IBM Cloud
IBM Public Cloud Platform

Report on IBM Cloud's IBM Public Cloud Platform System Relevant to Security and Availability

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

Prepared in Accordance with:
AT-C 205 pursuant to *TSP section 100, 2017 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" (assertion) that the controls within IBM Cloud's IBM Public Cloud Platform system (system) were effective throughout the period May 1, 2023 to April 30, 2024, 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, in 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 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 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 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 IBM Cloud's IBM Public Cloud Platform system were effective throughout the period May 1, 2023 to April 30, 2024, 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

New York, New York
June 20, 2024

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 IBM Public Cloud Platform system (the "system") throughout the period May 1, 2023 to April 30, 2024, 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, 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 IBM Cloud's service commitments and system requirements were achieved based on the applicable trust services criteria. 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, 2023 to April 30, 2024, to provide reasonable assurance that IBM Cloud's service commitments and system requirements were achieved based on the applicable trust services criteria.

Attachment A - Description of IBM Cloud's IBM Public Cloud Platform System

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 IBM 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

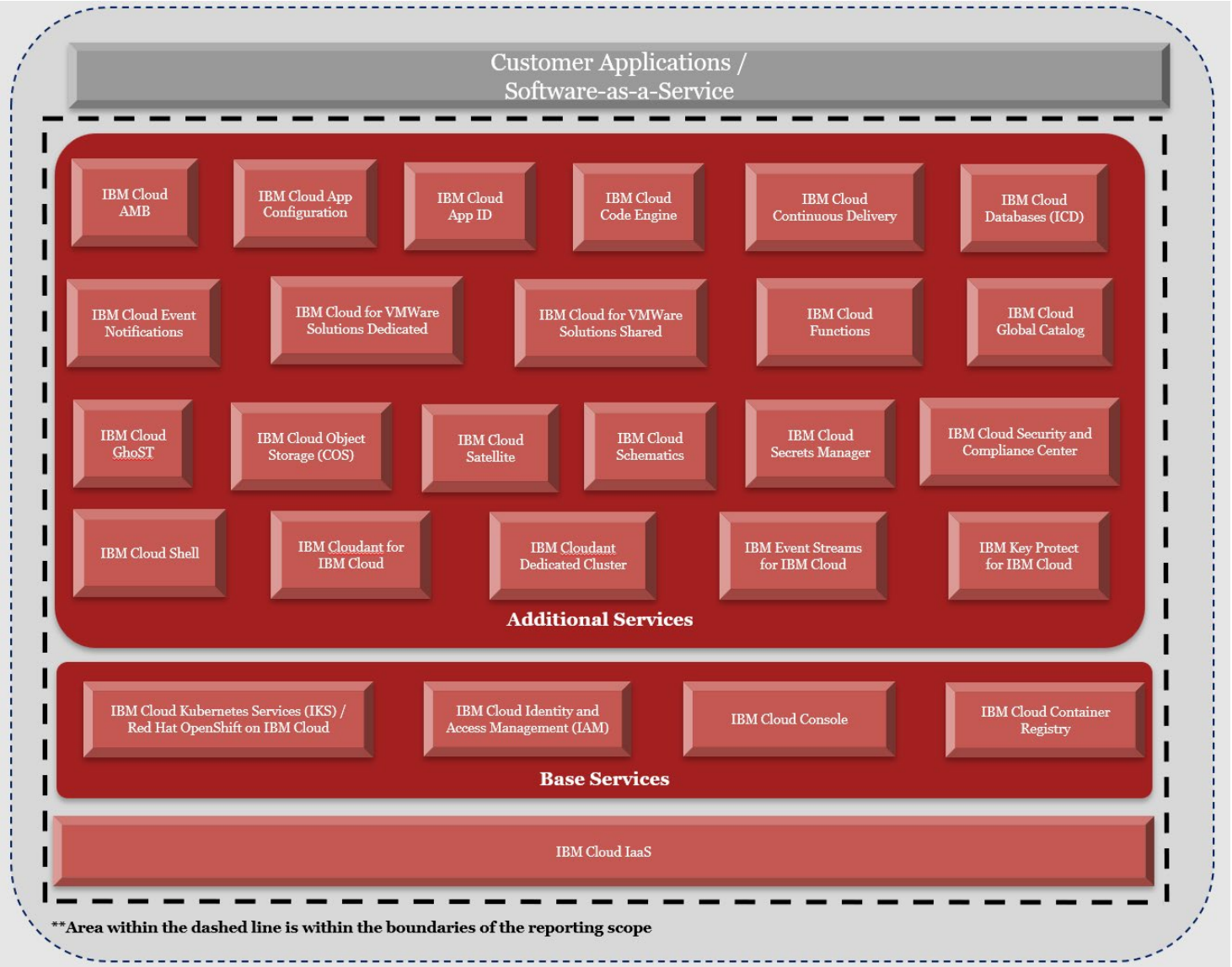

Diagram 2: Services, infrastructure, network devices, software, and data center locations within the scope of the IBM Public Cloud Platform system

Services	Data Center / Hardware Locations	Network	Platform	Operating System	Applications	Customer Data
IBM Cloud Account Management and Billing (AMB) IBM Cloud App Configuration IBM Cloud App ID IBM Cloud Code Engine IBM Cloud Console IBM Cloud Container Registry IBM Cloud Continuous Delivery IBM Cloud Databases (ICD) IBM Cloud Event Notifications IBM Cloud for VMware Solutions Dedicated IBM Cloud for VMware Solutions Shared IBM Cloud Functions IBM Cloud Global Catalog IBM Cloud Global Search & Tagging (GhoST) IBM Cloud Identity and Access Management (IAM) IBM Cloud Kubernetes Service IBM Cloud Object Storage (COS) IBM Cloud Satellite IBM Cloud Schematics IBM Cloud Secrets Manager IBM Cloud Security and Compliance Center IBM Cloud Shell IBM Cloudant for IBM Cloud IBM Cloudant Dedicated Cluster IBM Event Streams for IBM Cloud IBM Key Protect for IBM Cloud Red Hat OpenShift on IBM Cloud	In-scope components reside at IBM Cloud Infrastructure as a Service (IaaS) data center locations.	Vyatta Calico Firewall SSH	Linux Windows VMware	Ubuntu SafeNet Luna Red Hat Debian Windows vSphere ESXi Photon OS	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 IBM Public Cloud Platform Service Framework

IBM Cloud's IBM Public Cloud Platform system 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 description below 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 IBM Public Cloud Platform Service Offering Descriptions

Base 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.

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 (VA) tool, which finds potential security issues and vulnerabilities. VA 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 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 Red Hat 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 Red Hat 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 Red Hat 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.

Additional Services

IBM Cloud Account Management and Billing (AMB):

Customers utilize the IBM Public Cloud Platform's Account Management and Billing (AMB) functionality. This is a non-billable, non-provisionable service that assists customers with monitoring the spend and usage of their solutions. Although AMB provides customers with information regarding service usage and spend, IBM Public Cloud Platform services do not rely on these components to deliver a functioning system to its customers. If AMB was impacted by service availability, the IBM Public Cloud Platform services would continue to deliver each service that meets its customer commitments as defined by the Service Descriptions.

IBM Cloud App Configuration:

IBM Cloud App Configuration is a managed service on IBM Cloud that provides tools to manage configurations of distributed applications and environments. With App Configuration, developers and deployment engineers can create collections of properties and apply those properties to target applications and environments using App Configuration SDKs, continuous delivery pipelines, or plug-ins to other tools. The service also enables feature flags whereby properties are enabled and disabled within an application or environment from a centralized console in the cloud. Typically use cases for App Configurations are centralized property storage and delivery, dark launch, kill switch, environment version templating, trunk-based development, and GitOps enhancement.

IBM Cloud App ID:

IBM Cloud App ID helps developers add authentication to their web and mobile apps with few lines of code thereby securing their Cloud-native applications and services on IBM Cloud. By requiring users to sign-in to the application, user data such as app preferences or information from public social profiles can be stored. That data can then be leveraged to customize each user's experience within the app. IBM Cloud App ID provides a log-in framework for customers, but customers can also bring their own branded screens to use with Cloud Directory.

IBM Cloud Code Engine:

Customers provide IBM Cloud Code Engine with the application source code (by providing a container image or source code for IBM Cloud Code Engine to build a customer-specific container image) and define the services tailored to the customer needs. IBM Cloud Code Engine services available to customers include, function-as-a-Service, platform-as-a-Service, batch jobs, containers-as-a-Service, and events streams.

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 continuous integration and continuous delivery (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 Databases (ICD) – DataStax, Elasticsearch, Enterprise DB, etcd, Messages for RabbitMQ, MongoDB, MySQL, PostgreSQL, and Redis:

IBM Cloud Databases (ICD) provides enterprise-grade, database-as-a-service on the IBM Cloud. The service provides highly available, scalable, resilient, and secure databases through a common consumption model, orchestration APIs, and underlying architecture. The service automates tasks including hardware provisioning, networking set-up, database patching, backups, and health monitoring.

IBM Cloud Event Notifications:

IBM Cloud Event Notifications is a managed service on IBM Cloud that filters and routes event notifications from services on or off IBM Cloud to one or more destinations. Event Notifications supports both service-to-human channels like email, text, and push, and service-to-service channels. Application developers and DevOps engineers can use Event Notifications for event-driven application development, infrastructure alerting, and DevOps automation.

IBM Cloud for VMware Solutions Dedicated:

IBM Cloud for VMware Solutions Dedicated offers on-demand deployment and management of VMware solutions. Customers can automatically deploy a VMware instance on IBM Cloud bare metal servers. IBM Cloud provides access to the VMware instance/stack and allows centralized management of workloads without changing applications and tooling. Once deployed on the IBM Cloud, customers have the option of replicating and migrating their workloads across IBM Cloud IaaS data centers. The scope of this report for the IBM Cloud for VMware Solutions service offering is limited to the underlying infrastructure that supports the deployment of customer's VMware instance/stack and does not extend to the VMware customer instance after deployment is completed.

IBM Cloud for VMware Solutions Shared:

IBM Cloud for VMware Solutions Shared offers on-demand deployment and management of VMware virtual data centers. With standardized and customizable options, customers can migrate or deploy VMware workloads to IBM-hosted VMware infrastructure. IBM Cloud provides access to the customer to manage resources within the VMware virtual data center, including virtual storage, virtual memory, networking components, and IP addresses. The scope of this report for the IBM Cloud for VMware Solutions Shared service offering is limited to the underlying infrastructure that supports the deployment of customer's VMware virtual data center and does not extend to the VMware customer instance after deployment is completed.

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 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 customers are not required to provision backend infrastructure.

IBM Cloud Global Catalog:

IBM Cloud Global Catalog is the system of record that allows customers to find and manage IBM Cloud products across geographies, including options for compute, storage, networking, app deployment, security management services, databases, and cloud-native services. In addition to access from the IBM Cloud Console, API access allows customers to obtain metadata about products and manage catalog visibility. This non-billable, non-provisionable service, is built upon the IBM Public Cloud Platform containers-based architecture.

IBM Cloud Global Search & Tagging (GhoST):

Customers utilize the IBM Public Cloud Platform's Global Search and Tagging (GhoST). This is a non-billable, non-provisionable service that assists customers with monitoring the spend and usage of their solutions. Although GhoST provides customers with integrated abilities to search and tag APIs, IBM Public Cloud Platform services do not rely on these components to deliver a functioning system to its customers. If GhoST was impacted by service availability, the IBM Public Cloud Platform services would continue to deliver each service that meets its customer commitments as defined by the Service Descriptions.

IBM Cloud Object Storage (COS):

IBM Cloud Object Storage service provides secure, flexible, scalable public cloud storage for unstructured data. The Cloud Object Storage service provides customers the ability to store large volumes of unstructured data with durability, security, and availability.

With IBM Cloud Object Storage, developers and organizations can store and access data for analytics, IoT, social, cognitive and IBM Cloud workloads. Users can also use IBM Cloud Object Storage for archiving and long-term data retention. With IBM Cloud Object Storage, users can choose the level of resiliency for their workloads including cross region and regional resiliency. Users can deploy storage buckets with the IBM Cloud Object Storage UI and API and choose the storage class for their active, cool, cold and dynamic data workloads.

IBM Cloud Object Storage is an IBM Cloud IaaS service with devices locally attached, residing in the IBM Cloud IaaS control row. The IBM Cloud IaaS IMS system provides the underpinning for user and storage instance provisioning and is included in the IBM Cloud IaaS system boundary and therefore not included within the scope of this report. The provisioning path developers create and manage to authenticate to the IBM Cloud Object Storage is performed through the IBM COS Broker and included in the IBM Public Cloud Platform system boundary and as such, the COS Broker is included within the scope of this report.

IBM Cloud Satellite:

IBM Cloud Satellite can be utilized by customers to deploy IBM Public Cloud services onto non-IBM infrastructure, including on-premises data centers, other cloud providers, or edge networks. This deployment enables a hybrid cloud environment with the scalability and on-demand flexibility of public cloud services on a secure private cloud. This service is built upon the IBM Public Cloud Platform containers-based architecture. The scope of this report for the IBM Cloud Satellite service offering is limited to the IBM managed infrastructure hosted on the IBM Cloud, and does not extend to customer managed infrastructure hosted elsewhere such as on-premise data centers, other cloud providers.

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 Secrets Manager:

IBM Cloud Secrets Manager provides customers the ability to create, lease, and centrally manage secrets that are used in IBM Cloud services, including both Identity and Access Management (IAM) credentials and custom secrets. Secrets are stored in a dedicated Secrets Manager instance, built on open source HashiCorp Vault. This service is built upon the IBM Public Cloud Platform containers-based architecture.

IBM Cloud Security and Compliance Center:

IBM Cloud Security and Compliance Center (SCC) allows customers to manage their security and compliance posture, configuration governance, and security insights through a single dashboard view. Customers deploy a “Collector” in the customer’s environment and elect the SCC profile, which is a collection of controls and individual goals for the customer’s security and compliance reporting. IBM Cloud SCC provides the customer with real-time compliance results.

IBM Cloud Shell:

IBM Cloud Shell, a non-billable, non-provisionable service, is publicly available on the IBM Cloud Console and provides customers control of their cloud resources, applications and infrastructure from any web browser, with one click from the IBM Cloud Console. This temporary workspace is operating system (OS) agnostic, allowing customers to access command line within a secure containerized environment.

IBM Cloudant for IBM Cloud and IBM Cloudant Dedicated Cluster:

IBM Cloudant includes two service offerings viz. IBM Cloudant for IBM Cloud and IBM Cloudant Dedicated Cluster. IBM Cloudant provides a hybrid, open-source based approach that application developers, data scientists, and IT architects can use to address data-intensive needs via various Database-as-a-service (DBaaS) solutions. The service is a document-oriented NoSQL database designed to be the data layer for mission critical applications. Cloudant is offered both as a cloud service and an on-premise installation and as such offers maximum deployment flexibility between public cloud, private cloud, and open-source options. The Cloudant on-premise installations are not included in this report.

IBM Event Streams for IBM Cloud:

IBM Event Streams for IBM Cloud (Enterprise) and IBM Event Streams for IBM Cloud (Standard) are scalable, distributed, high throughput messaging services, built on top of Apache Kafka, that enables applications and services to communicate.

IBM Key Protect for IBM Cloud:

IBM Key Protect is a cloud-based security service that provides life cycle management for encryption keys that are used in IBM Cloud services or customer-built applications. IBM Key Protect allows customers to provision encrypted keys for applications across IBM Cloud services. Customers can also import their own encryption keys into IBM Key Protect for secure key management. Customers manage the lifecycle of their keys via FIPS 140-2 Level 3 certified, tamper resistant, hardware security modules (HSMs).

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.

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
AMS03	Almere, Netherlands	NL|DC
CHE01	Ambattur, India	TATA
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
PAR01	Paris, France	Global Switch

Facility	Physical Location	Facility Manager
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
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
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, SafeNet Luna, Debian)
- Windows
- VMware (vSphere, ESXi, Photon OS)
- Network Endpoints (Vyatta, Calico, Firewall, SSH)

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 and availability controls, as a part of the Security Steering Committee.

Procedures

The IBM Public Cloud Platform policies and procedures are a series of documents 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 are 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 customers through the IBM Customer Portal.

Only the principal service commitments and system requirements relevant to the applicable trust services criteria are within the boundaries of the system. Security and availability commitments include but are not limited to the following:

- 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.

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 in the IBM Cloud Terms of Use within the IBM Customer Portal.

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	Trust Services 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	Trust Services 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	Trust Services 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	Trust Services 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.