International Business Machines Corporation

IBM Cloud Infrastructure as a Service (IaaS)

Report on International Business Machines Corporation's IBM Cloud Infrastructure as a Service (IaaS) System Relevant to Security and Availability

For the period May 1, 2023 to April 30, 2024

Table of Contents

Section **Page**

Report of Independent Service Auditors

To the Management of International Business Machines Corporation

Scope

We have examined International Business Machines Corporation's accompanying assertion titled "Management of International Business Machines Corporation's Assertion" (the "assertion") that the controls within International Business Machines Corporation's IBM Cloud Infrastructure as a Service (IaaS) system (the "system") were effective throughout the period May 1, 2023, to April 30, 2024, to provide reasonable assurance that International Business Machines Corporation'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, in AICPA Trust Services Criteria.

Service Organization's Responsibilities

International Business Machines Corporation 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 International Business Machines Corporation's service commitments and system requirements were achieved. International Business Machines Corporation has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, International Business Machines Corporation is responsible for selecting, and identifying in its assertion, the applicable trust services 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 AICPA. 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.

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

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 International Business Machines Corporation'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 International Business Machines Corporation's service commitments and system requirements based on 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 International Business Machines Corporation's IBM Cloud Infrastructure as a Service (IaaS) system were effective throughout the period May 1, 2023, to April 30, 2024, to provide reasonable assurance that International Business Machines Corporation's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

PricewaterhouseCoopers LLP

June 21, 2024

International Business Machines Corporation
14001 North Dallas Parkway,
Suite M100
Dallas, Texas 75240

Management of International Business Machines Corporation's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within International Business Machines Corporation's IBM Cloud Infrastructure as a Service (IaaS) system (the "system") throughout the period May 1, 2023, to April 30, 2024, to provide reasonable assurance that International Business Machines Corporation'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*, in AICPA Trust Services Criteria and included as Attachment C. 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, 2023, to April 30, 2024, to provide reasonable assurance that International Business Machines Corporation's service commitments and system requirements were achieved based on the applicable trust services criteria. International Business Machines Corporation'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, 2023, to April 30, 2024, to provide reasonable assurance that International Business Machines Corporation's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A - International Business Machines Corporation's Description of its IBM Cloud Infrastructure as a Service (IaaS) System

A. System Overview

Background

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

IBM Cloud 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. IBM Cloud IaaS'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 IBM Cloud IaaS 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 IBM Cloud 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.

The following products and services are delivered within the IBM Cloud IaaS system boundaries:

- Networking: IBM Cloud Load Balancer, IBM Cloud Direct Link "1.0", Hardware Firewall, Gateway Appliance, IPSec VPN, Fortigate Security Appliance
- Storage: IBM Cloud File Storage, IBM Cloud Block Storage, IBM Cloud Backup, IBM Cloud Object Storage (IaaS), Storage Area Network (SAN)
- Compute: IBM Cloud Bare Metal, IBM Cloud Hardware Security Module, SAP-Certified Cloud Infrastructure, IBM Cloud Virtual Servers

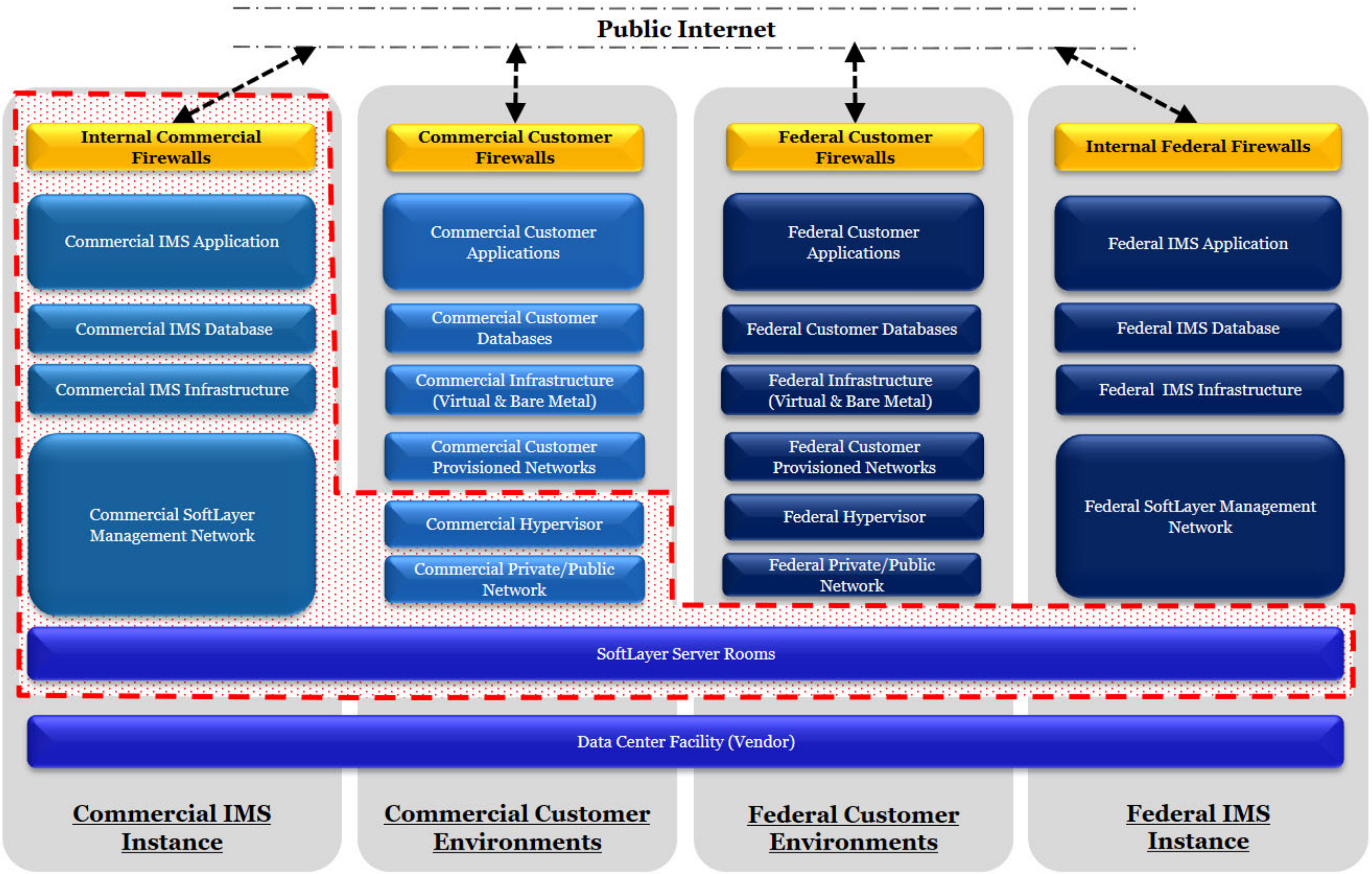
IBM Cloud IaaS delivers its products and services through the Internal Management System (IMS), which is an internally developed customer relationship management (CRM) system used to track customers' hardware and services. IMS allows customers to manage their cloud environments. Customer capabilities 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 IBM Cloud 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

IBM Cloud IaaS 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


Public Internet
Internal Commercial Firewalls
Commercial IMS Application
Commercial IMS Database
Commercial IMS Infrastructure
Commercial SoftLayer Management Network
Commercial Customer Firewalls
Commercial Customer Applications
Commercial Customer Databases
Commercial Infrastructure (Virtual & Bare Metal)
Commercial Customer Provisioned Networks
Commercial Hypervisor
Commercial Private/Public Network
Federal Customer Firewalls
Federal Customer Applications
Federal Customer Databases
Federal Infrastructure (Virtual & Bare Metal)
Federal Customer Provisioned Networks
Federal Hypervisor
Federal Private/Public Network
Internal Federal Firewalls
Federal IMS Application
Federal IMS Database
Federal IMS Infrastructure
Federal SoftLayer Management Network
SoftLayer Server Rooms
Data Center Facility (Vendor)
Commercial IMS Instance
Commercial Customer Environments
Federal Customer Environments
Federal IMS Instance

Note: Area within the dashed line is within the boundaries of the system.

The boundaries of the system covers the services managed by IBM Cloud IaaS, including global data center physical locations, the IMS portal and the supporting infrastructure devices. This also includes the network devices that are managed by IBM Cloud IaaS and infrastructure (including hypervisors) that support customer environments.

Customers are responsible within their commercial customer environment for management of the customer provisioned network devices, infrastructure (bare metal and virtual servers), databases, applications, and other systems/devices including the implementation, configuration, and maintenance of such, and are not included within the scope of this report.

The following products and services are delivered from within the IBM Cloud IaaS scope and are provisioned via IMS. Customers are responsible for the implementation, configuration, and maintenance within their environment.

Networking

- **IBM Cloud Load Balancer** enables customers to utilize public (internet facing) and private (internal) load balancing to distribute traffic between application servers deployed locally within an IBM Cloud data center.

- **IBM Cloud Direct Link "1.0"** enables customers to establish a point-to-point connection from their location to the cloud infrastructure terminating at IBM network points of presence (PoPs); it is delivered from within the security scope via a series of Layer 3 switches and routers (XCS/XCR/MBR/BCR/BAS/BCS). Customers are responsible for ordering their single mode fiber cross-connections and are responsible for the configuration of their routers. Customers are provided with an IP allocation for point-to-point connection configuration; additionally, they will be assigned a /24 (254 usable IPs) for their remote hosts.

- **Hardware Firewall** is a Fortigate device which allows customers to protect multiple VLANs using firewall rules, application control, anti-malware, and advanced inspection technologies.

- **Gateway Appliance** is a customer managed offering providing a selection of AT&T Vyatta 5600 vRouters or a Juniper vSRX device which allows the customer to manage their physical and virtual networks for VLAN routing, firewall and VPN management and traffic shaping.

- **IPSec VPN** is a service available to customers to facilitate management of their environment using an encrypted VPN tunnel.

- **Fortigate Security Appliance** is a customer managed, high throughput firewall that provides them with enhanced granular control over their networks.

Storage

- **IBM Cloud File Storage** is a flash-backed NFS-based file storage system that allows customers to increase storage capacity and adjust performance based on workload demands.

- **IBM Cloud Block Storage** is a persistent storage option available for Cloud Virtual and Bare Metal Servers.

- **IBM Cloud Backup** is a recovery system the customer manages, enabling customer to securely backup data between IBM servers in one or more IBM Cloud data centers.

- **IBM Cloud Object Storage (IaaS)** is a cross-regional, unstructured, scalable, and persistent data storage service designed to support exponential data growth.

- **Storage Area Network (SAN)** is architected to attach remote computer storage devices to servers in such a way that, to the operating system, the devices appear as locally attached.

Compute

- **IBM Cloud Bare Metal** is a dedicated physical server. Bare metal servers allow direct access to physical hardware to support high demand and processor-intensive workloads.

- **IBM Cloud Hardware Security Module** is a standalone appliance that provides dedicated single-tenant encryption and key management.

- **SAP-Certified Cloud Infrastructure** is a dedicated physical server purpose-built for SAP workloads.

- **IBM Cloud Virtual Servers** are computing "instances" that are a complete computing environment that includes 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.

This report does not extend to the workloads (data, files, information) sent by IBM Cloud IaaS customers to the IBM Cloud IaaS system. The integrity and conformity with regulatory requirements of such data are solely the responsibility of the applicable IBM Cloud IaaS customer. Additionally, the boundaries of the system do not extend to business process controls, automated application controls, or key reports.

IBM Cloud IaaS 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 IBM Cloud IaaS and customers' hosting environments utilizing IBM Cloud IaaS services detailed in this report. IBM Cloud IaaS also provides enterprise-class tools to help mitigate potential security risks and ensure availability. Tools provided by IBM Cloud IaaS 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 IBM Cloud IaaS's other services and tools.

Table 1: Components, infrastructure, network devices, software, and data center locations within the boundaries of the system:

Service Offering	**Data Center / Hardware Locations**	**Network**	**Operating System Infrastructure**	**System Software**	**Applications**	**Customer Data**
IBM Cloud IaaS	46 data centers (Refer to the Infrastructure section below)	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.	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.			Customer data is solely the responsibility of the customer and is not within the boundaries of the system.
		Network devices supporting customer managed environments and managed by IBM Cloud IaaS are within the boundaries of the system including: Routers, Switches, Firewalls, VPNs				
		Network devices directly in support of the IMS portal are within the boundaries of the system including: Routers, Switches, Firewalls, VPNs	Operating systems directly in support of the IMS portal are within the boundaries of the system including: Linux, UNIX, Windows	System software directly in support of the IMS portal are within the boundaries of the system including: Radius, Citrix, Active Directory	Internal Management System (IMS)/ Customer Portal	

B. System Components

Infrastructure

IBM Cloud IaaS provides infrastructure as a service 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 IBM Cloud IaaS facilities included within the boundaries of the system. Some services may vary depending on the facility.

Facility	Physical Location	Facility Manager
AMS03	Almere, Netherlands	NorthC
CHE01	Ambattur, India	STT
DAL05	Dallas, TX	Digital Realty
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	Cyrus One
FRA04	Frankfurt, Germany	E-Shelter
FRA05	Frankfurt, Germany	Interxion
LON02	Chessington, London	Digital Realty
LON04	Farnborough, UK	Ark Data Centres
LON05	Hemel Hempsted, UK	NTT
LON06	Slough, UK	Cyrus One
MAD02*	Madrid, Spain	DATA4
MAD04*	Madrid, Spain	NTT
MAD05*	Madrid, Spain	Digital Realty
MIL01	Milan, Italy	DATA4
MON01	Montreal, Canada	COLO-D
OSA2X	Osaka, Japan	IDC Frontier

Facility	Physical Location	Facility Manager
PAR01	Paris, France	Global Switch
PAR04	Paris, France	Global Switch
PAR05	Paris, France	BNPP
PAR06	Paris, France	BNPP
SAO01	Sao Paulo, Brazil	Ascenty
SAO04	Santana de Parnaíba, Brazil	Odata
SAO05	Sao Paulo, Brazil	Ascenty
SJC01	Santa Clara, CA	Digital Realty
SJC03	Santa Clara, CA	Digital Realty
SJC04	San Jose, CA	Stack Infrastructure
SNG01	Jurong East, Singapore	Digital Realty
SYD01	Sydney, Australia	Global Switch
SYD04	Erskine Park, Australia	Digital Realty
SYD05	Sydney, Australia	Equinix
TOK02	Tokyo, Japan	@Tokyo
TOK04	Saitama, Japan	Softbank
TOK05	Tokyo, Japan	NTT
TOR01	Ontario (Markham), Canada	Digital Realty
TOR04	Ontario, Canada	ServerFarm
TOR05	Ontario, 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

** MAD02, MAD04, and MAD05 DCs went live in 2023 and are inscope of this report of as 11/1/2024.*

Customers with bare metal, virtual, or hybrid environments can access the servers remotely (electronically) from anywhere in the world.

Software

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

For components of the environment managed by IBM Cloud IaaS, software systems are managed centrally by IBM Cloud IaaS using consistent controls and processes. IBM Cloud IaaS manages the Customer Portal (IMS), IMS infrastructure and operating systems, network devices supporting IMS and certain network devices supporting customer environments within the IBM Cloud IaaS environment. Additionally, IBM Cloud IaaS maintains a control for the inventory for their system components. The inventory asset management listing is documented, reviewed and approved on a periodic basis to ensure accuracy and completeness.

IBM Cloud IaaS Managed Component	Software Managed
IMS Database	• Oracle
IMS Infrastructure	• Various UNIX OS • Linux • Windows
Customer Portal / IMS	• Proprietary Software Developed by IBM Cloud IaaS
Shared network devices supporting customer environments	• RADIUS

People

Key security positions of authority and responsibility are documented in a formal organizational chart, which evidences key organizational structures and reporting lines. The organizational chart is reviewed and updated periodically for accuracy.

Within the organization, roles and responsibilities are defined and communicated. IBM Cloud leverages participation from multiple organizational levels, sites, locations, and 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 contracted services in a cost-effective manner. IBM Cloud may distribute some portion of its development and operations processes to IBM locations around the world, when permissible.

The IBM Cloud teams are comprised of diverse development and operations professionals, who maintain and follow IBM's 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 and availability controls.

Procedures

The IBM Cloud IaaS policies and procedures are a series of documents, which are used to describe the controls implemented within the 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 IBM's commitments. These policies and procedures are available to all IBM employees that support IBM Cloud IaaS. Additionally, each of the policies and procedures is reviewed by IBM management on a periodic basis, in accordance with the defined security policy.

Data

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

Attachment B - Principal Service Commitments and System Requirements

Customers are provided and required to agree to a Cloud Services Agreement (CSA) during the account creation 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 IBM Cloud IaaS system. The CSA documents the contractual obligations of IBM Cloud and the customers using IBM Cloud IaaS, including principal service commitments and system requirements. Any updates to the CSA are communicated to the existing customers through the customer portal.

Only the principal 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 CSA and DSP:

- Security and availability commitments to user entities are documented and communicated in contracts and customer agreements as well as in the description of the service offering that is available to customers
- Security and availability risk assessments of the IBM Cloud services are performed at least annually
- Monitoring controls are in place to provide oversight of controls and processes within the operation of the system
- Use of encryption technologies to protect customer data both at rest and in transit
- Security and availability categories within the fundamental design of the system are designed to permit system users least privileged access based on job responsibilities
- Physical access to facilities and restriction of protected information assets to authorized personnel
- Tone at the top, annual trainings and recertifications of skills development
- Monitoring controls are in place to assess, test, and apply security advisory patches to the IBM Cloud services and associated systems, networks, applications, and underlying components within the scope of services
- Policies and procedures are designed to manage risks associated with the application of changes
- A backup process is performed and available to allow restoration in the event of data loss or downtime

The relevant service commitments and system requirements are also included within the following sections of the CSA:

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

  Included within paragraph d. of the Content and Data Protection section is a link to IBM's Data Security and Privacy Principles for IBM Cloud Services (DSP). Relevant service commitments and system requirements are included within the following sections of the DSP:

  - Data Protection
  - Security Policies
  - Security Incidents
  - Physical Security and Entry Control
  - Access, Intervention, Transfer and Separation Control
  - Service Integrity and Availability Control
- 9. General

The CSA encompasses the full list of service commitments and system requirements delivered to IBM Cloud customers which may include services outside the scope of the report. As such, the CSA should be read in conjunction with the system boundaries and applicable trust services criteria. All other service commitments and system requirements described within the CSA are not in scope for this report.

Additional aspects of the system description that reflect the boundaries of the IBM Cloud IaaS system are posted online for customers and prospective customers.

Attachment C – AICPA Trust Services Criteria

This attachment includes the trust services criteria, included in the scope of the report, 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).*

Security and Availability Categories

- Security - Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability of information or systems and affect the entity's ability to meet its objectives.
- Availability - Information and systems are available for operation and use to meet the entity's objectives.

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.

Category	Criteria
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.
	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.

Category	Criteria
	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.
	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.

Category	Criteria
	CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.
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.