IBM Cloud
IBM Virtual Private Cloud (VPC)

Report on IBM Cloud's Virtual Private Cloud (VPC) System Relevant to Security and Availability

For the period May 1, 2023 through 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 Virtual Private Cloud (VPC) 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 Virtual Private Cloud (VPC) 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 Virtual Private Cloud (VPC) 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 Virtual Private Cloud (VPC) System

A. System Overview

Background

The IBM Virtual Private Cloud (VPC) system is composed of several 'as a service' offerings that provide the underlying infrastructure for virtualized compute, storage and networking solutions provisioned to IBM Cloud's customers as isolated virtual private cloud partitions. IBM VPC services use both IBM Cloud Kubernetes and custom Kubernetes solutions to enable customers to purchase, deploy, and manage virtual private clouds and associated compute, storage and networking resources (e.g., VPNs, Load Balancers, etc.). 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 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 VPC services. The scope does not include the data structures/schemas, customer applications and tools that customers use to load, analyze and manipulate data, as those are solely the responsibility of the customer. Refer to *Diagram 2: Services, infrastructure, network devices, software, and data center locations within the scope of the IBM VPC system* included in this report for details.

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

IBM VPC services provide interfaces that allow customers to request virtual servers, clusters, networks, storage and other cloud resources. These resources are created by IBM Cloud within an environment unique to each customer and logically isolated from other customers. Within each customer environment, these servers, clusters, networks, storage and other resources are managed by IBM Cloud's customers and are not included within the scope of the report. 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 report. The integrity and regulatory requirements of such data are solely the responsibility of the customer.

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

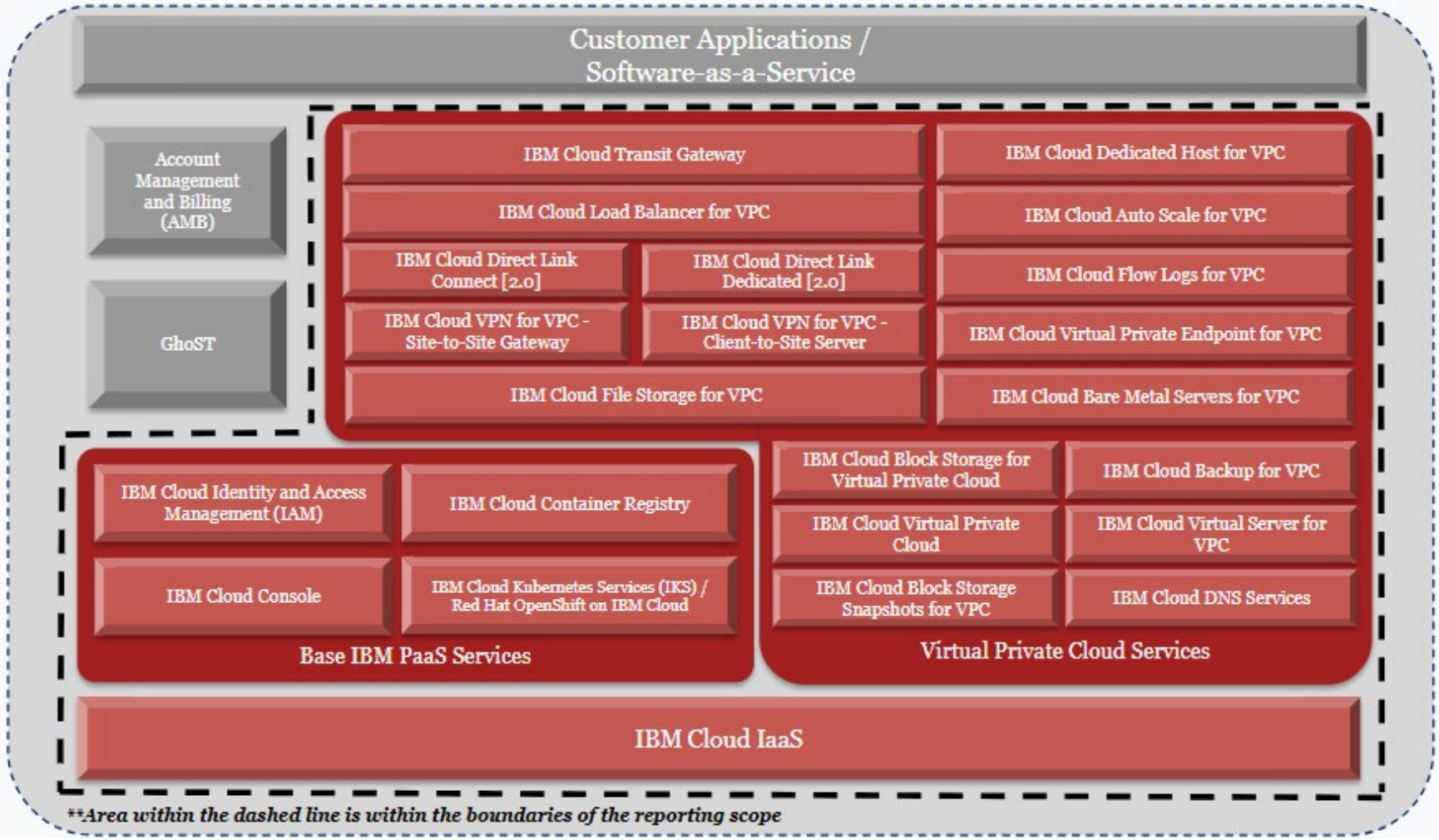

Diagram 2: Services, infrastructure, network devices, software, and data center locations within the scope of the IBM VPC system

Services	Data Center / Hardware Locations	Network	Platform	Operating System	Applications	Customer Data
IBM VPC services IBM Cloud Auto Scale for VPC IBM Cloud Backup for VPC IBM Cloud Bare Metal Servers for VPC IBM Cloud Block Storage for Virtual Private Cloud IBM Cloud Block Storage Snapshots for VPC IBM Cloud Dedicated Host for VPC IBM Cloud Direct Link Connect [2.0] IBM Cloud Direct Link Dedicated [2.0] IBM Cloud DNS Services IBM Cloud File Storage for VPC IBM Cloud Flow Logs for VPC IBM Cloud Load Balancer for VPC IBM Cloud Transit Gateway IBM Cloud Virtual Private Cloud IBM Cloud Virtual Private Endpoint for VPC IBM Cloud Virtual Server for VPC IBM Cloud VPN for VPC – Client-to-Site Server IBM Cloud VPN for VPC – Site-to-Site Gateway IBM Public Cloud services IBM Cloud Console IBM Cloud Container Registry IBM Cloud Identity and Access Management (IAM) IBM Cloud Kubernetes Service Red Hat OpenShift on IBM Cloud	In-scope components reside at IBM Cloud Infrastructure as a Service (IaaS) data center locations.	Vyatta Calico IP Tables	Linux	Ubuntu 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 VPC Services Framework

IBM Cloud's IBM VPC services are public cloud offerings that enable an enterprise to establish its own private cloud-like computing environment on a shared public cloud infrastructure. IBM VPC services give customers the ability to define and control a virtual network that is logically isolated from all other public cloud tenants, creating a private, secure place on the public cloud. As part of the delivery of IBM VPC services, IBM Cloud is responsible for administration of the underlying network and infrastructure layers within the IT architecture supporting IBM Cloud customers.

IBM VPC services, including the related security architecture, infrastructure, and operations 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. Additional 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.

IBM VPC Service Offering Descriptions

IBM Cloud Auto Scale for VPC:

IBM Cloud Auto Scale for VPC is an optional, managed auto-scale service compatible within the IBM VPC system. If a customer contracts for auto-scale, IBM VPC assets are provisioned and reduced in accordance with dynamic customer needs.

IBM Cloud Backup for VPC:

IBM Cloud Backup for Virtual Private Cloud (VPC) service provides VPC customers the ability to automatically back up, manage, and restore block storage volumes from backups generated by IBM Cloud Block Storage Snapshots for VPC. Customers can manage the frequency, retention period, and deletion of backups.

IBM Cloud Bare Metal Servers for VPC:

IBM Cloud Bare Metal Servers for VPC is an offering within the Compute Infrastructure-as-a-Service portfolio of IBM Cloud. IBM Cloud Bare Metal Servers for VPC provides access to dedicated (single-tenant) computing resources that the Client can provision as part of a VPC infrastructure environment.

IBM Cloud Bare Metal Servers for VPC, like the rest of the Infrastructure-as-a-Service offerings, is self-managed by the Client. This includes selection of available data centers and selection, configuration, and management of services (such as security, backup, failover, restore, and monitoring), which the Client determines are necessary to meet the Client's requirements and applicable laws, including data protection and other regulatory requirements for its workloads and all Content. Bare metal server-hour is equivalent to Instance-hour in definition and metric usage.

IBM Cloud Block Storage for Virtual Private Cloud:

IBM Cloud Block Storage for Virtual Private Cloud is an optional, managed block storage offering compatible within the IBM VPC system. The regional infrastructure API service (RIAS) component of the VPC network is leveraged to link storage blocks from the IBM Cloud Infrastructure-as-a-Service (IaaS) system to the customer's IBM VPC instances.

IBM Cloud Block Storage Snapshots for VPC:

IBM Cloud Block Storage Snapshots for VPC is an optional, managed backup service compatible with the IBM Cloud Block Storage for VPC service offering. Snapshots (i.e. backups) can be created and updated incrementally for customer block storage boot or data volumes. Snapshots are stored in IBM Cloud Object Storage and can be used to deploy or restore volumes in the customer environment.

IBM Cloud Dedicated Host for VPC:

IBM Cloud Dedicated Hosts for VPC is a managed virtual private cloud offering for customers that require IBM VPC instances on dedicated compute infrastructure. IBM VPC instances on dedicated hardware are deployed and managed identically to IBM VPC instances on shared hardware.

IBM Cloud Direct Link Connect (2.0):

IBM Cloud Direct Link provides connectivity from an external source into a customer's IBM Cloud private network. An alternative to a traditional site-to-site VPN solution, it is a routed, OSI Layer-3 service designed for customers that need more consistent, higher-throughput connectivity between a remote network and their IBM Cloud environments. IBM Cloud Direct Link Connect is a component service of IBM Cloud Direct Link that allows customers private access to IBM Cloud Infrastructure and to any other clouds linked to their service provider through their local IBM Cloud data center, creating multi-cloud connectivity in a single environment. This service is built upon the IBM Public Cloud Platform containers-based architecture.

IBM Cloud Direct Link Dedicated (2.0):

IBM Cloud Direct Link provides connectivity from an external source into a customer's IBM Cloud private network. An alternative to a traditional site-to-site VPN solution, it is a routed, OSI Layer-3 service designed for customers that need more consistent, higher-throughput connectivity between a remote network and their IBM Cloud environments. IBM Cloud Direct Link Dedicated (2.0) is a component service of IBM Cloud Direct Link that allows customers to terminate a single-tenant, fiber-based cross-connect into the IBM Cloud network. This service is built upon the IBM Public Cloud Platform containers-based architecture.

IBM Cloud DNS Services:

IBM Cloud DNS Services allows customers to manage hostnames and IP addresses on virtual private cloud networks while limiting access to DNS records from permitted networks only. Customers can create private DNS zones that hold domain names, create DNS resource records under DNS

zones, and specify access controls used for the DNS resolution of resource records on a zone-wide level. Private DNS zones are resolvable only on IBM Cloud, and only from explicitly permitted networks in an account. This service is built upon the IBM Public Cloud Platform containers-based architecture.

IBM Cloud File Storage for VPC:

IBM Cloud File Storage for VPC is a zonal file storage offering that provides NFS-based file storage services. The service enables customers to create, manage, and encrypt file shares across multiple VPCs and virtual server instances.

IBM Cloud Flow Logs for VPC:

IBM Cloud Flow Logs for VPC enables the collection, storage, and presentation of information about the Internet Protocol (IP) traffic going to and from network interfaces within a customer's IBM VPC instances.

IBM Cloud Load Balancer for VPC:

IBM Cloud Load Balancer for VPC is an optional, managed load balancer as-a-service (LBaaS) component within the IBM VPC system. With the assistance of the LBaaS control plane running on IBM Cloud Kubernetes Services containers infrastructure, configurable load balancer appliances are dynamically deployed onto IBM VPC instances and hosted by the same compute infrastructure.

IBM Cloud Transit Gateway:

IBM Cloud Transit Gateway allows customers to manage connections between virtual private cloud resources across multiple regions. Customers can create single or multiple transit gateways to connect virtual private cloud instances together, or to IBM Cloud classic infrastructure. This service is built upon the IBM Public Cloud Platform containers-based architecture.

IBM Cloud Virtual Private Cloud:

IBM Cloud Virtual Private Cloud is the networking component of the managed virtual private cloud offering. The service provides a software defined "virtual network" that is logically isolated from other IBM Public Cloud tenants. Customers are able to add other resources, such as virtual servers, to be connected to this virtual network.

IBM Cloud Virtual Private Endpoint for VPC:

IBM Cloud Virtual Private Endpoints for VPC enables customers to connect to supported IBM Cloud services from customer VPC networks by using the IP addresses of their choosing, allocated from a subnet within the customer's IBM VPC instances.

IBM Cloud Virtual Server for VPC:

IBM Cloud Virtual Server for VPC is a managed virtual private cloud offering. It represents the "core" offering through which IBM VPC instances are deployed to customers on shared compute infrastructure. To maximize availability, IBM VPC instances may be deployed across availability zones supported by multiple data centers within a chosen region referred to as a multi-zone region (MZR). An IBM Cloud Virtual Server for VPC with an s390x processor architecture is not included in scope of this report.

IBM Cloud VPN for VPC – Client-to-Site Server:

Client VPN for VPC provides the capability for individual users to connect to IBM Cloud through a secure and encrypted client-to-site connection. When these users are travelling, working remotely, or are connecting from a location without site-to-site connectivity, they can connect to VPN servers on IBM Cloud VPC using an OpenVPN client.

IBM Cloud VPN for VPC – Site-to-Site Gateway:

IBM Cloud VPN for VPC – Site-to-Site Gateway is an optional, managed virtual private network as-a-service (VPNaaS) component within the IBM VPC system. With the assistance of the VPNaaS control plane running on IBM Cloud Kubernetes Services containers infrastructure, configurable VPN appliances are dynamically deployed onto IBM VPC instances and hosted by the same compute infrastructure.

Other IBM Public Cloud Services Within Boundaries of the System

The following IBM Public Cloud services provide the building blocks necessary to deliver scalable, highly available "cloud native" offerings on the IBM Public Cloud. In addition to being offered directly to customers, these services are foundational to the delivery of many IBM Public Cloud offerings, including IBM VPC 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, 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 the IBM VPC services. IAM provides secure authentication with IBM VPC services, IBM Public Cloud services, 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 IAM access policies are used to assign users and service IDs access to the resources within an account, across IBM VPC 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.

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.

IBM Cloud Infrastructure as a Service (IaaS):

The 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

Account Management and Billing (AMB) / Global Search and Tagging (GhoST):

Customers utilize the IBM Cloud's Account Management and Billing functionality (AMB) 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 AMB 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 functioning system to its customers. If AMB 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 outside the boundaries of the system and accordingly outside the scope of the report.

B. System Components

Infrastructure

IBM VPC services share IBM Cloud IaaS 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
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
OSA2X	Osaka, Japan	IDC Frontier
PAR04	Paris, France	Global Switch
PAR05	Paris, France	BNPP
PAR06	Paris, France	BNPP

Facility	Physical Location	Facility Manager
SAO01	Sao Paulo, Brazil	Ascenty
SAO04	Santana de Parnaíba, Brazil	Odata
SAO05	Sao Paulo, Brazil	Ascenty
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 VPC system:

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

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 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, as a part of the Security Steering Committee.

Procedures

The IBM Cloud policies and procedures are a series of documents, which are used to describe the controls implemented within the IBM VPC 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 VPC 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 VPC system are solely the responsibility of the customers of the IBM VPC system. The IBM VPC 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 the 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 users of the IBM VPC system. The CSA documents the contractual obligations of IBM Cloud and the customers using IBM VPC services, 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 outlined below. 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 VPC 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	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.