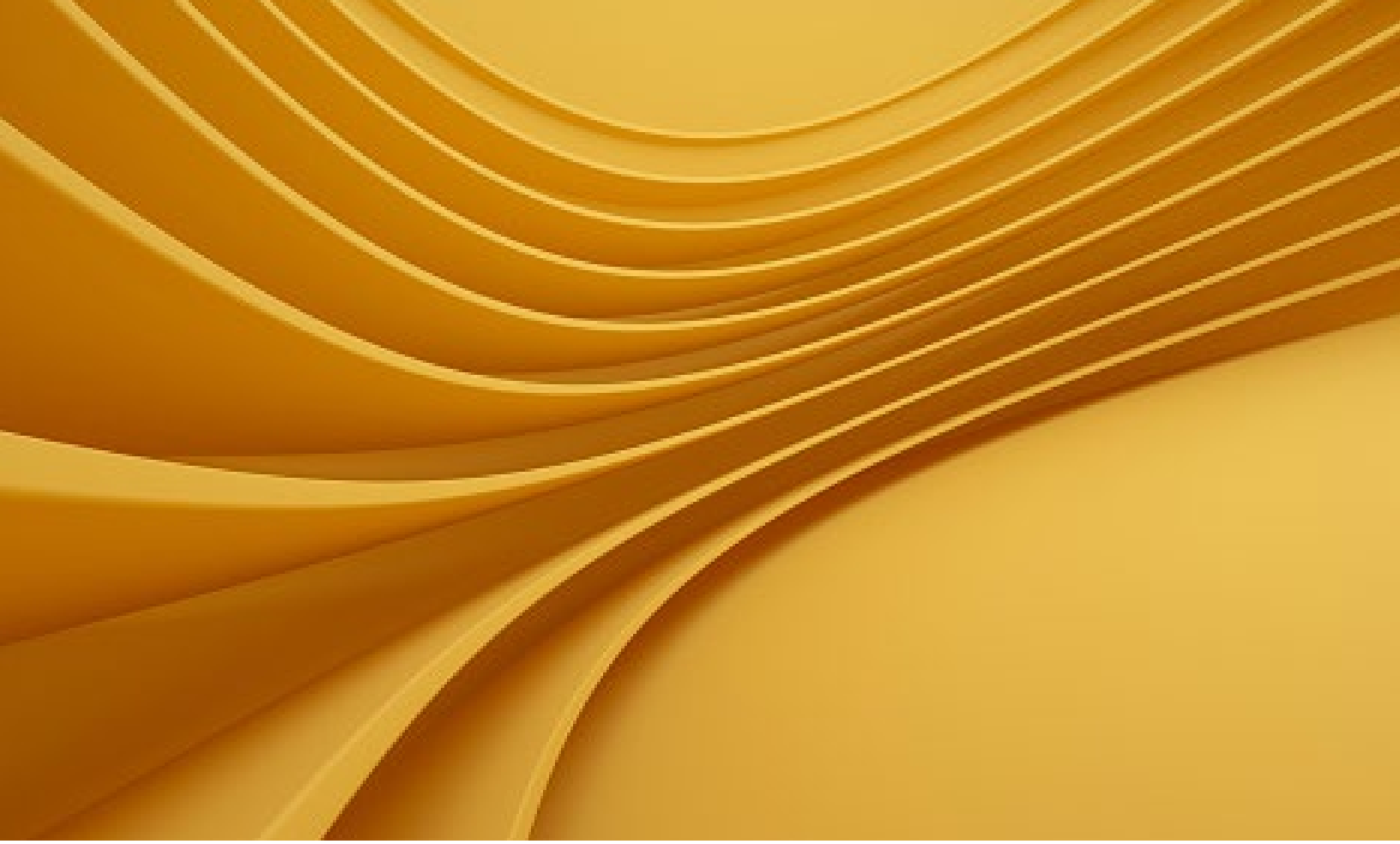
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

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

[Service auditor's signature]

[City and state where the report is issued]

[Date of the service auditor's report]



Section 3 — ABC Service Organization's Description of the ABC Processing System

Note to Readers: *The following system description is for illustrative purposes only and is not meant to be prescriptive. For brevity, the illustration does not include everything that might be described in the description of the service organization's system. Notes to readers indicate places where detail has been omitted from the illustration.*

TYPES OF SERVICES PROVIDED

ABC Service Organization, Inc. ("ABC," "the Company"), provides a worldwide cloud-based software application. The Company was founded in 2019 to connect businesses to their respective customers through automated means. The Company processes billions of customer requests per year via an application programming interface (API). The ABC Processing System provides ABC customers (customers) and their clients with an end-to-end solution that serves stakeholders through invoicing, secure payment processing, consumer engagement, recurring payments, automated payment plans, payment tracking, reconciliation, and mitigation of past-due payments (the services).

This description details the ABC Processing System and the related policies, procedures, and control activities for the ABC Processing System. This description does not include any other ABC services and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of subservice organizations).

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

ABC designs its processes and procedures related to the ABC Processing System to meet its objectives for its business connection solutions services. Those objectives are based on the service commitments

that ABC makes to its customers, business partners, vendors, and subservice organizations and the operational and compliance requirements that ABC has established for the services. Service commitments are declarations made by management to its customers regarding the performance of the ABC Processing System. Service commitments are set forth in standardized contracts, service level agreements, and in the description of the service offering provided online and include the following:[fn 5]

- Commitments regarding the security and availability of the system and confidentiality of information processed by the system in accordance with contractual stipulations
- Commitments regarding the invoicing, secure payment processing, consumer engagement, recurring payments, automated payment plans, payment tracking, reconciliation, and mitigation of past due payments as described in the master service agreement, *Service Level Agreement,* and the *System Reference Document*
- Commitments to support customer compliance with the security-related requirements of the EU General Data Protection Regulation as set forth in the master services agreement

Note to Readers: *For brevity, this illustration does not include a full list of principal service commitments.*

ABC establishes operational requirements that support the achievement of security commitments, relevant operational and compliance requirements, applicable laws and regulations, and other system requirements including the following:

- System functional and nonfunctional requirements derived from service commitments, published documentation of system functionality, and other descriptions of the system
- Monitoring of third-party providers to detect failures of those service providers to meet service agreements that could threaten the achievement of the service organization's service commitments and system requirements and respond to those failures

Such requirements are communicated in ABC's system policies and procedures, system design documentation, and contracts with customers.

[fn 5] Service commitments are commonly reflected in existing documents, such as service level agreements, available to customers and business partners. In most situations, rather than including a reference to the principal service commitments in these existing documents, management would list the individual commitments in the description.

ABC has adopted the NIST Cybersecurity Framework as the basis for its organization-wide information security policies. In addition to these policies, standard operating procedures have been developed and documented on how to carry out specific manual and automated processes required in the operation and development of the ABC Processing System. System requirements based on the NIST Cybersecurity Framework include the following:

- Data, personnel, devices, systems, and facilities are identified and managed.
- ABC management identifies, assesses, and manages the cybersecurity risk to organizational operations.
- ABC's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions.
- Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
- Information and records (data) are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.
- Security policies, processes, and procedures are maintained and used to manage protection of information systems and assets.
- Maintenance and repairs of information system components are performed consistent with policies and procedures.
- Technical security solutions are managed to help ensure the security and resilience of systems and assets.
- Anomalous activity is detected and the potential impact of events is understood.
- The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
- Detection processes and procedures are maintained and tested to help ensure awareness of anomalous events.
- Response processes and procedures are executed and maintained to help ensure response to detected cybersecurity incidents.
- Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident.

- Recovery processes and procedures are executed and maintained to help ensure restoration of systems or assets affected by cybersecurity incidents.

Note to Readers: *For brevity, this illustration does not include a full list of principal system requirements.*

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The system described herein is bounded by the specific aspects of ABC's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers and the data that is processed by the system. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the system. The components that directly support the services provided to user entities are as follows:

Note to Readers: *A diagram or other graphic may also be provided.*

INFRASTRUCTURE

ABC utilizes XYZ Cloud Hosting (XYZ) as a subservice organization to host the ABC Processing System. ABC leverages the experience and resources of XYZ to enable ABC to achieve its service commitments and system requirements. XYZ is responsible for designing and configuring the ABC Processing System architecture within XYZ to help ensure service commitments and system requirements are met.

The system's infrastructure uses XYZ IaaS, located in the eastern United States, to provide security and protection services as well as hosting services and utilizes the western United States region for backup in support of availability commitments.

SOFTWARE

The software component consists of the applications, programs, and other software that support the system. The list of software and ancillary software used to build, support, secure, maintain, and monitor the ABC Processing System are the following:

Production Application	Business Function
XYZ app software	Application monitoring for load and uptime performance.
XYZ logging system	SIEM/Logging system that provides log management and analytics that leverage machine-generated data to deliver real-time IT insights.
XYZ watch application	Infrastructure monitoring and analytics tool for IT and DevOps teams that can be used to determine performance metrics as well as event monitoring for infrastructure and cloud services.
XYZ patching tool	Patch management tool that can plan, manage, and deploy updates, patches, and hotfixes for Windows servers, client operating systems, and other Microsoft software.
XYZ file integrity platform	File integrity monitoring platform used to deliver security, monitoring, forensics, and collection of metrics about the environment.
XYZ anti-virus program	Anti-virus program that scans computers for security threats, prevents unapproved programs from running, and applies firewall policies that block or allow network traffic.
XYZ help application	Software application used for issue tracking and project management.
XYZ data loss prevention software	Data loss prevention software used to ensure that sensitive data is not lost, misused, or accessed by unauthorized users.
XYZ version control tool	Version control and DevOps tool used for source code management used to track changes in the source code.
XYZ IDS application	Intrusion detection system used to provide visibility into endpoint vulnerabilities by gathering data needed to identify, understand, and respond to attacks.

PEOPLE

ABC has various personnel groups that directly support the ABC Processing System. The responsibilities of these groups are defined in the following table:

Group/Role Name	Business Function
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives
Engineering	Responsible for the development, testing, deployment, and maintenance of new code for the ABC Processing System
InfoSec	Responsible for the overall security of the production environment, including evaluation and management of controls and other activities that relate to the ability of the system to meet its service commitments and system requirements. Also responsible for evaluating and managing controls and other activities that prevent, detect, mitigate, and remediate system incidents
Software Product Management	Responsible for the software product life cycle, including adding additional product functionality
Customer Service	Responsible for resolving issues raised by users of the ABC Processing System
Human Resources	Responsible for onboarding new personnel, defining role/position of new hires, performing background checks, and facilitating the employee termination process

Group/Role Name	Business Function
Operations	Staff that provide the day-to-day services such as invoicing, payment processing, consumer engagement, payment tracking, reconciliation, and mitigation of past due payments
IT Infrastructure	Responsible for monitoring the infrastructure services provided by the subservice organization

PROCEDURES

ABC has developed and communicated policies and procedures involved in the operation of the ABC Processing System. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to risk management, data backup, system and facility access, auditing, configuration management, breach/incidents, disaster recovery, intrusion detection, vulnerability assessment, data integrity, vendor management, and so on. These procedures are developed in alignment with the overall information security policy and are reviewed, updated, and approved as necessary for changes in the business, but no less than once annually.

The following provides a summary of ABC's policies and procedures that comprise the internal control for the system.

Control Environment

Management Philosophy

ABC's control environment reflects the philosophy of senior management concerning the importance of the availability of ABC system and the security and confidentiality of data and information within that system. ABC's Security Steering Committee meets quarterly and reports to the board annually. The committee, under the direction of the ABC board, oversees the security activities of ABC. The committee is charged with establishing overall security policies and procedures for ABC, including those related to the protection of confidential information. The importance of security is emphasized within ABC through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, ABC has taken

into consideration the relevance of controls to achieve the organization's service commitments and system requirements based on the applicable trust services criteria.

Information Security Management

ABC has a dedicated information security team consisting of a Security Officer and a Senior Security Specialist responsible for management of information security throughout the organization. They hold positions on the Security Steering Committee and maintain security credentials and are required to annually sign and acknowledge their review of the information security policies. They are responsible for developing, maintaining, and enforcing ABC's information security policies. The information security policy is reviewed annually by the Security Officer, CIO, and Vice President of Operations, and is approved by the Security Steering Committee.

Security Policies

Security policies and related processes are in place for the ABC processing system in areas such as the following:

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

Hiring and Training

Open positions are supported by job descriptions that include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system. Background verification checks are performed and experience verified on candidates as part of the interview process.

To help ensure that employees and contractors (workforce members) are aware of the importance of the availability of the ABC system and the security and confidentiality of data and information within that system, workforce members are granted access to organizational policies, which include the sanction policy for security violations. Sanction policies are defined to hold employees accountable and establish disciplinary actions for noncompliance. The ABC information security policy contains the Company's code of conduct, which states workforce responsibilities and

acceptable behavior regarding information system usage. The Company requires employees to read and accept the ABC information security policy upon hire and on an annual basis thereafter. Upon hire, workforce members must sign a confidentiality agreement that prohibits any disclosure of information and other data to which the employee or contractor has been granted access.

New workforce members are given training on security policies and procedures, including operations security. Security training includes training on the importance of information security topics, including the use and disclosure of confidential information and other data. ABC's monitoring of the access and activity of the information applications, systems, and networks is communicated through new employee orientation, ongoing training opportunities and events, and applicable policies. ABC workforce members are made aware of responsibilities about confidentiality and security of information as well as applicable sanctions/corrective disciplinary actions should the auditing process detect a workforce member's failure to comply with organizational policies.

Upon completion of training, workforce members receive proof of completion and records are kept of training. Workforce members are provided with annual training on security policy and procedure updates and latest security trends and threats.

Oversight Roles and Responsibilities

The Company has established defined roles and responsibilities to oversee the implementation of the information security policy and control environment. ABC has an independent board of directors that follows documented responsibilities and related qualifications for oversight of ABC and its system of internal control. The board of directors meets at least annually and is consulted and involved in all significant business decisions. Management and the board establish or update ABC's overall business objectives, including objectives for the system of internal control.

Senior management reports to the board of directors in conjunction with board meetings. Senior management is responsible for running the business of ABC as well as establishing overall policies and procedures for ABC, which includes an emphasis on the importance of security.

The Security Officer is responsible for facilitating the development, testing, implementation, training, and oversight of activities pertaining to ABC's efforts to meet its security and other objectives. Security Officer responsibilities are to maintain the confidentiality, security, and availability of confidential information. The Security Officer is responsible for the system of internal control and executing strategy and other decisions agreed upon by senior management and the board of directors. Although the Security Officer is responsible for implementing and overseeing activities related to maintaining compliance, it is the responsibility of all workforce members to supervise any user of ABC's systems, applications, servers, workstations, and so on that contain confidential information.

Issue Escalation

ABC workforce members are to escalate issues using the procedures outlined in the information security policy. Security incidents, particularly those involving confidential information, are handled

using the process described in the information security policy. If the incident involves a breach of confidential information, the incident response procedures are followed.

Policy Violations

Workforce members are direct to report noncompliance with ABC's policies and procedures to the Security Officer or other individual as assigned by the Security Officer. Individuals who report violations in good faith may not be subjected to intimidation, threats, coercion, discrimination against, or any other retaliatory action.

An investigation is performed on reported violations of ABC's policies and procedures. Violations of any security policy or the procedure by workforce members may result in corrective disciplinary action, up to and including termination of employment.

Information and Communication

As noted above, ABC has an information security policy to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to help ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

As the security team maintains security, it monitors known incidents and patches as well as results from recent vulnerability assessments and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans, and a verification of responsibilities for authorizing and monitoring accesses. Changes are reviewed and communicated during weekly IT maintenance meetings or through system alerts.

During annual security training and awareness programs, management ensures communication of the latest security and confidentiality policies as well as written job descriptions for security personnel.

Additionally, management is responsible for ensuring agreements with third parties are current and for updating the annual IT risk assessment. Applicable security and confidentiality commitments regarding services provided are identified in written contracts between the Company and its vendors, customers, and business associates. The Company provides a status page that notifies customers of critical changes that may affect their processing. The Company provides external users with a process for reporting system failures, incidents, concerns, and other complaints.

Data Classification and Retention

ABC has an established framework for classifying data based on its level of sensitivity, value, and criticality to ABC, which aids in determining appropriate security and confidentiality controls for the protection of data. ABC defines data as confidential, sensitive, and nonpublic information. Data classification reflects the level of impact to ABC if confidentiality, integrity, or availability is compromised. ABC data is classified into one of three sensitivity levels:

- *Restricted Data* — the unauthorized disclosure, alteration, or destruction of that data could cause a significant level of risk to ABC, its customers, or its affiliates
- *Private Data* — the unauthorized disclosure, alteration, or destruction of that data could result in a moderate level of risk to ABC, its customers, or its affiliates
- *Public Data* — the unauthorized disclosure, alteration, or destruction of that data would result in little or no risk to ABC, its customers, and its affiliates

Classification of data is performed by appropriate personnel, based on job description, or the Security Officer.

ABC's information security policy prohibits confidential or sensitive customer data from being used or stored in nonproduction systems or environments. Policy also requires that this data only be used and retained for the time required and for identified purposes unless a law or regulation specifically requires otherwise.

Data Destruction

Destruction or disposal of confidential information is performed in accordance with federal and state laws and regulations and pursuant to ABC's written retention policy/schedule. Records that have satisfied the period of retention are destroyed/disposed of according to policy.

ABC subcontractor agreements provide that, upon termination of the contract, the subcontractor will return or destroy/dispose of all confidential information. In cases where the return or destruction/disposal is not feasible, the contract limits the use and disclosure of the information to the purposes that prevent its return or destruction/disposal.

The methods of destruction, disposal, and reuse are reassessed periodically, based on current technology, accepted practices, and availability of timely and cost-effective destruction, disposal, and reuse technologies and services.

In the case of an ABC customer terminating a contract with ABC and no longer utilizing ABC services, ABC will remove or purge data upon request from the system per contractual obligations with the customer.

Removable media is restricted, monitored, and encrypted. ABC assumes disposable media in ABC Processing System may contain confidential information, so it treats all disposable media with the same protections and disposal policies. Before reusing any media, confidential information is rendered inaccessible, cleaned, or scrubbed. Media is formatted to restrict future access. Any media

containing confidential information is disposed of using a method that ensures the confidential information could not be readily recovered or reconstructed.

Risk Management

In support of the overall risk management program, ABC manages its risk portfolio based on a threat and vulnerability management program, which integrates risk assessment, control design and implementation, incident management, and monitoring of controls to mitigate risks to an appropriate level.

ABC's risk management program includes the following considerations related to threat and vulnerability management over the system:

- System characterization
- Identification of objectives
- Threat identification
- Vulnerability identification
- Likelihood determination
- Magnitude analysis
- Risk determination
- Risk treatment plan development
- Control design and implementation
- Incident management
- Monitoring

ABC workforce members are expected to participate in the risk management program based on their assigned responsibilities. Any workforce member who violates this policy is subject to disciplinary action. The risk management process is the responsibility of the Chief Risk Officer. Each functional unit within ABC assigns the responsibility for supporting risk management within the function. For the Information Service function, the implementation, execution, and maintenance of the information security risk analysis assessment and risk management process is the responsibility of ABC's Security Officer.

A documented risk management program is in place that includes guidance on the identification of potential threats (including fraud risks), rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks. The risk management program is updated on an annual basis or as needed should changes occur.

Annual Risk Assessment

The foundation of the ABC risk management program is an annual baseline risk assessment to identify threats to the achievement of ABC's corporate and client service objectives, including service commitments and system requirements for the system. ABC uses a combination of business resources, personnel understanding of the services provided, discussions with user entity and business partner personnel, and information provided by third-party threat monitoring and law and regulation monitoring services to identify threats. Threats from internal and external origins and those related to error, fraud, and environmental factors are also considered.

ABC uses its inventory of system components, including physical hardware, service providers, data access points, virtual devices, licensed and installed software, data files, and information flows, combined with published external and internal vulnerability catalogs and vulnerability reporting services to identify system vulnerabilities. The likelihood of a threat intersecting with a vulnerability, and the magnitude of an impairment to objectives as a result of such an intersection, is assessed for events deemed more than inconsequential. More than inconsequential risks are evaluated against ABC's risk appetite criteria and risk treatment plans to mitigate the risks to an acceptable level are developed and documented for each risk. The output of this process helps identify appropriate controls for reducing or eliminating risk.

Assessed risks are documented in a master risk register. On a quarterly basis, the Chief Risk Officer reviews the status of the annual risk assessment with the functional unit risk representatives to determine if an update is required. In addition, an update may be triggered based upon a request from functional unit leadership in response to a newly identified threat, changes to information systems architecture, changes in service offerings, newly identified vulnerabilities as a result of the design and implementation of controls, control deficiencies identified by monitoring activities, system incidents, or other sources. Updates are focused on the particular threat and vulnerability changes identified.

Significant Risks Related to the ABC Processing System

Risks that generally apply to all organizations, such as threats of a breach, public health crisis, and so on, are not included in this description. Instead, significant risks that are deemed unique to ABC are noted below:

- ABC utilizes cloud providers throughout the world to host its SaaS solution, in conformance with local laws and regulations. Given the ever-changing regulatory landscape across the globe and the interconnected nature of the cloud solution that ABC provides, any of its subservice organizations being found to be in noncompliance with local laws and regulations could, depending on the facts and circumstances, also affect ABC's ability to offer its services in those geographies where the subservice organization is found to be noncompliant. ABC connects with its key subservice organizations on a periodic basis in an effort to monitor any regulatory noncompliance matters that may also affect ABC.
- ABC's SaaS service is highly automated and integrated, utilizing various open-source technologies and subservice organizations. The vulnerability within any of the open-source

technologies or the solutions provided by the subservice organizations could result in a significant disruption to the SaaS service. ABC has vulnerability and vendor management programs to help monitor for vulnerabilities in solutions it utilizes, whether open-source or those provided by the subservice organizations.

- ABC regularly receives, from its customers, information that is proprietary and sensitive, including customer trade secrets, and other proprietary elements as identified by customers.

Risk Response

Risk response involves prioritizing, evaluating, and implementing the appropriate risk-reducing controls to address risks identified in the risk assessment process to help ensure the confidentiality (as applicable), integrity, and availability of information. Determination of appropriate controls to reduce risk is dependent upon the risk tolerance of the organization consistent with its goals and mission.

Monitoring Activities

Monitoring is a critical aspect of internal control in evaluating whether processes and controls at different levels of the organization are operating as intended and whether they are modified as appropriate for changes in conditions. ABC staff are responsible for the ongoing operation of effective controls and management personnel are responsible for monitoring the quality of internal control performance as a routine part of their activities. Ongoing monitoring activities are also built into the normal recurring activities of ABC and are included in the respective sections of this description. Management's monitoring includes a combination of the following:

- Implementation of controls designed to detect failures in the operation of other controls such as reconciliations, incident monitoring, and periodic review of key controls.
- Review of control metrics established during the design of the controls over processes and updated as necessary. When practicable, controls metrics are generated by automated reporting.
- Periodic (such as weekly or monthly) staff meetings within line and functional departments during which both operational and control metrics are reviewed and the need for corrective actions is identified.
- Quarterly control self-assessments performed by staff of the line and functional departments under the supervision and review of departmental management.

Management monitoring activities are overseen by the Internal Control group, which reports to the Chief Risk Officer. On a quarterly basis, the results of management monitoring activities are summarized and presented by the Chief Risk Officer to the Management Committee.

Evaluations are also periodically performed by the ABC internal audit function to help ensure controls continue to operate effectively. ABC's internal audit function is responsible for providing the ABC board, the Audit Committee, and management with feedback and recommendations after evaluating the effectiveness of risk management activities and internal control within the organization. Internal audit evaluates the adequacy and design of controls to mitigate risks, tests controls for operational effectiveness, and evaluates whether management has sufficient risk management and governance processes in place. The internal audit function relies on a process-based risk assessment to help determine the areas of focus for the annual internal audit plan.

In addition, security information and event management systems (SIEM) reports, and results of periodic system scanning and penetration testing, are reviewed by information technology management during monthly and quarterly staff meetings.

ABC's process for monitoring vendors is described in the section titled Subservice Organizations.

Note to Readers: *For brevity, this illustration does not include a full list of monitoring activities.*

Logical and Physical Access

Access to ABC systems and applications is limited to authorized users including, but not limited to, workforce members, volunteers, business associates, contracted providers, and consultants. Access by any other entity is allowable only on a minimum necessary basis. Users are responsible for reporting incidents of unauthorized use or access of the organization's information systems.

The Company enables a web application firewall to help protect web applications or APIs against common web exploits that may compromise security or consume excessive resources by creating security rules that block common attack patterns (such as SQL injection or cross-site scripting) and rules that filter out defined traffic patterns.

Establishment and Modification of System Access

Access to system components requires a documented access request form and manager approval prior to access being provisioned. The Security Officer will grant access to systems as dictated by the employee's job title and description. If additional access is required outside of the minimum necessary to perform job functions, the requester must include a description of why the additional access is required as part of the access request. Once the review is completed, the Security Officer approves or rejects the application. If the application is rejected, it goes back for further review and documentation. If the review is approved, the Security Officer then marks the application as done, adding any pertinent notes required.

New accounts are created with a temporary secure password which must be changed on the initial login and must meet minimum requirements. Password exchanges must occur over an authenticated channel. Access is not granted until receipt, review, and approval of the access application by the ABC Security Officer. Access to ABC systems and services are reviewed and

updated on a quarterly basis to help ensure proper authorizations are in place commensurate with job functions. Management performs quarterly access reviews for system components to help ensure that access is restricted appropriately.

Access to production systems is controlled using centralized user management and authentication. Temporary accounts are not used unless necessary for business purposes. Accounts that are inactive for over 90 days are removed.

Security Levels

The level of security assigned to a workforce member for the organization's information systems is based on the minimum necessary amount of data access required to carry out legitimate job responsibilities assigned to a user's job classification. Access requests are treated on a "least-access principle." Privileged access to system components is restricted to authorized users with a business need.

Authorization of Access

Role-based access categories for each ABC system and application are pre-approved by the Security Officer or an authorized delegate of the Security Officer. ABC utilizes software firewalls to segment data, prevent unauthorized access, and monitor traffic for denial-of-service attacks. Security groups are used and configured to prevent unauthorized access to the production environment. Security group rulesets are reviewed by management annually.

Monitoring System Access

Responsibility for monitoring access to and activity in information systems is assigned to ABC's Security Officer. ABC's monitoring activities address access and activity at the user, application, system, and network levels. Such processes address, but are not limited to, the date and time of log-on and log-off attempts, devices used, data accessed, data modified, functions performed, system denials, operational activity, penetrations, vulnerabilities, and so on.

System activity is documented in log files. These log files are protected from unauthorized access or modification to make sure that the information needed to evaluate a security incident or routine activities is complete and accurate. Logs are stored on a separate system to minimize the impact that monitoring activities may have on the system and to prevent access by those with system administrator privileges. Logs are protected in transit and encrypted at rest to control access to the content of the logs.

Log files are maintained based on organizational needs. Retention of this information is based on organizational history and experience as well as available storage space. Log data and reports summarizing monitoring activities are retained for a period of four years.

Authentication

Each workforce member, customer, business partner, or customer client has and uses a unique user ID and password that identifies them as the user of the information system. Authentication to system components require unique usernames and passwords or authorized Secure Shell (SSH) keys. Authorized workforce members are permitted access to the production system using a valid multi-factor authentication (MFA) token.

The Company has enabled a password policy that enforces the creation of strong user passwords for users accessing resources. Default accounts on production systems, including root, are disabled by default. Shared accounts are not allowed within ABC systems or networks.

Customer support desk interactions must be verified before ABC support personnel will satisfy any request having information security implications.

Password Management

ABC information security policy states that user IDs and passwords are used to control access to ABC systems and may not be disclosed to anyone for any reason. Users may not allow anyone, for any reason, to have access to any information system using another user's unique user ID and password. Passwords cannot be displayed at any time and are not transmitted or stored in plain text.

Employee Access Termination

The Human Resources Department (or other designated department), users, and their supervisors notify the Security Officer upon notification of voluntary or involuntary termination. The Human Resources Department, users, and supervisors are required to notify the Security Officer to terminate a user's access rights if there is evidence or reason to believe the user has been using their access rights inappropriately, a user's password has been compromised, or an unauthorized individual is utilizing a user's login ID and password. A new password may be provided to the user if the user is not identified as the one violating the Company access policies.

As part of the termination process, the Company terminates users' access rights within 48 hours of notification. Passwords are inactivated immediately upon an employee's termination. Company management coordinates with the appropriate ABC employees to recover any physical devices (such as badges, laptops, or mobile devices) that the terminated employee may have. The Security Officer reviews and may terminate the access of users who have not logged into the organization's information systems/applications for an extended period of time.

Workstation Security

Workstations may only be accessed and utilized by authorized workforce members to complete assigned job/contract responsibilities. Workforce members are required to monitor workstations

and report unauthorized users and/or unauthorized attempts to access systems/applications. Data loss prevention software is designed to prevent or detect, restrict, and report the transfer of confidential information to workstations used to connect to production systems.

Production System Security

System, network, and server security is managed and maintained by the Security Officer. The network is segmented to prevent unauthorized access to customer data. Architecture and data flow diagrams are kept for production environments to support the design and operation of controls. A formal inventory of production system assets is maintained by management.

Production systems disable services that are not required to achieve the business purpose or function of the system. Access to production systems is logged following ABC's monitoring procedures. Data stores housing sensitive customer data are encrypted at rest.

The Company utilizes a file integrity monitoring (FIM) tool for monitoring of the production environment. The tool includes monitoring activities that do the following:

- Collect monitoring and operational data in the form of logs, metrics, and events, to monitor applications, respond to system-wide performance changes, and optimize resource utilization
- Identify trends that may have a potential impact on the Company's ability to achieve its security objectives
- Provide increased visibility into user activity in the production account that may have a potential impact on the Company's ability to achieve its security commitments

Transmission Security

Secure data transmission protocols are used to encrypt confidential and sensitive data over public networks. Data transmission is encrypted end to end using encryption keys managed by ABC. Encryption is not terminated at the network endpoint and is carried through to the application. The system logs transmissions of production data access.

System Operations

Management subscribes to industry security bulletins and email alerts and uses them to monitor the impact of emerging technologies on security.

An infrastructure monitoring tool is utilized to monitor infrastructure availability and performance and generates alerts when specific predefined thresholds are met.

Network and system hardening standards are documented, based on industry best practices, and reviewed by management at least annually.

Malware Prevention

Production systems commonly susceptible to attack have an anti-malware tool installed and running to help ensure no malware is present. Detected malware is evaluated and removed. Virus scanning software is run on sensitive or at-risk production systems for antivirus protection. The tool is configured for routine updates.

Production systems are only to be used for ABC business needs. Public-facing servers or hosts are protected from unauthorized or malicious software through a defense in depth strategy that includes a combination of secure architecture, segmentation and isolation, and hardened configurations.

Intrusion Detection

Production systems are monitored using intrusion detection systems to provide continuous monitoring of the Company's network and early detection of potential security breaches. Suspicious activity is logged, and alerts are generated. Automatic monitoring is done to identify patterns that might signify the lack of availability of certain services and systems. ABC firewalls monitor incoming traffic to detect potential denial-of-service attacks. Suspected attack sources are blocked automatically.

The security administration team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, intrusion detection system (IDS) or intrusion prevention system (IPS) alerts, vulnerability assessment reports, and operating system event logs. These alerts and notifications are reviewed daily by the security administration team using a SIEM product. Additionally, the security administration team has developed and will review the following SIEM reports:

- Failed object level access
- Daily IDS or IPS attacks
- Critical IDS or IPS alerts
- Devices not reporting in the past 24 hours
- Failed login detail
- Firewall configuration changes
- Windows policy changes
- Windows system shutdowns and restarts

Security events requiring further investigation are tracked using a help desk ticket and monitored until resolved.

Vulnerability Management

Vulnerability management is performed by the ABC Security Officer or an authorized delegate of the Security Officer. As part of vulnerability assessment and management, the Company performs quarterly internal and external vulnerability scans and annual penetration tests.

Reviewing vulnerability scan and penetration testing reports and findings, as well as any further investigation into discovered vulnerabilities, is the responsibility of the ABC Security Officer. A remediation plan is developed based on the results of the vulnerability scans and penetration tests, and changes are implemented by management to remediate critical and high vulnerabilities at a minimum.

Incident Response

ABC's security incident response policies and procedures are documented and communicated to authorized users. ABC's incident response classifies security-related events based on an assessment of the severity of the event. If the event is a security incident or involves a breach of confidential information, an incident response team is activated. Significant security incidents are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management.

System Incident Identification and Evaluation

ABC employees must report any unauthorized or suspicious activity as outlined in the information security policy. Issues that are brought to management are assigned an owner. If the incident involves a breach of confidential information, the Security Officer will manage the incident. Suspected and known events, precursors, indications, and incidents are to be reported immediately upon observation through various means of communication.

The Security Officer determines if the issue is an event, precursor, indication, or incident. If the issue is an event, indication, or precursor, the Security Officer forwards it to the appropriate resource for resolution. If the issue is a security incident, the Security Officer activates the security incident response team (incident response team). Significant security incidents are subject to the incident response plan and are evaluated, logged, tracked, and communicated to affected parties by management.

The Security Officer or other appointed ABC representative notifies any affected customers and partners. If no customers and partners are affected, notification is at the discretion of the Security Officer.

Incident Containment

The incident response team reviews any information that has been collected by the Security Officer or any other individual investigating the security incident and secures the network perimeter. Senior management is continuously informed of progress. Affected customers and partners are continuously informed of relevant updates as needed.

Eradication

The incident response team removes the cause, and the resulting security exposures on the affected system(s). Symptoms and causes related to the affected system(s) are determined. The defenses surrounding the affected system(s) are strengthened where possible (a risk assessment may be needed and can be determined by the Security Officer).

Recovery

The incident response team restores the affected system(s) back to operation after the resulting security exposures, if any, have been corrected. The technical team determines if the affected system(s) have been changed in any way. If they have, the technical team restores the system to its proper, intended functioning ("last known good"). Once restored, the team validates that the systems function the way they were intended to/had functioned in the past.

If the operation of the system(s) had been interrupted (that is, the system[s] had been taken offline or dropped from the network while triaged), the incident response team restarts the restored and validated system(s) and monitors for behavior.

Documentation with the detail that was determined is updated, senior management is updated of progress, and affected customers and partners are provided relevant updates as needed.

Periodic Evaluation of Response Process

The processes surrounding security incident response are periodically reviewed and evaluated for effectiveness. This involves appropriate training of resources expected to respond to security incidents, as well as the training of the general population regarding ABC's expectation for them relative to security responsibilities. The incident response plan is tested at least annually according to the information security policy.

Change Management

ABC has a formalized change management process in place, which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality.

ABC standardizes and automates configuration management using tools and scripts to help ensure system configurations are deployed consistently throughout the environment. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed. The IT management team meets weekly to review and schedule changes to the IT environment.

Changes to production systems and networks are documented and communicated to authorized internal users. The Company automatically configures ABC systems according to established and tested policies. The Company uses a configuration management system to assess, audit, and evaluate the configurations of the platform's hosting resources.

The Company utilizes a systems development life cycle (SDLC) methodology to govern the development, acquisition, and implementation of changes (including emergency changes) and maintenance of information system and related technology requirements.

Access to migrate changes to production is restricted to authorized personnel with legitimate business needs and must be approved by authorized personnel. Changes to software and infrastructure components of the service are authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.

System changes are communicated to authorized internal users.

Patch Management

Software patches and updates are applied to systems in a timely manner. Infrastructure supporting the services provided is patched as a part of the change management process to help ensure that servers supporting the service are hardened against security threats. Routine updates are applied after thorough testing. In the case of updates to correct known vulnerabilities, priority will be given to testing to speed the time to production. Critical security patches are applied within three days from identification and security patches are applied within seven days after identification.

Risk Mitigation

Availability and Resilience

ABC has developed and documented a business continuity and disaster recovery plan. The plan is updated and tested on at least an annual basis. The Company contingency plan establishes procedures to recover the ABC Processing System following a disruption resulting from a disaster. Versioning is enabled on data storage to support recovery from unintended events, actions, and application failures. Databases are replicated to a secondary data center in real time. Alerts are configured to notify ABC personnel if replication fails. ABC employs a multi-location strategy for production environments to permit the resumption of operation at other Company data centers in the event of a loss of a facility.

System Capacity Monitoring

Current processing capacity is systematically evaluated in real time and production resources are automatically scaled to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.

Testing of Contingency Plan

The Security Officer establishes criteria for contingency plan validation/testing, a testing schedule that meets the requirements of the information security policy, and proper implementation of the test. This process also serves as training for personnel involved in the plan's execution. Validation/testing exercises include tabletop and technical testing.

Disruption Response

Actions are taken to detect and assess the damage inflicted on ABC by a disruption to ABC. Known information is presented to the Security Officer for initial assessment and estimated recovery time. Based on the assessment of the event and criteria as determined by ABC policies, the contingency plan may be activated by the Security Officer.

Vendor Management

ABC requires a standard business agreement with customers, vendors, partners, and subcontractors. The agreement includes the security protocols, services management, and responsibilities that are required in accordance with ABC's security policies. Vendors must coordinate, manage, and communicate any changes to services provided to ABC. ABC utilizes monitoring tools to regularly evaluate vendors against relevant requirements of the agreement.

ABC maintains and reviews a list of current vendors, partners, and subcontractors on at least a quarterly basis. The list is maintained by the ABC Security Officer and includes details on provided services and contact information. During this review, ABC assesses security, compliance, and other requirements and considerations with vendors, partners, and subcontractors. This includes an assessment of independent third-party or other attestation reports as available.

ABC does not allow third-party access to production systems containing confidential information. Connections and data in transit between the ABC platform and third parties are encrypted end to end.

Changes to third-party services are classified as configuration management changes and thus are subject to the Company's change management policies and procedures. Substantial changes to services provided by third parties will invoke a risk assessment.

No ABC customers, vendors, or partners have access outside of their own environment, meaning they cannot access, modify, or delete any information related to other third parties.

DATA

Data related to the ABC Processing System consists of transaction streams, files, data stores, tables, and output used or processed by ABC.

Production Application	Description	Data Store
Usage Information	ABC keeps track of user activity in relation to the types of services users and their customers use, the configuration of their computers, and performance metrics related to their use of the ABC service.	XYZ Databases
User/Account Data	ABC collects data from its employees, customers, customers' employees, and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Via the platform, ABC customers define and control the data they load and store in the ABC Processing System production network. Customer data is loaded into the system and accessed remotely by customers via the Internet.	XYZ Databases
Log Information	ABC logs information about customers and their users, including Internet Protocol (IP) address. Log files are immutable records of computer events about an operating system, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.	SIEM Tool

SYSTEM INCIDENTS

There were no significant system incidents identified that (a) were the result of controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements during the period January 1, 20XX, to December 31, 20XX.

Note to Readers: *The above example assumes no significant system incidents were identified. Paragraph 3.41 of AICPA Guide* SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy *provides an illustrative disclosure made about an identified system incident that resulted in a significant failure of the service organization to achieve one of its availability commitments.*

APPLICABLE TRUST SERVICES CRITERIA AND RELATED CONTROLS

APPLICABLE TRUST SERVICES CRITERIA

The security, availability, and confidentiality categories and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description.

- The security criteria and the controls designed, implemented, and operated to meet those criteria ensure that the information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability or confidentiality of information or systems and affect the organization's ability to meet its objectives.
- The availability criteria and the controls designed, implemented, and operated to meet those criteria ensure that information and systems are available for operation and use to meet the organization's objectives.
- The confidentiality criteria and the controls designed, implemented, and operated to meet those criteria ensure that information designated as confidential is protected to meet the organization's objectives.

CONTROLS RELATED TO THE APPLICABLE CRITERIA

The objective of ABC's system of internal control is to provide reasonable assurance that its service commitments and system requirements are achieved. ABC's system of internal control consists of the policies and procedures at ABC as well as relevant controls, and addresses all aspects of the organization.

The controls supporting ABC's system of internal control are included in section 4 of this report. Although the controls supporting ABC's system of internal control are included in section 4, they are an integral part of ABC's description of the ABC Processing System.

COMPLEMENTARY USER ENTITY CONTROLS (CUECS)

There are no controls at the user entity that are necessary, in combination with ABC's controls, to provide reasonable assurance that ABC's service commitments and system requirements were achieved based on the applicable trust services criteria (complementary user entity controls).

User Entity Responsibilities

There are, however, certain responsibilities that users of the system must fulfill for the user entity to derive the intended benefits of the services of the ABC Processing System. The user entity responsibilities presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities. User entities are responsible for their own control environments and their operational effectiveness.

Criteria	User Entity Responsibilities
CC2.1	• User entities have policies and procedures to that require reporting any material changes to their control environment that may adversely affect the ability of ABC to deliver service. • User entities have controls that require providing notice to ABC of any material changes in security requirements and the authorized users list.

Criteria	User Entity Responsibilities
CC2.3	• User entities have policies and procedures to determine how to file inquiries, complaints, or disputes to ABC.
CC6.1	• User entities have policies and procedures that grant ABC system access only to authorized and trained personnel.
CC6.4	• User entities deploy physical security and environmental controls for all local and remote devices and access points that access the ABC system.
CC6.6	• User entities have policies and procedures for controlling user IDs and passwords that are used to access the ABC system.

SUBSERVICE ORGANIZATIONS

The description does not extend to the services provided by XYZ Cloud Hosting (the subservice organization). Section 4 of this report and the description of the system only cover the relevant trust services criteria and related controls in support of the achievement of ABC's service commitments and system requirements and exclude the related controls of the subservice organization.

Although the subservice organization has been carved out for the purposes of this report, ABC management has assumed, in the design of the system, that certain complementary subservice organization controls (CSOCs) would be implemented by the subservice organization. Such controls are necessary, in combination with controls at ABC, to provide reasonable assurance that ABC's service commitments and system requirements were achieved. Because the related service commitments and system requirements can only be achieved if the CSOCs are suitably designed and operating effectively during the period January 1, 20XX, to December 31, 20XX, each user entity must evaluate ABC's controls, related tests of controls, and results of tests described in section 4 of this report, considering the types of related CSOCs expected to be implemented at the subservice organization as shown below.

Subservice Organization	Services Provided	Criteria	Expected CSOCs
XYZ Cloud Hosting	Infrastructure Hosting	CC6.4	• Physical access to data centers is approved by an authorized individual. • Physical access is revoked within 24 hours of an employee or vendor record being deactivated. • Physical access to data centers is reviewed on a quarterly basis by appropriate personnel. • Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations. • Access to server locations is managed by electronic access control devices.
		CC7.2 A1.2	• Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents. • Data centers are protected by fire detection and suppression systems. • Data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels • Data centers are monitored for power outages and have generators to provide backup power in case of electrical failure..

Subservice Organization	Services Provided	Criteria	Description
		CC8.1	• Changes to customer-affecting aspects of a service are reviewed, tested, and approved. • Separate production and development environments are maintained. • Changes are reviewed for business impact and approved by authorized personnel prior to migration to production. • Deployment validations and change reviews are performed to detect unauthorized changes to the environment.
		C1.2	• Production media is securely decommissioned, physically destroyed, and verified prior to leaving the data center.

Management of ABC receives and reviews independent third-party assessment reports of its subservice organization annually. In addition, ABC management monitors the services performed by the subservice organization to determine whether operations and controls expected to be implemented at the subservice organization are suitably designed and operating effectively. Management monitors the subservice organization status page to stay informed of any changes in the services performed and has a customer support portal to relay any issues or concerns to subservice organization management.

SPECIFIC CRITERIA NOT RELEVANT TO THE SYSTEM

There were no specific security, availability, or confidentiality Trust Services Criteria as set forth in TSP Section 100 that were not relevant to the system as presented in this report.

Note to Readers: *The above example assumes that all criteria related to security, availability, and confidentiality were relevant to the system presented in this report. Paragraph 3.72 of AICPA Guide* SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy *provides an example of a situation where a criterion may not be applicable and of the information that should be disclosed.*

CHANGES TO THE ABC PROCESSING SYSTEM

There were no changes that are likely to affect report users' understanding of how the system is used to provide the service from January 1, 20XX, to December 31, 20XX.

Note to Readers: *The above example assumes that there were no significant changes to the system. AICPA Guide* SOC 2® Reporting on an Examination of Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy *provides examples of changes that may be discussed beginning at paragraph 3.74.*

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

Note to Readers: *The following example presents one way of providing a detailed description of controls alongside the service auditor's tests of controls and results thereof (section 4), with a reference in the body of the description (section 3) to those detailed controls. Although the applicable trust services criteria, related controls, and management responses to deviations, if any, are presented in this section, they are an integral part of the ABC system throughout the period January 1, 20XX, to December 31, 20XX. This is not the only way the detailed description of controls may be presented. For example, management may choose to describe the controls in detail in the description of the system in section 3 with a reference to those controls in section 4. When deciding how best to present controls, service organization management may select the format that best meets its objectives, the needs of its users, and its users' likely frame of reference; it may also consider the risk that use of a particular format may be misleading to users.*

ABC's controls and test of controls presented in this section are for illustrative purposes and, accordingly, are not all-inclusive and may not be suitable for all service organizations and examinations. For brevity, not all trust services criteria and not all controls are presented. Ellipses (…) are used to designate areas where content has been omitted. As described in section 3, ABC Service Organization has engaged the service auditor to examine and report on the description of the service organization's payment solutions system and its controls relevant to security, availability, and confidentiality to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. As such, management would present all criteria for the security, availability, and confidentiality categories and the related controls designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved.

ABC has designed and implemented controls to provide reasonable assurance that ABC's service commitments and system requirements were achieved. These controls are presented below and are an integral part of ABC's description of the ABC Processing System throughout the period January 1, 20XX, to December 31, 20XX. Controls are mapped to each applicable trust services criteria and are organized by criteria area. Control numbers are unique identifiers designed to align with the relevant trust service criteria.

Controls Mapped to Criteria			
Criteria Area	**TSC Reference #**	**Supporting Control Activity**	**Criteria**
CC1.0	Control Environment		
	CC1.1	ABC1	*COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.*
		ABC2	
		ABC3	
		ABC4	
		ABC5	
		ABC6	

..... Content omitted for brevity .....

CC6.0	Logical and Physical Access		
	CC6.2	ABC31	*Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.*
		ABC32	
		ABC34	

..... Content omitted for brevity .....

Control Number	Control Activity	Criteria Mapping	Service Auditor's Tests	Results of Tests
ABC1	Employees are required to read and accept the information security policy upon hire and on an annual basis thereafter. The information security policy includes the Company's code of conduct describing the responsibilities and expected behavior of employees.	CC1.1 CC1.5 CC5.3	For a population of active and newly hired employees from the HR system: • Inspected acknowledgments for a sample of new hires to determine that new hires were required to acknowledge that they had read and agreed to the information security policy upon hire. • Inspected acknowledgments or a sample of employees to determine that employees were required to annually acknowledge that they had read and agreed to the information security policy.	No exceptions noted in the sample of new hires. One exception was noted in a sample of 25 active employees selected for testing.

			Inspected the information security policy to determine that it documented the code of conduct, which includes employee responsibilities and expected behavior regarding data and information system usage.	No exceptions noted.
			Inspected the Company intranet to determine that the information security policy was communicated and available to internal employees.	No exceptions noted.

..... Content omitted for brevity .....

ABC31	Access to in-scope system components requires a documented access request form and manager approval prior to access being provisioned. The control did not operate during the period because the circumstances that warrant the operation of the control did not occur during the period. No new access requests were initiated during the review period.	CC6.2 CC6.3	Inquired of management and inspected the access request management process to the in-scope system components to determine that the circumstances that warrant the operation of the control did not occur during the period.	Not tested. No new access requests were initiated during the review period.

..... Content omitted for brevity .....

Section 5 — Other Information Provided by Example Service Organization That Is Not Covered by the Service Auditor's Report

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

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

For brevity, an example is not provided.

P: 888.777.7077 | F: 800.362.5066 | W: aicpa-cima.com

Founded by AICPA and CIMA, the Association of International Certified Professional Accountants powers leaders in accounting and finance around the globe.