IBM Cloud
Public Cloud Platform for Wave 4 Service Offerings

Report on IBM Cloud's Public Cloud Platform System for Wave 4 Service Offerings Relevant to Security and Availability

For the period May 1, 2020 through October 31, 2020

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

Report of Independent Service Auditors

To the Management of IBM Cloud:

Scope

We have examined IBM Cloud's accompanying assertion titled "IBM Cloud's Assertion" (the "assertion") that the controls within IBM Cloud's Public Cloud Platform system for Wave 4 service offerings[1] (the "system") were effective throughout the period May 1, 2020 to October 31, 2020, to provide reasonable assurance that IBM Cloud'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

IBM Cloud 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 IBM Cloud's service commitments and system requirements were achieved. IBM Cloud has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, IBM Cloud 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

1 IBM Public Cloud Platform service offerings in scope of this report include: IBM Cloud Kubernetes Service, Red Hat OpenShift on IBM Cloud, IBM Cloud Container Registry, IBM Cloud Identity and Access Management (IAM), IBM Cloud Console, IBM Cloud App Service, IBM Cloud Certificate Manager, IBM Cloud Functions, IBM Cloud Continuous Delivery, and IBM Cloud Schematics.

- Assessing the risks that controls were not effective to achieve IBM Cloud'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 IBM Cloud'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 IBM Cloud's Public Cloud Platform system for Wave 4 service offerings were effective throughout the period May 1, 2020 to October 31, 2020, to provide reasonable assurance that IBM Cloud's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

PricewaterhouseCoopers LLP

December 23, 2020

International Business Machines Corporation
11501 Burnet RD
Austin, TX 78758-3400
United States

IBM Cloud's Assertion

We are responsible for designing, implementing, operating, and maintaining effective controls within IBM Cloud's Public Cloud Platform system for Wave 4 service offerings[1] (the "system") throughout the period May 1, 2020 to October 31, 2020, to provide reasonable assurance that IBM Cloud'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, 2020 to October 31, 2020, to provide reasonable assurance that IBM Cloud'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. IBM Cloud'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, 2020 to October 31, 2020, to provide reasonable assurance that IBM Cloud's service commitments and system requirements were achieved based on the applicable trust services criteria.

1 IBM Public Cloud Platform service offerings in scope of this report include: IBM Cloud Kubernetes Service, Red Hat OpenShift on IBM Cloud, IBM Cloud Container Registry, IBM Cloud Identity and Access Management (IAM), IBM Cloud Console, IBM Cloud App Service, IBM Cloud Certificate Manager, IBM Cloud Functions, IBM Cloud Continuous Delivery, and IBM Cloud Schematics.

Attachment A - Description of IBM Cloud's Public Cloud Platform System for Wave 4 Service Offerings

A. System Overview

Background

IBM Cloud is composed of a number of cloud and 'as a service' businesses that provide the underlying infrastructure for platform, database, and application/software-as-a-service solutions to IBM's customers. IBM Public Cloud Platform services use an IBM Cloud Kubernetes solution to enable customers to purchase, tailor, and use products included in a catalog of complementary service offerings (e.g., compute and development tools, analytics, security, AI, mobile services, etc.) that are hosted and managed by IBM service offering teams under a container-based architecture. Once purchased by a customer, the products are made available to the customer and should be tailored by the customer to meet their specific needs. All of the service offerings and devices are logically and/or physically separated from other customer information.

Boundaries of the System

This report includes the underlying server infrastructure, system software and network devices used to support IBM Cloud's Public Cloud Platform system. The boundaries do not include the data structures/schemas, applications and tools that customers use to load, analyze and manipulate data, as those are solely the responsibility of the customer.

Within each customer environment, servers, clusters, VMs and other systems/devices are managed by IBM Cloud's customers and are not included within the boundaries of the system. Additionally, this report does not extend to the workloads sent by customers to IBM Cloud. Customer applications and customer data are outside the scope of the system. The integrity and regulatory requirements of such data are solely the responsibility of the customer.

This report does not extend to business process controls, automated application controls, or key reports.

Diagram 1: IBM Cloud services within the scope of this report

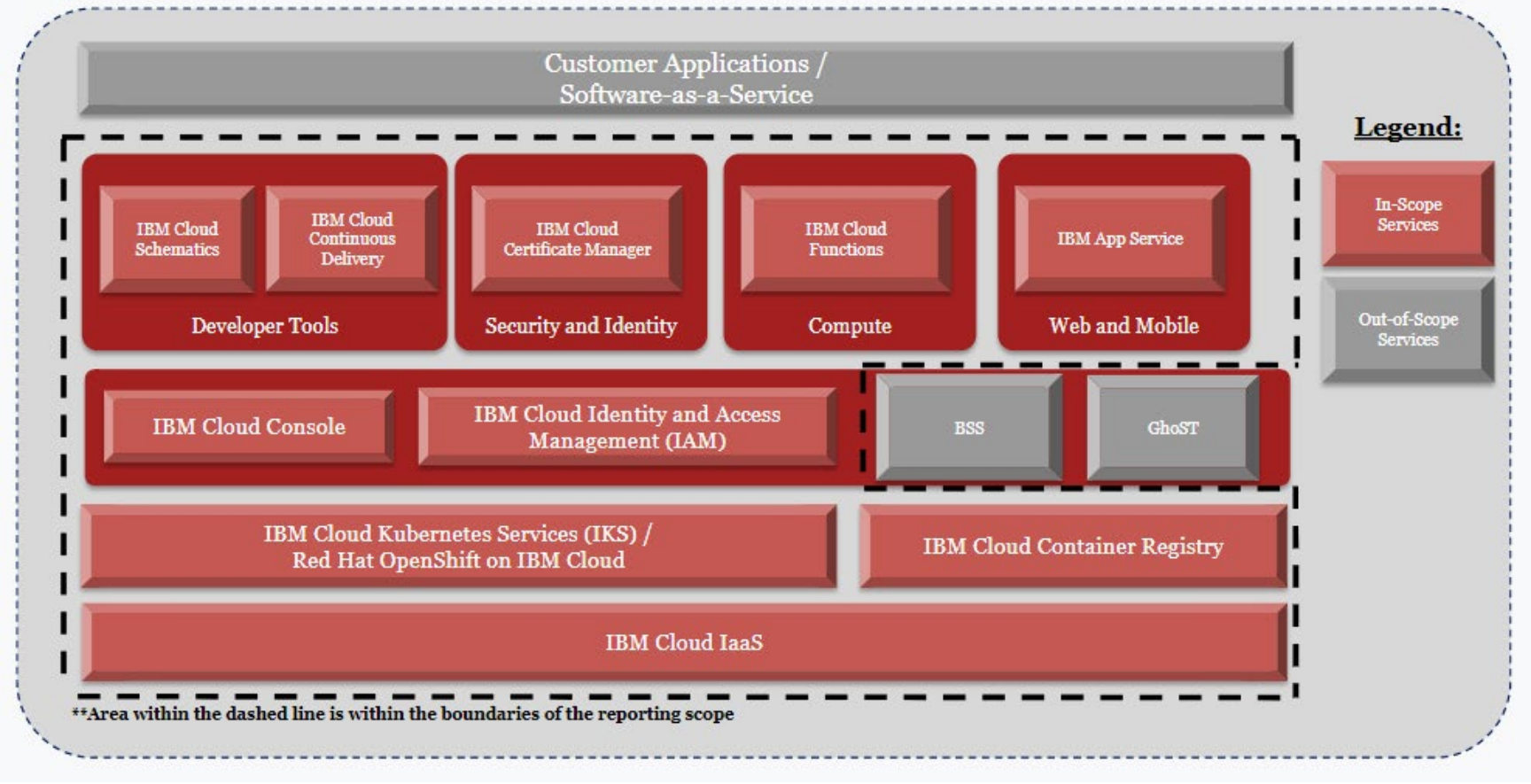

Diagram 2: Services, infrastructure, network devices, software, and data center locations within the scope of the IBM Public Cloud Platform system

Services	Data Center / Hardware Locations	Network	Platform	Operating System	Applications	Customer Data
IBM Cloud Kubernetes Service IBM Red Hat OpenShift on IBM Cloud IBM Cloud Container Registry IBM Cloud Identity and Access Management (IAM) IBM Cloud Console IBM Cloud App Service IBM Cloud Certificate Manager IBM Cloud Functions IBM Cloud Continuous Delivery IBM Cloud Schematics	In-scope components reside at IBM Cloud Infrastructure as a Service (IaaS) data center locations.	Vyatta Calico	Linux	Ubuntu Vyatta Red Hat	Customer applications and tools are solely the responsibility of the customer and are not within the scope of this report.	Customer data is solely the responsibility of the customer and is not within the scope of this report.

IBM Cloud's Public Cloud Platform Services Framework

IBM Cloud's Public Cloud Platform delivery model consists of complementary service offerings utilizing clusters of compute hosts to deploy highly available containers. These offerings are administered by a common cloud management platform, system software, and logical access structure utilizing a common control framework. As part of the delivery of IBM Cloud services, IBM Cloud is responsible for administration of the underlying network and infrastructure layers within the IT architecture supporting IBM Cloud customers.

The below description outlines the related security architecture, infrastructure, and operational details of the IBM Public Cloud Platform system that are designed in accordance with security compliance standards and deployed under common IBM Cloud policies, procedures, and related control activities.

Interacting with the Service

The IBM Cloud Console web UI can be used to order, delete, manage and interact with IBM Cloud services. Programmatic access is available via a command line interface (CLI) or through application programming interfaces (APIs). All of the access methods rely on a common IBM Cloud authentication and authorization implementation.

Kubernetes

Kubernetes is an open-source system that is used for management of containerized applications. Via Kubernetes, users can automatically deploy and scale containers. Customers who sign up for Kubernetes management using IBM Cloud Kubernetes Service, deploy their containerized applications within the isolated IBM Cloud. IBM provides security updates, monitoring, recovery, and scalability to customers deployed within the IBM Public Cloud Platform system.

In order to run applications, customers need server, storage, network equipment, and physical hardware on which an operating system can be installed. This stack allows an application to run. The IBM Cloud Kubernetes Service consists of physical (bare metal) or virtual machines that run on physical hardware located in IBM Cloud IaaS data centers.

IBM Cloud's Public Cloud Platform Service Offering Descriptions

The IBM Cloud compliance program over the Public Cloud Platform system is a multi-year effort, using a phased approach of adding "waves" of service offerings to the scope of the report once IBM Cloud compliance has determined the service offering is ready for inclusion. IBM Cloud compliance criteria, for service offerings to be added to the scope of the report, includes the compliance team's assessment of the service offering's remediation results and ability to operate controls effectively over a period of time. The scope of this report includes the Base Services, as well as the Developer Solutions that are deemed Wave 4 service offerings as part of the above compliance program.

Base Services

IBM Cloud Kubernetes Service (IKS) / Red Hat OpenShift on IBM Cloud:

IBM Cloud Kubernetes Service (IKS) is a managed Kubernetes offering to deliver management tools and built-in security and isolation to enable delivery of applications while leveraging IBM Cloud services. IKS provides native Kubernetes capabilities such as intelligent scheduling, self-healing, horizontal scaling, service discovery and load balancing, automated rollouts and rollbacks, and secret and configuration management. IBM Cloud customers may deploy their IBM Cloud Kubernetes Service on Ubuntu or RedHat OpenShift nodes. IBM Cloud Kubernetes Service runs clusters with native subnet and VLAN network on classic infrastructure.

Customers have the option to deploy apps via Red Hat OpenShift on IBM Cloud, also referred to as "ROKS". As defined in the IBM Cloud Catalog, with Red Hat OpenShift on IBM Cloud, OpenShift developers have a way to containerize and deploy enterprise workloads in Kubernetes clusters. OpenShift clusters build on Kubernetes container orchestration managed by the IBM Cloud Kubernetes Services offering. This platform is used for developing and running containerized applications on RedHat devices. It is designed to allow applications and the data centers that support them to scale only the required services instead of the entire application, allowing customers to meet application demands with minimal resources. The scope of this report does not include the RedHat OpenShift Platform itself that is provided by Red Hat.

IBM Cloud Kubernetes Service can be utilized by a customer as a stand-alone service offering or included in the service stack when a customer purchases an IBM Cloud service. The deployment, operation, scaling, and monitoring of clusters, including container security, are common across

all customers and IBM Cloud services utilizing the IBM Cloud Kubernetes Service as outlined under common IBM Cloud policies, procedures, and related control activities, below.

All other IBM Cloud services utilize the IBM Cloud Kubernetes Service and are entitled to the same security and availability service commitments and system requirements as external IBM Cloud customers.

IBM Cloud Container Registry:

IBM Cloud Container Registry provides a private image registry that is hosted and managed by IBM under common IBM Cloud policies, procedures, and related control activities. Customers can use the private registry by setting up their own image namespace and pushing container images to their namespace.

Images stored in IBM Cloud Container Registry are automatically scanned by Vulnerability Advisor, which finds potential security issues and vulnerabilities. Vulnerability Advisor checks for vulnerable packages in specific container base images and known vulnerabilities in application configuration settings. When vulnerabilities are identified, information about the vulnerability is provided along with remediation steps. Customers can use this information to resolve security issues so that containers are not deployed from vulnerable images.

IBM Cloud Identity and Access Management (IAM):

Identity and Access Management (IAM) is a non-billable, non-provisionable service that provides identity and access management for IBM Public Cloud Platform system. IAM provides secure authentication with IBM Cloud services, IBM Cloud Kubernetes Service, and all the resources in a customer's account. IAM enables IBM customers to securely authenticate users for platform services and control access to resources across IBM Cloud. The Cloud IAM access policies are used to assign users and service IDs access to the resources within an account, across IBM Cloud services.

IBM Cloud Console:

IBM Cloud Console is a non-billable service that provides a web-browser user interface for IBM Cloud. The Console allows users to create accounts, log in, access documentation, access the catalog, view pricing and account information, get support, and to order, manage and check the status of all their IBM Cloud resources.

Developer Solutions

IBM Cloud App Services:

IBM Cloud App Services allows developers to build cloud-native applications, in the language of their choice, and deploy them to IBM Cloud. Customers can build their portfolio of apps using any number of available starter kits provided by the offering, and integrate the functionality provided by other IBM Cloud service offerings, such as IBM App ID or IBM Cloud Databases, to polish off their applications.

IBM Cloud Certificate Manager:

IBM Cloud Certificate Manager helps customers obtain, store and manage SSL/TLS certificates used for IBM Cloud deployments, or other Cloud and on-prem deployments. Customers can also import SSL/TLS certificates that have been obtained for their apps and services, store them securely, and get a central view of the certificates being used. IBM Cloud Certificate Manager continuously monitors certificates for their expiration dates to notify customers of upcoming expiring certificates and other lifecycle events such as reimports, orders, or renews through Slack or Callback URLs.

IBM Cloud Schematics:

IBM Cloud Schematics delivers Terraform-as-a-Service so that customers can use a high-level scripting language to model the resources that they want in their IBM Cloud environment and enable Infrastructure as Code (IaC). Terraform is an Open Source software that enables predictable and consistent resource provisioning to rapidly build complex, multi-tier cloud environments.

IBM Cloud Schematics provides customers with the ability to organize their IBM Cloud resources across environments by using workspaces. Workspaces allow for the separation of duties for cloud resources and can be individually managed with IBM Cloud Identity and Access Management.

IBM Cloud Continuous Delivery:

IBM Cloud Continuous Delivery provides customers with DevOps capabilities in an enterprise-ready and cloud-native way by creating toolboxes that support app delivery tasks to automate builds, tests, and deployments. IBM also provides a managed CI/CD experience with Tekton pipelines in IBM Cloud Continuous Delivery toolchains, so customers can deliver cloud native applications across multiple cloud providers or on-premises systems, monitored by an integrated dashboard.

IBM Cloud Functions:

IBM Cloud Functions is a functions-as-a-service (FaaS) programming platform, based on Apache OpenWhisk, and allows users to develop lightweight code that scalably executes on demand. IBM Cloud Functions accelerates application development, which enables developers to quickly build apps with action sequences that execute in response to the event-driven world. IBM Cloud Functions is serverless, which allows for the use of multiple code languages and customer don't have to provision backend infrastructure.

Additional IBM Cloud Services Within Boundaries of the System

IBM Cloud Infrastructure as a Service (IaaS):

The IBM Public Cloud Platform system uses IBM Cloud IaaS for computer hosting facilities, including physical security access management, the supply of power, data connectivity, and secured space for the physical infrastructure.

Customers with bare metal, virtual, or hybrid environments can access the servers remotely (electronically) from anywhere in the world. Certain facilities use both co-location servers and IaaS related servers. Co-location customers do not have logical or physical access to the IBM Cloud IaaS. As such, co-location cages housing customers' servers are not included within the boundaries of the system.

Services Outside the Boundaries of the System

BSS / Global Search and Tagging (GhoST):

Customers utilize the IBM Cloud's billing and metering functionality (BSS) and Global Search and Tagging (GhoST). These are non-billable, non-provisionable services that assist customers with monitoring the spend and usage of their solutions. Although BSS and GhoST, provide customers with information regarding service usage, spend, and integrated abilities to search and tag APIs, IBM Cloud services do not rely on these components to deliver a fully-functioning system to its customers. If BSS or GhoST were impacted by service availability, the IBM Cloud services would continue to deliver each service that meets its customer commitments as defined by the IBM Cloud Service Agreement (CSA). As a result, these components are deemed to be outside the boundaries of the system and accordingly outside the scope of the report.

B. System Components

Infrastructure

IBM Cloud services use IBM Cloud IaaS for physical hosting facilities and certain aspects of network management, including physical security access management. IBM Cloud IaaS uses 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.

Facility	Physical Location	Facility Manager
AMS01	Amsterdam, Netherlands	Digital Realty
AMS03	Almere, Netherlands	NL|DC
CHE01	Ambattur, India	TATA
DAL02	Dallas, TX	SoftLayer
DAL05	Dallas, TX	Digital Realty
DAL06	Dallas, TX	SoftLayer
DAL07	Plano, TX	SoftLayer

Facility	Physical Location	Facility Manager
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
HKG02	Hong Kong, China	Digital Realty
HOU02	Houston, TX	SoftLayer
LON02	Chessington, London	Digital Realty
LON04	Farnborough, UK	Ark Data Centres
LON05	Hemel Hempsted, UK	NTT
LON06	Slough, UK	Cyrus One
MEL01	Melbourne, Australia	Digital Realty
MEX01	Queretaro, Mexico	Equinix
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	Sabey / Internap
SEO01	Gyeonggi-do, South Korea	SK C&C
SJC01	Santa Clara, CA	Digital Realty

Facility	Physical Location	Facility Manager
SJC03	Santa Clara, CA	Digital Realty
SJC04	San Jose, CA	Infomart
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
WDC01	Chantilly, VA	Digital Realty
WDC03	Ashburn, VA	Digital Realty
WDC04	Ashburn, VA	Digital Realty
WDC06	Ashburn, VA	Raging Wire
WDC07	Ashburn, VA	Sabey

Software

Overview

Software systems are managed globally by IBM using consistent controls and processes. The following systems are managed by IBM Cloud within the IBM Public Cloud Platform system:

- Linux (Ubuntu, Red Hat)
- Network Endpoints (Vyatta, Calico)

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, 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 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, as a part of the Security Steering Committee.

Procedures

The IBM Public Cloud Platform policies and procedures are a series of documents, which are used to describe the controls implemented within the IBM Public Cloud Platform 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 the IBM Public Cloud Platform system. 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 data sent to the IBM Public Cloud Platform system are solely the responsibility of the customers of the IBM Public Cloud Platform system. The IBM Public Cloud Platform system is at no time fulfilling the responsibilities of the Data Controller. Customers are responsible for maintaining their data and appointing the appropriate Data Controllers.

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 IBM Public Cloud Platform system. The CSA documents the contractual obligations of IBM Cloud and the customers using the IBM Public Cloud Platform system, 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 following sections of the CSA:

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

  Included within paragraph c. 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:

  - 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

The CSA encompasses the full list of service commitments and system requirements delivered to IBM Cloud customers that 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.

Additionally, aspects of the system description that reflect the boundaries of the IBM Public Cloud Platform system are posted online for customers and prospective customers.

Attachment C – AICPA Trust Services Criteria

This attachment includes the AICPA 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)*.

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.

Category	Criteria
	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.
	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.