SoftLayer Technologies, Inc.
Infrastructure as a Service (IaaS)

Report on SoftLayer Technologies, Inc.'s Description of its Infrastructure as a Service (IaaS) System Relevant to Security and Availability

For the period May 1, 2018 to April 30, 2019

Prepared in Accordance with:
AT-C 205 pursuant to *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*

Table of Contents

Section **Page**

Report of Independent Accountants

To the Management of SoftLayer Technologies, Inc.

Scope

We have examined SoftLayer Technologies, Inc.'s accompanying assertion titled "SoftLayer Technologies, Inc. Assertion" (assertion) that the controls within SoftLayer Technologies, Inc.'s Infrastructure as a Service (IaaS) system (system) were effective throughout the period May 1, 2018 to April 30, 2019, to provide reasonable assurance that SoftLayer Technologies, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

SoftLayer Technologies, Inc. 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 SoftLayer Technologies, Inc.'s service commitments and system requirements were achieved. SoftLayer Technologies, Inc. has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, SoftLayer Technologies, Inc. is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that controls were not effective to achieve SoftLayer Technologies, Inc.'s service commitments and system requirements based on the applicable trust services criteria

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve SoftLayer Technologies, Inc.'s service commitments and system requirements based the applicable trust services criteria

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within SoftLayer Technologies, Inc.'s IaaS system were effective throughout the period May 1, 2018 to April 30, 2019, to provide reasonable assurance that SoftLayer Technologies, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

PricewaterhouseCoopers LLP

July 12, 2019

SoftLayer Technologies, Inc.
14001 North Dallas Parkway,
Suite M100
Dallas, Texas 75240

SoftLayer Technologies, Inc.'s Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within SoftLayer Technologies, Inc.'s Infrastructure as a Service (IaaS) system (system) throughout the period May 1, 2018, to April 30, 2019, to provide reasonable assurance that SoftLayer Technologies, Inc.'s service commitments and system requirements relevant to security and availability were achieved. Our description of the boundaries of the system is presented in Attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period May 1, 2018, to April 30, 2019, to provide reasonable assurance that SoftLayer Technologies, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) and included as Attachment C. SoftLayer Technologies, Inc.'s objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period May 1, 2018 to April 30, 2019, to provide reasonable assurance that SoftLayer Technologies, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A - Description of SoftLayer Technologies, Inc.'s Infrastructure as a Service (IaaS) System

A. System Overview

Background

SoftLayer Technologies, Inc., also referred to as "IBM Cloud IaaS", "IBM SoftLayer," "SoftLayer," or "Bluemix IaaS," an IBM Company, provides on-demand cloud infrastructure as a service (IaaS) to its customers, allowing them to create scalable bare metal server, virtual server, or hybrid computing environments, via SoftLayer's Customer Portal, leveraging global data centers and points of presence (PoP).

SoftLayer's IaaS is built using a Network-Within-A-Network topology that provides remote access to allow customers the ability to build and manage computing environments remotely. SoftLayer's "Network-Within-A-Network" configuration includes three (3) network interfaces. Public, private, and management traffic travel across separate network interfaces, segregating and securing traffic while streamlining management functions.

- Public Network - Network traffic from anywhere in the world will connect to the closest network PoP, and it will travel directly across the network to its data center, minimizing the number of network hops and handoffs between providers.

- Private Network - Provides a connection to the customer's servers (bare metal or virtual) in SoftLayer data centers around the world. Data can be moved between servers through the private network; and customers can utilize various services, update and patch servers, software repositories, and backend services, without interfering with public network traffic.

- Management Network - Each server within the SoftLayer IaaS is connected to the management network. This out-of-band management network, accessible via VPN, allows access to each server for maintenance and administration, independent of its CPU and regardless of its firmware or operating system.

SoftLayer delivers its IaaS through the Internal Management System (IMS), which is an internally developed customer relationship management (CRM) system used to track customers' hardware and services. IMS allows customers to manage their cloud environments. Customer capabilities include management of system and network devices provisioned by the customer, account management, ordering and deployment, and customer support.

IMS has two components: IMS, as viewed by internal employees, and the Customer Portal, as available to users of SoftLayer's IaaS. The Customer Portal allows customers to:

- Create and manage tickets for incident response and resolution
- Review account information
- View information and certain configuration data regarding their purchased solutions

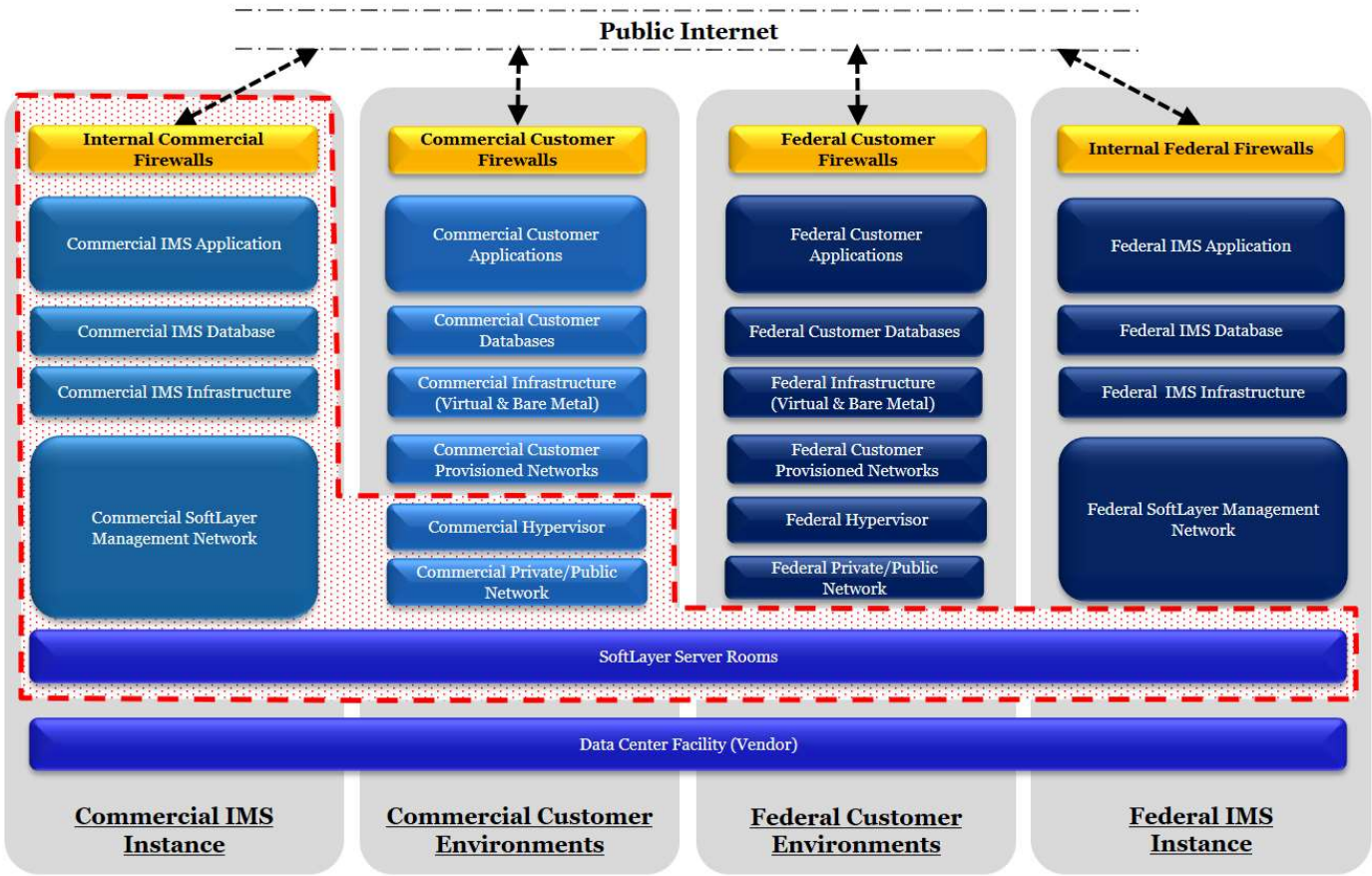
- Perform functions such as OS reloads, and access RescueLayer
- Maintain customer provisioned firewall and DNS configurations that affect their bare metal servers
- Purchase or upgrade services to initiate the automated provisioning process for new systems

Customers build their environments using virtual servers and/or bare metal servers.

- Virtual servers are computing "instances" that are complete computing environments that include a full hardware and software stack accessed and controlled over the Internet. The computing resources can be scaled on demand, adding or resizing instances as needed, but without having to purchase physical systems. Public and private virtual nodes are available.
- Bare metal servers are dedicated physical servers. Bare metal servers allow direct access to physical hardware to support high demand and processor-intensive workloads.

SoftLayer personnel also have access to IMS to set up and configure purchased solutions, assist in troubleshooting technical issues, and respond to customer requests.

Boundaries of the System



This report covers the services managed by SoftLayer, including global data center physical locations, the IMS portal and the supporting infrastructure devices. Additionally, this report includes network devices that are managed by SoftLayer supporting the IMS portal and infrastructure including hypervisors, and network devices that support customer environments but are not provisioned/managed by customers within the SoftLayer IaaS. The report includes supporting services to the virtual and bare metal services, such as storage. These devices can be locally attached, accessible by API (such as Public Cloud Object Store), or accessible via a storage area network. Cloud Object Storage is an IaaS service with devices locally attached, residing in the SoftLayer control row. The SoftLayer IMS system provides the underpinning for user and

storage instance provisioning. The Cloud Object Storage Bluemix provisioning path including the COS Broker are not included within the IaaS system boundary.

The Storage Area Network (SAN) is architecture to attach remote computer storage devices to servers in such a way that, to the operating system, the devices appear as locally attached. Within each customer environment, servers, VMs and other systems/devices are managed by SoftLayer's customers and are not included within the boundaries of the system. This report does not extend to the workloads (data, files, information) sent by SoftLayer IaaS customers to the SoftLayer IaaS system. The integrity and conformity with regulatory requirements of such data are solely the responsibility of the applicable SoftLayer IaaS customer. Additionally, this report does not extend to business process controls, automated application controls, or key reports.

SoftLayer provides services to the Federal government and Department of Defense (DoD) via the FedRAMP and Defense Information Systems Agency (DISA)/DoD programs in two data centers (DAL08 and WDC03). A separate instance of IMS (FedIMS) provides provisioning functionality and infrastructure management. These data center facilities are included within the physical security boundaries of the system. However, other aspects of the services including the FedIMS system and its processes, are not included within the boundaries of the system.

The accompanying description includes only those controls directly impacting SoftLayer's IaaS and customers' hosting environments utilizing SoftLayer's IaaS, and does not include controls over other services. SoftLayer also provides enterprise-class tools to help mitigate potential security risks and ensure availability. Tools provided by SoftLayer include, but are not limited to, load balancing, intrusion detection and prevention, standard and dedicated hardware firewalls, anti-virus, anti-spyware, anti-malware, VeriSign® and GeoTrust® SSL Certificates. This report does not extend to controls over SoftLayer's other services and tools.

Components, infrastructure, network devices, software, and data center locations within the scope of the system:

<table>
<tr><th>Service Offering</th><th>Data Center / Hardware Locations</th><th>Network</th><th>Operating System Infrastructure</th><th>System Software</th><th>Applications</th><th>Customer Data</th></tr>
<tr><td rowspan="3">IBM SoftLayer

IaaS</td><td rowspan="3">43 data centers

(See Infrastructure section below)</td><td>Customer provisioned and managed network devices, firewalls and VPNs are solely the responsibility of the customer and are not within the boundaries of the system.</td><td colspan="3" rowspan="2">Customer environments (including the development and maintenance) provisioned and managed using the Customer Portal, including OS, system software, and applications are solely the responsibility of the customer and are not within the boundaries of the system.</td><td rowspan="3">Customer data is solely the responsibility of the customer and is not within the boundaries of the system.</td></tr>
<tr><td>Network devices supporting customer managed environments and managed by SoftLayer are within boundaries of the system including:

Routers, Switches, Firewalls, VPNs</td></tr>
<tr><td>Network devices directly in support of the IMS portal are within the boundaries of the system including:

Routers, Switches, Firewalls, VPNs</td><td>Operating systems directly in support of the IMS portal are within boundaries of the system including:

Linux, UNIX, Windows, CentOS</td><td>System software directly in support of the IMS portal are within boundaries of the system including:

Radius, Citrix, Active Directory</td><td>Internal Management System (IMS)/ Customer Portal</td></tr>
</table>

B. System Components

Infrastructure

SoftLayer provides Infrastructure as a Service (IaaS) using multiple telecom service providers for backbone connectivity and multiple co-location management providers for data center facility management. Refer to the table below for a list of data center vendors that provide facility management services in the SoftLayer facilities included within the scope of this report.

Facility *	Physical Location	Facility Manager
AMS01	Amsterdam, Netherlands	Digital Realty
AMS03	Almere, Netherlands	KPN
CHE01	Chennai, India	TATA
DAL01	Dallas, TX	Flexential
DAL02	Dallas, TX	SoftLayer
DAL05	Dallas, TX	Digital Realty
DAL06	Dallas, TX	SoftLayer
DAL07	Plano, TX	SoftLayer
DAL08	Richardson, TX	Digital Realty
DAL09	Richardson, TX	Digital Realty
DAL10	Irving, TX	QTS
DAL12	Richardson, TX	Digital Realty
DAL13	Carrollton, TX	Cyrus One
FRA02	Frankfurt, Germany	Zenium Technology
FRA04	Frankfurt, Germany	E-Shelter
FRA05	Frankfurt, Germany	Interxion
HKG02	Hong Kong, China	Digital Realty
HOU02	Houston, TX	SoftLayer
LON02	Chessington, London	Digital Realty
LON04	Farnborough, UK	Ark Data Centres

Facility *	Physical Location	Facility Manager
LON06	Slough, UK	Zenium Technology
MEL01	Melbourne, Australia	Digital Realty
MEX01	Queretaro, Mexico	Alestra
MIL01	Milan, Italy	DATA4
MON01	Montreal, Canada	COLO-D
OSL01	Oslo, Norway	EVRY
PAR01	Paris, France	Global Switch
SAO01	Sao Paulo, Brazil	Ascenty
SEA01	Tukwila, WA	Internap
SEO01	South Korea	SK C&C
SJC01	Santa Clara, CA	Digital Realty
SJC03	Santa Clara, CA	Digital Realty
SJC04	Santa Clara, CA	Infomart
SNG01	Jurong East, Singapore	Digital Realty
SYD01	Sydney, Australia	Global Switch
SYD04	Erskine Park, Australia	Digital Realty
TOK02	Tokyo, Japan	@Tokyo
TOR01	Ontario (Markham), Canada	Digital Realty
WDC01	Chantilly, VA	Digital Realty
WDC03	Ashburn, VA	Digital Realty
WDC04	Ashburn, VA	Digital Realty
WDC06	Ashburn, VA	Raging Wire
WDC07	Ashburn, VA	Sabey

* Note: Only those data centers that were operational and hosting customer servers for at least six (6) months are considered in scope for this report.

Customers with bare metal, virtual, or hybrid environments can access the servers remotely (electronically) from anywhere in the world. Certain facilities (i.e., DAL02, DAL07 and HOU02) house both co-location servers and Infrastructure as a Service (IaaS) related servers. Co-location

customers do not have logical or physical access to the SoftLayer Infrastructure as a Service (IaaS) system. As such, co-location cages housing customers' servers are not included within the boundaries of the system.

Software

SoftLayer IaaS customers are solely responsible for customer owned and managed software and applications as these components are not within the boundaries of the system. SoftLayer IaaS does not maintain responsibility for customer software and applications that SoftLayer IaaS customers run on their bare metal, virtual, or hybrid environment; the software and applications are the responsibility of SoftLayer IaaS customers.

For components of the environment managed by SoftLayer IaaS, software systems are managed centrally by SoftLayer using consistent controls and processes. SoftLayer manages the Customer Portal (IMS), IMS infrastructure and operating systems, network devices supporting IMS and certain network devices supporting customer environments within the SoftLayer environment.

SoftLayer Managed Component	Software Managed
IMS Database	• Oracle
IMS Infrastructure	• Various Unix OS • Windows
Customer Portal / IMS	• Proprietary Software Developed by SoftLayer

In addition, SoftLayer manages certain shared network devices that support customer environments. RADIUS software is used to manage customer's network devices.

People

Key SoftLayer positions of authority and responsibility are documented in a formal organizational chart via IBM's BluePages, which evidences key organizational structures and reporting lines. The organizational chart is reviewed by HR and updated periodically for accuracy by managers.

Within the organization, roles and responsibilities are defined and communicated. SoftLayer leverages participation from multiple organizational levels, sites, locations, geographies and organizations are involved, as required, to perform the day-to-day oversight of service delivery related functions, matters, responsibilities and issues. Functional roles may be combined within management positions to deliver services in a cost effective manner.

The SoftLayer IaaS teams are diverse teams of development and operations professionals, which maintain and follow IBM's industry leading processes, standards and procedures in the execution of their work. Security and availability requirements are generated from senior

management. These requirements are distributed to the operational management leaders. These leaders are responsible for the implementation and monitoring of security controls.

The General Manager of Cloud Infrastructure Services oversees daily operations and reports to the Senior Vice President IBM Watson & Cloud Platform. Supporting the GM are Tribe Leaders, Directors and Vice Presidents that manage and perform the daily operations of SoftLayer. These core competencies have been established to provide full capabilities to serve customers worldwide. Functional and administrative responsibilities are broadly defined and communicated through organizational charts, which are reviewed and updated regularly.

Procedures

Customers are provided and required to agree to a Cloud Service Agreement (CSA) during the ordering process. The CSA acts as the formal contract and usage policy for customer users of the SoftLayer IaaS system. The CSA documents the contractual obligations of SoftLayer and the customers using SoftLayer IaaS. Any updates to the CSA are communicated to the existing customers through the Customer Portal. Additionally, SoftLayer Technologies, Inc. posts its system description that reflects the boundaries of the IaaS system online for customers and prospective customers.

The policies and procedures are a series of documents, which are used to describe the controls implemented within the SoftLayer IaaS system. The purpose of the policies and procedures is to describe the environment and define the practices performed on behalf of the customer. The policies and procedures include diagrams and descriptions of the network, infrastructure, environment and SoftLayer's commitments. These policies and procedures are available to all SoftLayer employees that support the SoftLayer IaaS system. Additionally, each of the policies and procedures are reviewed by SoftLayer management on a periodic basis, per the defined policy.

Data

The integrity and conformity with regulatory requirements of workloads sent to the SoftLayer IaaS system are solely the responsibility of SoftLayer IaaS customers. SoftLayer IaaS does not maintain responsibility for the data SoftLayer IaaS customers store on their bare metal, virtual, or hybrid environment. The data is the responsibility of SoftLayer IaaS customers.

Attachment B - Principal Service Commitments and System Requirements

Customers are provided and required to agree to a Cloud Service Agreement (CSA) during the ordering process. The CSA is available to customers through the Customer Portal and acts as the formal contract and usage policy for customer users of the SoftLayer IaaS system. The CSA documents the contractual obligations of SoftLayer and the customers using SoftLayer IaaS, including principle service commitments and system requirements. Any updates to the CSA are communicated to the existing customers through the Customer Portal.

Only the principle service commitments and system requirements relevant to the applicable trust services criteria are within the boundaries of the system. The relevant service commitments and system requirements are included within the following sections of the CSA:

- 1. Cloud Services
- 2. Content and Data Protection

  Included within c. of the section is a link to IBM's Data Security and Privacy Principles for IBM Cloudant Services (DSP). Relevant service commitments and system requirements are included within the following sections of the DSP:
  - 1. Data Protection
  - 2. Security Policies
  - 3. Security Incidents
  - 4. Physical Security and Entry Control
  - 5. Access, Intervention, Transfer and Separation Control
  - 6. Service Integrity and Availability Control
- 9. General

Principle service commitments and system requirements within the boundaries of the system are outlined further in the sections below.

Attachment C – AICPA Trust Services Criteria

This attachment includes the AICPA trust services criteria, included in the scope of the engagement, relevant to security and availability set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Criteria

Category	Criteria
CC 1.0 Control Environment	CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
	CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
	CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
	CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
	CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC2.0 Communication and Information	CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
	CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
	CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
CC3.0 Risk Assessment	CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
	CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.

Category	Criteria
	CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.
	CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.0 Monitoring Activities	CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
CC5.0 Control Activities	CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
	CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
	CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC6.0 Logical and Physical Access Controls	CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.

Category	Criteria
	CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
	CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
	CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
	CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
	CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.
CC7.0 System Operations	CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
	CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
	CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
	CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
	CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.

Category	Criteria
CC8.0 Change Management	CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
CC9.0 Risk Mitigation	CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
	CC9.2 The entity assesses and manages risks associated with vendors and business partners.
Additional Criteria for Availability	A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
	A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
	A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.