Illustrative Type 2 SOC 2SM Report with the Criteria in the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM)

The AICPA guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2SM)* specifies the components of a SOC 2SM report and the information to be included in each component, but it does not specify the format for these reports. Service organizations and service auditors may organize and present the required information in a variety of formats. The format of the illustrative type 2 SOC 2 report presented in this document is meant to be illustrative rather than prescriptive. The illustrative report contains all of the components of a type 2 SOC 2 report; however, for brevity, it does not include everything that might be described in a type 2 SOC 2 report. Ellipses (...) or notes to readers indicate places where detail has been omitted.

The trust services principle(s) being reported, the controls specified by the service organization, and the tests performed by the service auditor are presented for illustrative purposes only. They are not intended to represent the principles that would be addressed in every type 2 SOC 2 engagement, or the controls, or tests of controls, that would be appropriate for all service organizations. The trust services principles on which the report is based, 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 SOC 2 engagement will vary based on the specific facts and circumstances of the engagement. Accordingly, it is expected that actual type 2 SOC 2 reports will address different principles and include different controls and tests of controls that are tailored to the service organization that is the subject of the engagement.

The Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM) Version 1.4 is used for the purpose of this illustrative report. The CSA periodically issues new criteria. The practitioner should identify the CCM version being used as criteria in management's assertion and the service auditor's report.

Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2009) is used for the purpose of this illustrative report. The AICPA periodically issues new *Trust Services Principles and Criteria*. The practitioner should identify the current *Trust Services Principles and Criteria* version for management's assertion and the service auditor's report.

Illustrative Type 2 SOC 2[SM] Report: Reporting on the Security and Availability of a System Using the Criteria for Security and Availability in Section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) and on the Controls of a System Using the Criteria in the Cloud Security Alliance Cloud Controls Matrix

In the following illustrative type 2 SOC 2 report, the service auditor is reporting on

- the fairness of the presentation of the service organization's description of its system based on the description criteria identified in management's assertion; and
- the suitability of the design and operating effectiveness of its controls relevant to security and availability based on the criteria for security and availability in TSP Section 100A, Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Technical Practice Aids) and, the suitability of the design and operating effectiveness of its controls in meeting the criteria in the CCM.

Description of Example Cloud Service Organization's Infrastructure Services System Relevant to Security and Availability For the Period January 1, 20XX, through December 31, 20XX, with Independent Service Auditor's Report including Tests Performed and Results Thereof

---

Section 1 — Management of Example Cloud Service Organization's Assertion Regarding its Infrastructure Services System Throughout the Period January 1, 20X1, to December 31, 20X1

Section 2 — Independent Service Auditor's Report

Section 3 — Example Cloud Service Organization's Description of its Infrastructure Services System Throughout the Period January 1, 20X1, to December 31, 20X1

System Overview and Background

Infrastructure
Software
People
Procedures
Data

Customer Responsibilities

A. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring
B. Policies and Procedures
C. Communication
D. Physical Security
E. Logical Security
F. Monitoring
G. Relationship between CCM Criteria, Description Sections, and Trust Services Criteria

---

Section 4 — Applicable Trust Services Principles, Criteria, and CCM Criteria and Related Controls, Tests of Controls, and Results of Tests

---

Section 5 – Other Information Provided by Example Cloud Service Organization Not Covered by the Service Auditor's Report

---

Language shown in ***boldface italics*** represents modifications that would be made to the service auditor's report if complementary user-entity controls are needed to meet certain applicable trust services criteria.

Section 1 — Management of Example Cloud Service Organization's Assertion Regarding its Infrastructure Services System Throughout the Period January 1, 20X1, to December 31, 20X1

We have prepared the description in the section titled, "Example Cloud Service Organization's Description of its Infrastructure Services System Throughout the Period January 1, 20X1, to December 31, 20X1," (description), based on the criteria for a description of a service organization's system identified in paragraph 1.34 of the AICPA guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2[SM])* (description criteria). The description is intended to provide users with information about the Infrastructure Services System, particularly system controls intended to meet the criteria for the security and availability principles (applicable trust services criteria) set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*), and the criteria set forth in the CSA Cloud Controls Matrix (CCM) Version 1.4 control specifications (CCM criteria[1]). We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the Infrastructure Services System throughout the period January 1, 20X1, to December 31, 20X1, based on the following description criteria:

i. The description contains the following information:

(1) The types of services provided

(2) The components of the system used to provide the services, which are the following:

(a) **Infrastructure.** The physical and hardware components of a system (facilities, equipment, and networks)

(b) **Software.** The programs and operating software of a system (systems, applications, and utilities)

(c) **People.** The personnel involved in the operation and use of a system (developers, operators, users, and managers)

(d) **Procedures.** The automated and manual procedures involved in the operation of a system

(e) **Data.** The information used and supported by a system (transaction streams, files, databases, and tables)

(3) The boundaries or aspects of the system covered by the description

(4) How the system captures and addresses significant events and conditions

(5) The process used to prepare and deliver reports and other information to user entities or other parties

(6) If information is provided to, or received from, subservice organizations or other parties, (a) how such information is provided or received and the role of the subservice organization or other parties, and (b) the procedures performed to determine

[1] The control specifications included in the CCM constitute suitable criteria, as defined in paragraph 24 of AT 101, *Attest Engagements* (AICPA *Professional Standards*). Omission of one or more of the criteria is likely to result in criteria that are not suitable because they are not complete. The CSA periodically issues new criteria. The practitioner should check the CSA website for current applicable criteria and identify the CCM version being used as criteria in management's assertion and the service auditor's report.

that such information and its processing, maintenance, and storage are subject to appropriate controls[2]

(7) For each principle being reported on, the applicable trust services and CCM criteria and the related controls designed to meet those criteria, including, as applicable, (a) complementary user-entity controls contemplated in the design of the service organization's system, and (b) when the inclusive method is used to present a subservice organization, controls at the subservice organization[3]

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria; and for privacy, the types of activities that the subservice organization would need to perform to comply with our privacy commitments[4]

(9) Any applicable trust services criteria that are not addressed by a control at the service organization and the reasons therefore

(10) Other aspects of the service organization's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria

(11) Relevant details of changes to the service organization's system during the period covered by the description

ii. The description does not omit or distort information relevant to the service organization's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. the controls stated in the description were suitably designed throughout the period January 1, 20X1, to December 31, 20X1, to meet the applicable trust services criteria and the CCM criteria; and

c. the controls stated in the description operated effectively throughout the period January 1, 20X1, to December 31, 20X1, to meet the applicable trust services criteria and the CCM criteria.

---

[2] Certain description criteria may not be pertinent to a particular service organization or system. For example, a service organization may not use any subservice organizations or other parties to operate its system. Because the criteria in paragraph 1.34 of the SOC 2 guide may not be readily available to report users, management of a service organization should include in its assertion all of the description criteria in paragraph 1.34 of the SOC 2 guide. For description criteria that are not pertinent to a particular service organization or system, report users generally find it useful if management presents all of the description criteria and indicates which criteria are not pertinent to the service organization and the reasons therefore. Management may do so either in its system description or in a note to the specific description criteria. The following is illustrative language for a note to criteria that are not pertinent to the service organization or its system:

Example Cloud Service Organization does not use subservice organizations or other parties to operate its infrastructure services system. Accordingly, our description does not address the criteria in items (a)(i)(6) and (a)(i)(8).

[3] See footnote 3.

[4] See footnote 3.

Section 2 — Independent Service Auditor's Report

Independent Service Auditor's Report

To Management of Example Cloud Service Organization

Scope

We have examined the description in the section titled "Example Cloud Service Organization's Description of its Infrastructure Services System Throughout the Period January 1, 20X1, to December 31, 20X1" (the description) based on the criteria set forth in paragraph 1.34 of AICPA guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2[SM])* (the description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the security and availability principles set forth in TSP section 100A, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), throughout the period January 1, 20X1, to December 31, 20X1. We have also examined the suitability of the design and operating effectiveness of controls to meet the requirements set forth in the Cloud Security Alliance's (CSA's) Cloud Controls Matrix (CCM) Version 1.4 control specifications (CCM criteria).

The information in the section titled "Other Information Provided by Example Cloud Service Organization Not Covered by the Service Auditor's Report" describes the service organization's future plans for new systems. It is presented by the management of Example Cloud Service Organization to provide additional information and is not a part of the service organization's description of its Infrastructure Services System made available to user entities during the period from January 1, 20X1, to December 31, 20X1. Information about Example Cloud Service Organization's future plans for new systems has not been subjected to the procedures applied in the examination of the description of the Infrastructure Services System and the suitability of the design and operating effectiveness of controls to meet the related applicable trust services criteria and CCM criteria stated in the description of the Infrastructure Services System.

Service Organization's Responsibilities

Example Cloud Service Organization has provided its accompanying assertion titled "Management of Example Cloud Service Organization's Assertion Regarding its Infrastructure Services System Throughout the Period January 1, 20X1, to December 31, 20X1," regarding the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria and the CCM criteria. Example Cloud Service Organization is responsible for (1) preparing the description and the assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and the CCM criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria and the CCM criteria.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the

- fairness of the presentation of the description based on the description criteria; and
- suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria and suitability of the design and operating effectiveness of the controls to meet the CCM criteria, based on our examination.

We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria and CCM criteria throughout the period January 1, 20X1, to December 31, 20X1.

Our examination involved performing procedures to obtain evidence about (1) the fairness of the presentation of the description based on the description criteria and (2) the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria and CCM criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria and CCM criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria and CCM criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria and CCM criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the description criteria identified in Example Cloud Service Organization's assertion and the applicable trust services criteria and CCM criteria,

a. the description fairly presents the system that was designed and implemented throughout the period January 1, 20X1, to December 31, 20X1;

b. the controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria and CCM criteria would be met if the controls operated effectively throughout the period January 1, 20X1, to December 31, 20X1; and

c. the controls tested, which if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria and CCM criteria were met, operated effectively throughout the period January 1, 20X1, to December 31, 20X1.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section titled, "Applicable Trust Services Principles, Criteria, and CCM Criteria and Related Controls, Tests of Controls, and Results of Tests," of this type 2 report in columns 2, 3, and 4, respectively.

Restricted Use

This report and the description of tests of controls and results thereof are intended solely for the information and use of Example Cloud Service Organization; user entities of Example Cloud Service Organization's Infrastructure Services System during some or all of the period January 1, 20X1, to December 31, 20X1; and prospective user entities, independent auditors and practitioners providing services to such user entities, 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 or other parties
- Internal control and its limitations
- The applicable trust services criteria and CCM criteria
- The risks that may threaten the achievement of the applicable trust services criteria and CCM criteria 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*]

[*Date of the service auditor's report*]

[*Service auditor's city and state*]

Section 3 — Example Cloud Service Organization's Description of its Infrastructure Services System Throughout the Period January 1, 20X1, to December 31, 20X1

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 management's description of the service organization's system. Ellipses (…) or notes to readers indicate places where detail has been omitted from the illustration.

System Overview and Background

Example Cloud Service Organization (Company) provides cloud computing, managed hosting, and co-location services to organizations worldwide. These services are primarily provided from the data centers in Chicago, San Diego, Bristol, Paris, Mumbai, and Tokyo.

Types of Services Provided

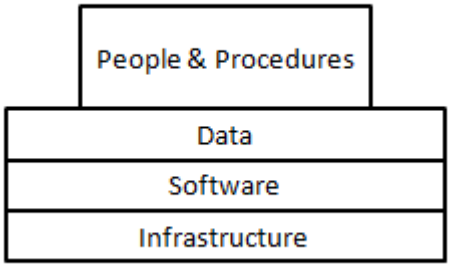
This description addresses Example Cloud Service Organization's infrastructure-as-a-service public and private cloud offerings. Example Cloud Service Organization provides the following services, all of which are covered by this report. If a customer of Example Cloud Service Organization's infrastructure-as-a service public and private cloud offerings has not purchased certain services, the portions of the description that cover those services will not be relevant to those customers. For that reason, it is recommended that customers confirm the services they have purchased by selecting XXX in the Control Panel or contacting their Example Cloud Service Organization account executive.

- Cloud Services
  - Infrastructure implementation and management
  - OS patch management
  - Managed backups
  - Managed Intrusion Protection System (IPS)
  - Managed load balancing
  - Managed firewalling and Virtual Private Network (VPN)

- Managed Hosting /Co-location Services
  - Cloud computing (sites and/or servers)
  - OS patch management
  - Managed backups
  - Managed Intrusion Protection System (IPS)

- Managed load balancing
- Managed virtual firewalling

Components of the System Providing Services



Infrastructure

Cloud services are provided to users using IT equipment located in the data center locations in Chicago, San Diego, Bristol, Paris, Mumbai, and Tokyo. Failover services[1] are provided from San Diego, Paris facilities, and a second facility in Tokyo.

Services are provided using a range of hardware, including IBM and Dell servers, EMC Storage Area Networks (SANs), and Networking Equipment from multiple providers.

Software

Example Cloud Service Organization provides cloud services using the hardware identified under the heading "Infrastructure," which supports a range of operating system software. These provide common or dedicated platforms that are maintained by Example Cloud Service Organization. In addition, for certain customers that have contracted with Example Cloud Service Organization to perform these services, Example Cloud Service Organization will also provide server backups, management of dedicated customer firewalls, and managed load-balancing.[2]

People

Services are provided by Example Cloud Service Organization Network Operations, Security, Support, Sales, Billing, Retention, Product Development, Information Technology (IT), Facilities, and Executive Management teams.

All Example Cloud Service Organization teams are recruited and managed using Example Cloud Service Organization policies and procedures which are described in the following sections.

Procedures

---

[1] Failover services involve switching to a redundant or standby computer, server, system, hardware component, or network upon the failure or abnormal termination of the previously active application, server, system, hardware component, or network.

[2] Load balancing is a computer networking method for distributing workloads across multiple computing resources, such as computers, a computer cluster, network links, central processing units, or disk drives. Load balancing aims to optimize resource use, maximize throughput, minimize response time, and avoid overload of any one of the resources.

Formal IT policies and procedures exist that describe incident response, network security, encryption, and system security standards. All teams are expected to adhere to the Example Cloud Service Organization policies and procedures that define how services should be delivered. These are located on the company's intranet and can be accessed by any Example Cloud Service Organization team member.

Data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer contracts. This data is managed and stored in a range of database technologies.

Customer Responsibilities

Administrator-level user access privileges granted to customers and to their respective environment(s) are initially provided via e-mail using uniquely generated passwords that follow the Example Cloud Service Organization standard for secure passwords (at least 8 characters, lower and uppercase letters, one number, and one symbol). The password is paired with the customer's account information to establish accountability for user actions in the Example Service Organization's system. In addition, although recommended, at the customer's discretion, the uniquely generated initial password associated with the customer's user ID must be changed upon initial login.

Because Dedicated and Virtual customers have system administrator-level privileged access to most configurations and have the ability to perform logical security administration functions for their respective environments, any customer-initiated changes or modifications to servers, services (including anti-virus definitions), or logical access entitlements are exclusively the responsibility of these customers.

Hypervisors are not used on dedicated servers unless enabled. Example Cloud Service Organization requires that a customer's ability to gain logical access be performed from behind a dedicated firewall and on a customized encrypted network session in order to implement a hypervisor.[3] It is the customer's responsibility to maintain hypervisors where installed and this process is excluded from the scope of this report.

Since customers are assigned physical data center keys that provide them with physical access to the racks on which their dedicated servers reside, customer-initiated server maintenance activities performed by customers are excluded from the scope of this report.

[3] A hypervisor is a piece of computer software, firmware, or hardware that creates and runs virtual machines.

Outside of Scope
-Client administrator level access management
-Hypervisor management
-Physical server keys
-Other Complementary User Entity Controls

A. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication Systems, and Monitoring

This section provides information about the five interrelated components of internal control at Example Cloud Service Organization:

1. **Control Environment.** Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.
2. **Control Activities.** The policies and procedures that help make sure that management's directives are carried out.
3. **Information and Communication.** Systems, both automated and manual, that support the identification, capture, and exchange of information in a form and time frame that enable people to carry out their responsibilities.
4. **Monitoring.** A process that assesses the quality of internal control performance over time.
5. **Risk Assessment.** The entity's identification and analysis of relevant risks to the achievement of its objectives, forming a basis for determining how the risks can be managed.

Example Cloud Service Organization internal control components include controls that may have a pervasive effect on the organization, or may affect specific processes or applications, or both. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or applications. When evaluating internal control, we consider the interrelationships among the five components.

Control Environment

The objectives of internal control as it relates to the Cloud Infrastructure Service System are to provide reasonable, but not absolute, assurance that controls are suitably designed and operating effectively to meet the relevant controls, that assets are protected from unauthorized use or disposition, and that transactions are executed in accordance with management's authorization and client instructions. Management has established and maintains controls designed to monitor compliance with established policies and procedures. The remainder of this subsection discusses the tone at the top as set by management, the integrity, ethical values, and competence of Example

Cloud Service Organization employees, the policies and procedures, the risk management (RM) process and monitoring, and the roles of significant control groups. The internal control structure is established and refreshed based on Example Cloud Service Organization's assessment of risk facing the organization.

Integrity and Ethical Values

Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of key processes. Integrity and ethical behavior are the products of Example Cloud Service Organization's ethical and behavioral standards, how they are communicated, and how they are monitored and enforced in its business activities. They include management's actions to remove or reduce incentives/pressures, and opportunities that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of the entity's values and behavioral standards to personnel through policy statements and codes of conduct, and by the examples the executives set.

The Example Cloud Service Organization Board of Directors (the Board) and management recognize their responsibility to foster a strong ethical environment within Example Cloud Service Organization to determine that its business affairs are conducted with integrity, and in accordance with high standards of personal and corporate conduct. This responsibility is characterized and reflected in the Example Cloud Service Organization Code of Business Conduct and Ethics (the Code of Conduct), which is distributed to all employees of the organization. Specifically, employees and their immediate families are prohibited from using their positions with Example Cloud Service Organization for personal or private gain, disclosing confidential information regarding clients, or taking any action that is not in the best interest of clients. Employees' personal securities transactions are governed by corporate policy and employee account trades are reviewed to monitor adherence to Example Cloud Service Organization policy. All employees are required to maintain ongoing compliance with all statements of policies, procedures, and standards of the Code of Conduct and with lawful and ethical business practices, whether or not they are specifically mentioned in the Code of Conduct. Each employee is required to affirm annually that he or she received, read, understood, and complied with the requirements set forth in the Code of Conduct and the Employee Handbook. Employee recertification status is monitored periodically for compliance.

Organizational Structure and Assignment of Authority and Responsibility

Example Cloud Service Organization's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Example Cloud Service Organization has established an organizational structure that includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting.

Example Cloud Service Organization has an established organization structure with defined roles and responsibilities.

Governance and Oversight: The Board of Directors

Example Cloud Service Organization's control environment is influenced significantly by the Board and other groups (as defined later in this subsection) who are charged with governance.

The Board consists of seven independent, non-executive directors, two executive directors, and a Chairman. Each member of the Board possesses adequate, relevant experience, and is recognized as an individual of high integrity and good stature. The Board is actively involved in and scrutinizes the activities of Example Cloud Service Organization's functional groups, and takes action with respect to its fiduciary responsibilities. Additionally, the Board raises questions and pursues key initiatives with management, as well as interacts periodically with both the internal and external auditors. Specifically, the Board meets on a regular basis to review operating performance, strategy, corporate governance and risks, and to oversee appropriate shareholder reporting. The Board is responsible for overseeing Example Cloud Service Organization's corporate governance, and has discretion to delegate a broad range of powers and decisions to the Management Committee (described in the following subsection) in order to manage the entity and its business on a daily basis. The Board meets on a quarterly basis, or more frequently if necessary. The Board has three formal committees: the Nominations Committee, the Audit Committee, and the Compensation Committee.

The Audit Committee is responsible for, among other things, overseeing and monitoring the integrity of Example Cloud Service Organization's consolidated financial statements, the entity's compliance with legal and regulatory requirements as they relate to financial reporting or accounting matters, and the organization's internal accounting and financial controls; overseeing and monitoring Example Cloud Service Organization's independent auditor's qualifications, independence, and performance; providing the Board with the results of its monitoring and recommendations; providing the Board with additional information and materials as it deems necessary to make the Board aware of significant financial matters that require the attention of the Board; and overseeing the Example Cloud Service Organization's internal audit function. The Audit Committee generally meets three times a year, and has discussions with both the external and internal auditors at each meeting.

Governance and Oversight: The Management Committee

The Management Committee, chaired by the Chief Executive Officer ("CEO"), has been delegated by the Board the responsibility for managing Example Cloud Service Organization and its business on a daily basis. Members of Example Cloud Service Organization's Management Committee draw experience from their former roles as senior executives of large international banks and organizations specializing in middle- and back-office support services for investment advisors.

In its role, the Management Committee assigns authority and responsibility for operating activities, and establishes reporting relationships and authorization hierarchies. The Management Committee designs policies and communications so that personnel understand Example Cloud Service Organization's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. The Management Committee convenes weekly.

Lines of authority and responsibility are clearly established throughout the organization under the Management Committee. These lines of authority and the associated responsibilities are communicated through: (1) management's philosophy and operating style, (2) organizational structure, (3) employee job descriptions, and (4) policy and procedure manuals. Managers are expected to be aware of their responsibilities and lead employees in complying with Example Cloud Service Organization's policies and procedures.

Governance and Oversight: Human Resource Policies and Practices

Human resource (HR) policies and practices relate to hiring, orienting, training, evaluating, counseling, promoting and compensating personnel. The competence and integrity of Example Cloud Service Organization's personnel are essential elements of its control environment. The organization's ability to recruit and retain a sufficient number of competent and responsible personnel is dependent to a great extent on its HR policies and processes.

The HR policies and processes of Example Cloud Service Organization are designed to: (1) identify and hire competent personnel, (2) provide employees with the training and information they need to perform their jobs, (3) evaluate the performance of employees to verify their ability to perform job assignments, and (4) through performance evaluation, identify opportunities for growth and job performance improvement.

Formal written job descriptions are developed and maintained for each position. Each job description is reviewed and updated annually by a manager responsible for overseeing employees with that description. Job description reviews occur in conjunction with the annual performance review process. The review includes evaluation of the job for incompatible duties. Changes to formal written job descriptions are submitted to HR for review and approval. Formal written job descriptions are also prepared for contractors who work under the direct supervision of Example Cloud Service Organization's management.

Example Cloud Service Organization has also established formal classroom instruction, web-based training, and on-the-job employee training programs for critical departments and functions. Programs include orientation on the basics of the functional team's operations, individualized instruction manuals for selected departments, and regularly scheduled department workshops. Employees are also encouraged to actively participate in professional organizations and forums to maintain their knowledge and develop awareness of issues facing Example Cloud Service Organization.

Governance and Oversight: New Hire Process

Managers within the respective functional groups of the organization determine the need for additional resources and submit formal job requisitions to senior management for approval. Once requisitions have been approved by the appropriate individual(s), HR begins sourcing for the available position. HR screens potential candidates and sends

selected résumés to the respective managers. The managers review documentation, select candidates, and inform HR of individuals with whom they wish to schedule interviews. The relevant manager and HR conduct interviews and potential offers are submitted to the appropriate authority within the organization for approval.

Individuals offered a position at Example Cloud Service Organization are subject to background checks (as appropriate for each country with respect to local laws and regulations) prior to commencing employment. Vendor employees requiring access card/IDs are also subject to background checks. The background check for employees includes substantiation of educational credentials, previous employment, compensation history, credit history, and criminal record, as applicable. The background check for vendor employees addresses only their criminal record. Prospective employees complete an employment application and sign waivers to release information for the background check. In addition, it is the policy of Example Cloud Service Organization to request employment references to determine whether the candidate is well-qualified and has the potential to be productive and successful during his or her tenure.

In each location, employees receive data packages containing an overview of Example Cloud Service Organization's HR policies and procedures. These offer packages include the offer letter or employment contract, the Employee Handbook, relevant compensation materials, benefit materials and the Code of Conduct. Employees are asked in signing their offer to confirm that they have read through these materials.

Vendor employees and non-employee personnel must sign an access and use agreement, the terms being substantially similar to the Code of Conduct, prior to being granted access to Example Cloud Service Organization assets or facilities.

HR is responsible for managing voluntary and involuntary terminations. Voluntary terminations are identified by the employee's supervisor and are recorded in the event management system. HR personnel communicate with the employee to identify the employee's final day of employment and to inform the employee of his or her rights and responsibilities. The final day is entered into the HR management system and an exit interview is scheduled for that date. During the exit interview, the employee is asked to return any of Example Cloud Service Organization's assets in his or her possession, including access card/ID, two-factor authentication token, credit card, laptop, and so on. The HR person records the information in the event management system and provides the employee with a signed receipt for the items.

Governance and Oversight: Performance Management

Example Cloud Service Organization has implemented a structured performance appraisal process. Managers are asked to discuss performance expectations and goals with each employee at the start of the year. These objectives and development goals are documented in a web-based performance management system. Example Cloud Service Organization has a formal mid-year review process, and also conducts an annual performance review for each employee at the completion of the calendar year. Employees are also required to complete an annual self-appraisal of their performance, attributes, and progress toward stated goals. Annual performance evaluations affirmed by the employee, his or her manager, and director are maintained in electronic form. Managers are also strongly encouraged to have ongoing, informal conversations with employees regarding their performance throughout the year.

Example Cloud Service Organization has developed a mandatory training program for its employees, including a coordinated new hire orientation program and targeted courses that must be passed to be eligible for promotion. Additional continuing professional education and development opportunities are identified through the goal-setting and development-planning process. Managers and HR identify learning plans both by role and level. It is also the manager's role to identify what training a particular employee requires to comprehend Example Cloud Service Organization's policies and procedures as they relate to specific job requirements. Each employee has the opportunity to partake in formal training classes, on-the-job training, or online education courses. A record of training program attendance is maintained for each employee.

Risk Assessment

The process of identifying, assessing, and managing risks is a critical component of Example Cloud Service Organization's internal control system. The purpose of Example Cloud Service Organization's risk assessment process is to identify, assess, and manage risks that affect the organization's ability to achieve its objectives. The management of Example Cloud Service Organization also monitors controls to consider whether they are operating as intended, and whether they are modified as appropriate for changes in conditions or risks facing the organization.

Ongoing monitoring procedures are built into the normal recurring activities of Example Cloud Service Organization and include regular management and supervisory activities. Managers of the various organizational units are regularly in touch with personnel and may question the accuracy of information that differs significantly from their knowledge of operations.

Example Cloud Service Organization has established an independent organizational business unit, Risk Management (RM), that is responsible for identifying risks to the entity and monitoring the operation of the firm's internal controls. RM's approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. RM attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management, including the Management Committee.

Internal Audit (IA) is responsible for assessing the Example Cloud Service Organization's risk and control environment through rigorous evaluation of financial, operational, and administrative controls, RM practices, and compliance with laws, regulations, and Example Cloud Service Organization's policies and procedures. The Global Head of IA reports functionally to the Chairman of the Example Cloud Service Organization Audit Committee and administratively to the President and COO. IA communicates significant findings and the status of corrective actions directly to these individuals. IA adheres to standards of moral and ethical conduct, including those set forth in the Employee Handbook and the Institute of Internal Auditors' (IIA) *Code of Ethics and Standards for the Professional Practice of Internal Auditing*.

Information and Communication

Information and communication is an integral component of Example Cloud Service Organization's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Example Cloud Service Organization, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Various weekly calls are held to discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, town hall meetings are held bi-annually in each geographic location to provide staff with updates on the firm and key issues affecting the organization and its employees. Senior executives lead the town hall meetings with information gathered from formal automated information systems and informal databases, as well as conversations with various internal and external colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Example Cloud Service Organization personnel via e-mail messages.

B. Policies and Procedures

Example Cloud Service Organization has the following security procedures and policies in place, which are owned by the Director of Information Security:

- Acceptable Use Policy
- Cellular Phone and BYOD Policy
- Disaster Recovery Manual
- Encryption Policy
- Enterprise Security Policy
- General Emergency Policy
- Information Sensitivity Policy
- Internal Lab Security Policy
- Internet DMZ Equipment Policy
- Media Destruction Policy
- Network Access/Configuration Policy
- Password Policy
- Patch Management Policy
- Remote Access/VPN Policy
- Router Security Policy
- Server Security Policy
- Software Policy
- User Account Policy
- Wireless Communication Policy

Policies are reviewed at least annually and may be reviewed more frequently if necessary. Members of the Security team are authorized to perform reviews of policies with final approval for changes from the Director of Security in conjunction with other senior management. Approvals are documented via e-mail as they occur. Any changes to the policies are then communicated to employees via e-mail and are posted on an internal SharePoint site accessible to employees.

To mitigate any potential for loss or exploitation of sensitive data, Example Cloud Service Organization maintains a data sensitivity policy to determine whether the appropriate controls are in place for data of higher sensitivity. This policy classifies data into categories and specifies protection accordingly. Policy points are in place to specify privacy treatment of data. The Security team conducts vulnerability assessments of relevant data to ensure compliance with policy points.

C. Communication

Terms and Conditions

Terms and conditions are presented to provide a mechanism for communicating the terms of service within the company and between the company, customers, and website users. The terms and conditions outline terms and payment for services, use of services, enforcement, intellectual property rights, and warranties. Terms of service documents can be found at www.Example Cloud Service Organization.com and the service level agreement can be found at www.Example Cloud Service Organization.com.

Obligations that are outlined within the terms of service and Service Level Agreement as they relate to security and availability are as follows:

- Example Cloud Service Organization shall make all reasonable attempts to provide a 100 percent uptime for Dedicated and Virtual Dedicated Servers.
- Example Cloud Service Organization shall make all reasonable attempts to provide a 99.93 percent server Virtual Private Server (VPS) uptime. This is a legacy product that is no longer offered to new customers.
- Example Cloud Service Organization may schedule network maintenance periods resulting in network interruptions. These maintenance periods will be announced in advance via e-mail to the primary technical contact for the account.
- Customer understands and agrees that occasional temporary interruptions of any Internet services may occur as normal events in the provision of Internet services.
- Indemnification of company and its affiliated parties.

The terms of service are reviewed at least annually or more frequently when deemed necessary. Any changes are reviewed by management and sent to the Marketing Communications team for execution of the changes. Customers are notified via e-mail of any changes. The customer is not required to accept or agree to any change.

D. Physical Security

Physical security throughout Example Cloud Service Organization is the responsibility of Corporate Security. Under the direction of the Director of Physical Security, Corporate Security has developed a set of security policies and procedures that address the following:

- Securing of physical access to and within Example Cloud Service Organization facilities by employees, vendors, and visitors
- Standards for receptions areas, perimeters, surveillance, security guards, and security patrols
- Standards for securing specified types of locations and assets
- Lock and physical security device standards
- Background investigation of employees, prospective employees, and vendor employees
- Issuance of access cards/IDs used to access facilities
- Removal of access by terminated employees/vendor personnel
- Investigation of physical security violations
- Movement of assets

Wholly occupied company facilities are protected by walls and fencing around the entire perimeter. Each facility has a designated reception area which is attended by either a receptionist or a security guard 24 hours per day. Access to the reception area is unlocked from 8am to 5pm on business days and is locked at all other times. When locked, a visitor presses a buzzer to attract the attention of the guard at the visitor desk who can release the lock. The door may also be unlocked through the use of an access card/ID that has been assigned general access to the facility. Access beyond the reception area is controlled through the access card system.
All remaining exterior ingress doors are restricted to users possessing an access card/ID that has been assigned access to use the door. The access card/ID system uses zones to control access. Each exterior door and doors to restricted areas within the facilities are assigned to door zones. Access to zones is restricted through the use of access control lists. Employees and vendors granted access cards are assigned to roles based on their job responsibilities.

Emergency exit doors are alarmed and permit only exit. In an emergency, users are required to hold the release bar for five seconds before the door opens.

All doors are equipped with an audible alarm if the door is forced open. All alarms sound an alert in the physical security center. Closed circuit cameras are in position at each side of each exterior door and within the facilities at sensitive locations within and outside the facilities. The images from these cameras are transmitted to the physical security center for observation and recorded and stored for 90 days.

Each facility has a loading dock secured by a key-activated garage door. Keys are secured in a locked cabinet within the physical security center. Any use of a loading dock requires the presence of a security guard.

Receipt or removal of items through a data center loading dock requires a “gate pass” record in the event management system. Gate pass records record the items received or removed, identify the physical custodian of the item, record the date and time of the event, and require approval of an authorized employee. Receipt or removal of hardware requires the approval of the asset manager or Director of Operations. Receipt or removal of media requires the approval of an operations supervisor. Each receipt or removal is acknowledged by the security guard and attending member of the operations staff on the event record.

Assets with integrated storage media have been data wiped using industry standard methods, or the storage media are physically destroyed prior to the assets’ transfer to a third party or its disposal. Destruction is documented on the gate pass record and must be completed prior to the approval of the gate pass.

Access and ID cards contain a photo ID of the employee and must be worn at all times.

Visitors check in with the receptionist or security guard stationed in the reception area. Visitors must present a valid, government-issued photo ID. The visitor’s name, employer, and purpose for visit are recorded in a visitor log and his or her visit must be approved by an Example Cloud Service Organization employee who is authorized to sign non-employees into the facility. The visitor is issued a temporary ID badge to be worn throughout his or her visit. This temporary badge does not permit users access through any secured doors within the facility.

Entrances to data centers are restricted by two doors; access through the first door is gained by using a key card to deactivate the locking mechanism, and access through the second door is granted by using a biometric hand reader and personal identification number (PIN).

Employees are provided an access card/ID on their first day of work. General access is granted to all employees, permitting access to the facility though reception and employee entrances. Managers may request access cards/IDs for vendor personnel requiring regular access to facilities. Prior to issuance of the card, vendors are subject to background checks. Access to restricted zones is requested by the employee’s supervisor and must be approved by a designated security zone owner. Access is requested through the event management system and is automatically routed to the zone owner for approval. Access to data centers must be approved by the operation manager. Approved requests are entered into the access management system by designated physical security personnel.

The security system isolated from other data networks and the physical security server is housed in the physical security center. A backup physical security server is housed in each data center in the event communication is lost with the physical security center. Logical access to the physical security server is limited to the server administrators and physical security personnel. The ability to create and modify access records is limited to designated access administrators. All changes to access records are logged and stored for seven years. All security events, including permitted and denied access, are logged by the security system and retained for one year. Access to the security system logs is restricted to security supervisors.

Upon an employee’s termination of employment, the HR system automatically generates an access deletion record in the event management system on the last day of employment. This record is routed to the access administrators for deletion. In addition, terminated employees turn over their access cards/IDs during their exit interview. These cards are then sent via interoffice mail to physical security for recording and destruction. On a monthly basis, the director of physical security runs a report detailing access cards with deleted access that have not been recorded as returned. The director investigates all missing cards and documents the resolution in the event management system.

On a quarterly basis, zone owners review access to their zones. Access listings are generated by security and distributed to the zone owners via the event management system. Zone owners review the listings and indicate the required changes in the event management record. The record is routed back to the access administrators for processing. The director of physical security identifies any records not returned within two weeks and follows up with the zone owner.

On a semi-annual basis, the director of physical security sends a list of each vendor’s employees who have been granted access to the vendor contact to review appropriateness of employee access. Vendors are required to return the confirmation of access within two weeks. The director follows up on any access lists not returned.

Example Cloud Service Organization requires employees to adhere to a clean desk policy. As part of security patrols, guards record any violations of the clean desk policy in a log book. Log entries are entered into the event management system for review and follow-up by the director of physical security.

E. Logical Security

Organizational Structure

Example Cloud Service Organization has implemented an information security management program (ISMP) headed by the Chief Information Security Officer (CISO) under the direction of the Security Council. The Security Council is comprised of the Chief Operating Officer, the Chief Financial Officer, and CISO, and is chaired by the Chief Technology Officer (CTO). The council establishes and reviews the security strategy and approves RM plans, security policies, Information Security Group (ISG) organizational structure, and security communication plans. The council also reviews and approves changes to the system development methodology as it relates to system security and availability and publishes a quarterly security newsletter that is communicated to all employees.

The ISG is comprised of the following functional units:

- Security architecture
- Security implementation and change management
- Security operations and monitoring
- Security help desk
- Physical security

Each unit is headed by a manager who reports directly to the CISO.

ISG personnel are active in various security organizations and are encouraged to spend at least 40 hours per year in organization activities. Employees are expected to participate in 40 hours of continuing education in approved security classes.

Security Policy

Security policies are communicated in the Example Cloud Service Organization Security Policies Manual, which is available to all employees on the Example Cloud Service Organization intranet. In addition, all vendors and vendor personnel with access to the Example Cloud Service Organization system receive a copy of the Manual on an annual basis. The Manual is reviewed and updated by the CISO annually and is approved by the Security Council. The Manual includes the following elements:

- Chief Executive Officer's Statement on security practices
- Organization and responsibility of the Security Council
- Organizational structure of the ISG
- ISG roles and responsibilities
- Link to ISG job descriptions
- Link to the Example Cloud Service Organization Code of Conduct
- Acceptable-Use Policy
- Disciplinary and Sanctions Policy
- Mobile Device Policy
- Encryption Policy
- Network Access/Configuration Policy
- Password Policy
- Patch Management Policy
- Enterprise Security Policy
- Data Classification Policy
- Internet DMZ Equipment Policy
- Media Destruction Policy

- Remote Access/VPN Policy
- Router Security Policy
- Server Security Policy
- Software Policy
- User Account Policy
- Wireless Communication Policy
- Vendor employee security responsibilities
- Client-employee security responsibilities

Upon hire/initial grant of access, and each January thereafter, employees and vendors are required to complete a web-based security awareness training program. Training must be completed by the end of January. Completion is tracked by HR for employees and by the contractor office for vendor employees. In addition, as part of this process, employees and vendors with access to the Example Cloud Service Organization system are required to confirm that they have read the Security Policies Manual and accept responsibility for complying with it.
Client-employee responsibilities are communicated in the master services agreement and are available through a link on the sign-on page.

Security Architecture

Example Cloud Service Organization uses role-based security architecture and requires users of the system to be identified and authenticated prior to the use of any system resources. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles in access control lists. In situations in which incompatible responsibilities cannot be segregated, Example Cloud Service Organization implements monitoring of one or more of the responsibilities. Monitoring must be performed by a superior without responsibility for performing the conflicting activities or by personnel from a separate department.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Defined configuration standards exist for each hardware platform and each software system. The standards are developed by a security architect and are updated on an as-needed basis (at least annually). Standards are reviewed and approved by the lead security architect and lead system architect prior to implementation. Changes are classified as (1) emergency deployment, meaning that they must be deployed on all production elements within a defined number of weeks, (2) standard deployment, which must be deployed on all production elements within a defined number of months, and (3) deploy on rebuild, which is classified as being deployed only when other changes are made to the system configuration. Development servers are updated on a standard deployment or on a rebuild basis. Configuration standards include the use of locking screen savers on all work stations.

User Identification and Authentication

Employees and approved vendor personnel sign on to the Example Cloud Service Organization network using an Active Directory user ID and password. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality of Active Directory. Passwords must conform to defined password standards and are enforced through parameter settings in the Active Directory. These settings are part of the configuration standards and force users to change passwords at a defined interval, disable the user ID's ability to access the system and components after a specified number of unsuccessful access attempts, and mask workstation screens, requiring reentry of the user ID and password after a period of inactivity.

Employees accessing the system from outside the Example Cloud Service Organization network are required to use a token-based two-factor authentication system. Employees are issued tokens upon employment and must return the token during their exit interview. Vendor personnel are not permitted to access the system from outside the Example Cloud Service Organization network.

Customer employees access cloud services through the Internet using the SSL functionality of their web-browser. These customer employees must supply a valid user ID and password to gain access to customer cloud resources. Passwords must conform to password configuration requirements configured on the virtual devices using the virtual server administration account. Virtual devices are initially configured in accordance with Example Cloud Service Organization's configuration standards, but these configuration parameters may be changed by the virtual server administration account.

Customer employees may sign on to their systems using virtual server administration accounts. These administration accounts use a two-factor digital certificate-based authentication system.

Access Provisioning/De-provisioning

Upon hire, employees are assigned to a position in the HR management system. Two days prior to the employees' start date, the HR management system creates a report of employee user IDs to be created and access to be granted. The report is used by the security help desk to create user IDs and access rules. Access rules have been pre-defined based on the defined roles. The system lists also include employees with position changes and the associated roles to be changed within the access rules.

On an annual basis, access rules for each role are reviewed by a working group composed of security help desk, data center, customer service, and HR personnel. In evaluating role access, group members consider job description, duties requiring segregation, and risks associated with access. Completed rules are reviewed and approved by the CISO. As part of this process, the CISO reviews access by privileged roles and requests modifications based on this review.

Managers may request changes to role access rules through the event management system. Managers document the business purpose of the change, risks associated with the change, and consideration of segregation of duties. Access is approved by a data center manager. Upon approval, the security help desk enters the rule change.

Managers may also request a temporary access rule for an individual user for a period of time up to six months. Approved requests are submitted through the event management system to the security help desk, which enters the rule for the specified period of time.

Access by vendor employees is requested through the temporary access rule system, and access may be granted for periods up to 12 months. Vendor personnel access must be reviewed and approved by the contracting office personnel prior to processing by the security help desk.

Customer virtual server administration accounts are created by the security help desk upon contracting. Customers identify the number of administration accounts needed and the contact information for the primary customer administrator. The contact provides the Example Cloud Service Organization security help desk with the names and contact information of the individuals having administration accounts. User IDs are distributed to the contact via telephone, certificates are distributed by ground delivery on USB drives, and passwords are communicated directly to each administration account user via telephone.

Accounts are forced to change passwords upon initial sign-on.

Virtual server administration accounts are unique to each client environment in order to give the client access to all of their resources while preventing them from accessing other clients' resources.

The HR system generates a list of terminated employees on a daily basis. This daily report is used by the security help desk to delete employee access. On an annual basis, HR runs a list of active employees. The security help desk uses this list to suspend user IDs and delete all access roles from IDs belonging to terminated employees.

Customers are responsible for requesting deletion of virtual server administration accounts when Customer employees are terminated or change responsibilities.

Vendors are responsible for informing the contracting department when employees are no longer assigned to serve Example Cloud Service Organization. The contracting department also reviews access by a vendor's employees when a request for access by a new vendor employee is received.

On a quarterly basis, managers review roles assigned to their direct reports. Role lists are generated by security and distributed to the managers via the event management system. Managers review the lists and indicate the required changes in the event management record. The record is routed back to the security help desk for processing. The security help desk manager identifies any records not returned within two weeks and follows up with the manager. As part of this process, the CISO reviews employees with access to privileged roles and requests modifications through the event management system.

On a semi-annual basis, the contracting department sends a list of each vendor's employees who have been granted system access to the vendor contact to review appropriateness of employee access. Vendors are required to return the confirmation of access within two weeks. The contracting department follows up on any access lists not returned and submits received changes to the security help desk for entry.

Encryption of Communication Outside the Boundaries

Authorized employees may access the system from the Internet through the use of a leading VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system.

Vendors are not granted access from the Internet.

Customers may interact with their virtual environments through a secure session manager. Customers are responsible for maintaining access to individual virtual assets within their virtual environment. Customers are also responsible for implementing encryption solutions for each virtual server based on their individual risk assessments.

Example Cloud Service Organization uses Certificate Co., a certificate authority, to provide digital certificates used to support encrypted communication.

F. Monitoring

Vulnerability Scanning and Monitoring

Example Cloud Service Organization uses a third party vendor (TPV) to perform quarterly security vulnerability assessment and penetration testing services on its infrastructure and software. A variety of technologies, tools, and techniques are employed by the TPV to provide broad coverage against various types of threats.

The TPV's services are managed by the CISO and the security architect, who meet with the TPV and the Director of IT Internal Audit prior to the start of quarterly testing for planning purposes. As part of this meeting, Example Cloud Service Organization provides the TPV with a current list of infrastructure and software generated by the asset management system. This information is used in planning penetration and vulnerability testing. Weekly status meeting are held between the security architect and TPV personnel to monitor the status of the testing and preliminary findings identified.

A closing meeting is held at the conclusion of testing to formally review the results of testing and remediation plans. This meeting is attended by the CIO, CISO, security architect, and all CIO and CISO direct reports. The Director of IT Internal Audit also observes the meeting and prepares a report summarizing the meeting and the test results for presentation to the audit committee.

TPV personnel and testing tools are granted access only for the period during which testing is performed and are removed upon completion of testing. Logical access is restricted to access needed to perform the functions, and all use of the access is logged.

Assessments

- **Penetration Testing.** Penetration testing is conducted to measure the security posture of a target system or environment. The TPV uses an accepted industry standard penetration testing methodology specified by Example Cloud Service Organization. The TPV's approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the TPV attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. Penetration testing includes network and application layer testing as well as testing of controls and processes around the networks and applications, and occurs from both outside (external testing) and inside the network.

- **Vulnerability Scans**. Vulnerability scanning is performed by a TPV on a quarterly basis in accordance with Example Cloud Service Organization policy. The TPV uses industry standard scanning technologies and a formal methodology specified by Example Cloud Service Organization. These technologies are customized to test Example Cloud Service Organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as-needed basis. Scans are performed during non-peak windows. Tools requiring installation in the Example Cloud Service Organization system are implemented through the Change Management process. Scanning is performed with approved scanning templates and with bandwidth-throttling options enabled.

Testing Results

The TPV quarterly reports specify identified vulnerabilities, a level of assessed risk for each vulnerability identified, and suggested remediation. The report includes an executive summary and client summary, which is available to Example Cloud Service Organization customers upon request.

Individual vulnerabilities identified during penetration and vulnerability testing are logged to the event management software and managed through the incident management process.

In addition to the quarterly testing, continuous monitoring tools are in place. Refer to Incident Management above (not included for brevity).

Availability Monitoring

A formal data center operations assessment is performed monthly during the data center staff meeting. As part of this staff meeting, led by the VP of Operations, system availability is reviewed. Data regarding availability-related incidents is generated from the event management system. An analysis of device outages, availability events, and capacity utilization is prepared by the third shift operations manager. This report is reviewed at the staff meeting. Based on the review, additional incident tickets or change management tickets may be created to address trends and patterns identified.

IT personnel review and monitor industry-appropriate technological and regulatory changes via webcasts, seminars, and printed media.

G. Relationship between CCM Criteria, Description Sections, and Trust Services Criteria:

The description sections and the trust services principles and criteria address the CCM as follows (this example mapping represents one approach to providing this information):

CCM Area (based on version 1.4)	Relevant Description Section	Trust Services Criteria
1. Compliance		
2. Data Governance		
3. Facility Security		
4. Human Resources Security		
5. Information Security		
6. Legal		
7. Operations Management		
8. Risk Management		
9. Release Management		
10. Resiliency		
11. Security Architecture		

Partial Mapping
Limited for Brevity

An alternative approach may be to map the controls into three areas:

1. A mapping of the trust services principles and criteria to the Service Organization's controls
2. A mapping of the CCM to the Service Organization's controls
3. A listing of the Service Organization's controls with test descriptions

Note to Readers:

The source of the criteria used in this document is

1. *the 2009 version of the AICPA* Trust Services Principles, Criteria and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy (TSP Section 100A)*; and*

2. *Version 1.4 of the Cloud Controls Matrix.*

Although the applicable trust services criteria and related controls are presented in this section, they are, nevertheless, an integral part of Example Cloud Service Organization's description of its infrastructure services system throughout the period January 31, 20X1, to December 31, 20X1. This type 2 SOC 2 report is for illustrative purposes only and is not meant to be prescriptive. Example Cloud Service Organization'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.

Security and Availability Principles and Criteria

The system is protected against unauthorized access (both physical and logical). The system is available for operation and use as committed or agreed.

1.0 Policies				
Source: Trust Services Principles and Criteria for Security (S) and Availability (A) ***S1.1 The entity's security policies are established and periodically reviewed and approved by a designated individual or group.*** ***A1.1 The entity's system availability and related security policies are established and periodically reviewed and approved by a designated individual or group.***				
CCM ID	***CCM Criteria[4]***	***Description of Example Cloud Service Organization's Controls***	***Tests of Controls***	***Results of Tests***
IS-03	Management shall approve a formal Information Security Policy document which shall be communicated and published to employees, contractors and other relevant external parties. The Information Security Policy shall establish the direction of the organization and align to best practices, regulatory, federal/state and international laws where applicable. The Information Security Policy shall be supported by a strategic plan and a security program with well-defined roles and responsibilities for leadership and officer roles.	**Content** The Information Security Policy is reviewed by xxx to ensure it includes • strategic plan considerations, • applicable laws for the respective territories, and • roles and responsibilities for leadership and officers. **Updates** Responsibility for and maintenance of the Information Security Policy is assigned to the director of information security under the direction of the chief technology officer (CTO). The Information Security Policy is updated at least annually. **Communication** Example Cloud Service Organization publishes and communicates the Information Security Policy to employees, contractors, and external parties at least annually.	Inspected the Information Security Policy dated XX/XX/XXXX and noted that it included • strategic plan considerations, • applicable laws for the respective territories, • roles and responsibilities for leadership and officers, and • evidence of review of the update which occurred within the last year. Obtained evidence of the Information Security Policy being communicated to all employees, contractors and vendors via annual written communications and confirmation with each respective party	No exceptions noted.

1.0 Policies

[4] CCM Criteria are control specifications set forth in CCM version 1.4.

1.0 Policies

S1.2 The entity's security policies include, but may not be limited to, the following matters:

- ***a. Identifying and documenting the security requirements of authorized users***
- ***b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements***
- ***c. Assessing risks on a periodic basis***
- ***d. Preventing unauthorized access***
- ***e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access***
- ***f. Assigning responsibility and accountability for system security***
- ***g. Assigning responsibility and accountability for system changes and maintenance***
- ***h. Testing, evaluating, and authorizing system components before implementation***
- ***i. Addressing how complaints and requests relating to security issues are resolved***
- ***j. Identifying and mitigating security breaches and other incidents***
- ***k. Providing for training and other resources to support its system security policies***
- ***l. Providing for the handling of exceptions and situations not specifically addressed in its system security policies***
- ***m. Providing for the identification of and consistency with applicable laws and regulations, defined commitments, service level agreements, and other contractual requirements***
- ***n. Providing for sharing information with third parties.***

A1.2 The entity's system availability and related security policies include, but may not be limited to, the following matters:

- ***a. Identifying and documenting the system availability and related security requirements of authorized users***
- ***b. Classifying data based on its criticality and sensitivity and that classification is used to define protection requirements, access rights and access restrictions, and retention and destruction requirements***
- ***c. Assessing risks on a periodic basis***
- ***d. Preventing unauthorized access***
- ***e. Adding new users, modifying the access levels of existing users, and removing users who no longer need access***
- ***f. Assigning responsibility and accountability for system availability and related security***
- ***g. Assigning responsibility and accountability for system changes and maintenance***
- ***h. Testing, evaluating, and authorizing system components before implementation***
- ***i. Addressing how complaints and requests relating to system availability and related security issues are resolved***
- ***j. Identifying and mitigating system availability and related security breaches and other incidents***
- ***k. Providing for training and other resources to support its system availability and related security policies***
- ***l. Providing for the handling of exceptions and situations not specifically addressed in its system availability and related security policies***
- ***m. Providing for the identification of and consistency with, applicable laws and regulations, defined commitments, service-level agreements, and other contractual requirements***
- ***n. Recovering and continuing service in accordance with documented customer commitments or other agreements***
- ***o. Monitoring system capacity to achieve customer commitments or other agreements regarding availability.***

CCM ID	***CCM Criteria***	***Description of Example Cloud Service Organization's Controls***	***Tests of Controls***	***Results of Tests***

1.0 Policies				
IS-01	An Information Security Management Program (ISMP) has been developed, documented, approved, and implemented that includes administrative, technical, and physical safeguards to protect assets and data from loss, misuse, unauthorized access, disclosure, alteration, and destruction. The security program should address, but not be limited to, the following areas insofar as they relate to the characteristics of the business: 1. Risk management 2. Security policy 3. Organization of information security 4. Asset management 5. Human resources security 6. Physical and environmental security 7. Communications and operations management 8. Access control 9. Information systems acquisition, development, and maintenance	The written ISMP includes the following elements: 1. Chief Executive Officer's Statement on security practices 2. Organization and responsibility of the Security Council 3. Organizational structure of the ISG 4. ISG roles and responsibilities 5. Link to ISG job descriptions 6. Link to the Example Cloud Service Organization Code of Conduct 7. Acceptable-Use Policy 8. Disciplinary and Sanctions Policy 9. Mobile Device Policy 10. Encryption Policy 11. Network Access/Configuration Policy 12. Password Policy 13. Patch Management Policy 14. Enterprise Security Policy 15. Data Classification Policy 16. Internet DMZ Equipment Policy 17. Media Destruction Policy 18. Remote Access/VPN Policy 19. Router Security Policy 20. Server Security Policy 21. Software Policy 22. User Account Policy 23. Wireless Communication Policy 24. Vendor employee security responsibilities 25. Client and client employee security responsibilities	Verified through inspection that the written ISMP, dated XX/XX/XXXX, includes 1. the 25 matters listed in the second column, 2. the 9 areas identified in the first column, and 3. approval. Inspected the User Access policy dated XX/XX/XXXX and noted that it included • linkage to procedures for granting,	No exceptions noted. No exceptions

1.0 Policies				
		Content The written User Access Policy is reviewed to ensure it includes • linkage to procedures for granting, changing, and terminating access to applications, databases, servers, and network infrastructure, and • directions for meeting requirements in particular user entity service level agreements (SLAs). **Updates** Responsibility and maintenance of the User Access Policy is assigned to the Director of Information Security under the direction of the CTO. The User Access Policy is updated at least annually. **Communication** Example Cloud Service Organization has published the User Access Policy and communicated it to employees, contractors, and external parties at least annually.	changing, and terminating accesses to applications, databases, servers, and network infrastructure, • directions for meeting requirements in particular user entity SLAs, and • approval.	noted.

1.0 Policies				
S1.3	***Responsibility and accountability for developing and maintaining the entity's system security policies, and changes and updates to those policies, are assigned.***			
A1.3	***Responsibility and accountability for developing and maintaining the entity's system availability and related security policies, and changes and updates to those policies, are assigned.***			
	CCM Criteria	***Description of Example Cloud Service Organization Controls***	***Tests of Controls***	***Results of Tests***
IS-05	Management shall review the Information Security Policy at planned intervals or as a result of changes to the organization to ensure its continuing effectiveness and accuracy.	See IS-03	See IS-03	

(Remainder of the report, including Section 5, omitted for brevity)