IBM Cloud

Platform as a Service (PaaS) System for the IBM Cloud Foundry Public Environment

Report on IBM Cloud's Platform as a Service (PaaS) System for the IBM Cloud Foundry Public Environment Relevant to Security

For the period September 1, 2018 to August 31, 2019

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

IBM Cloud
Platform as a Service (PaaS) System for the IBM Cloud Foundry Public Environment
SOC 3 Report Relevant to Security
For the period September 1, 2018 to August 31, 2019

Table of Contents

Report of Independent Accountants

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 Platform as a Service (PaaS) System (system) for the IBM Cloud Foundry Public Environment were effective throughout the period September 1, 2018 to August 31, 2019, to provide reasonable assurance that IBM Cloud's service commitments and system requirements were achieved based on the trust services criteria relevant to security (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

- 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 PaaS system for the IBM Cloud Foundry Public Environment were effective throughout the period September 1, 2018 to August 31, 2019, 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

November 21, 2019

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 Platform as a Service (PaaS) System (system) for the IBM Cloud Foundry Public Environment throughout the period September 1, 2018, to August 31, 2019, to provide reasonable assurance that IBM Cloud’s service commitments and system requirements relevant to security 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 September 1, 2018, to August 31, 2019, to provide reasonable assurance that IBM Cloud’s service commitments and system requirements were achieved based on the trust services criteria relevant to security (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 September 1, 2018 to August 31, 2019, 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 Platform as a Service (PaaS) System for the IBM Cloud Foundry Public Environment

A. System Overview

Background

IBM Cloud Foundry is an open-standards, cloud platform for developing, operating, and managing applications via a Platform as a Service (PaaS) delivery model. IBM Cloud Foundry is designed to manage and maintain software and services solutions to meet a variety of changing requirements, while being responsible for providing operations support and maintenance, operating and maintaining system software, and platform disaster recovery capabilities. IBM Cloud Foundry also includes IBM SoftLayer's Infrastructure as a Service (IaaS) for physical hosting services.

Customers that subscribe to IBM Cloud Foundry acknowledge receipt and agreement of a standard Cloud Services Agreement (CSA). The CSA is standard for all customers of the service and includes a description of the services provided by IBM Cloud, and certain legal terms and conditions. All users of the IBM Cloud Foundry are subject to the CSA developed for IBM Cloud.

IBM Cloud Foundry includes the following service offerings:

- **Cloud Public Platform** provides customers functional support, infrastructure support and operational support for the core, public-based platform.
- **Cloud Dedicated Platform** is similar to the Public Platform, but offers dedicated services and systems to customers that are logically and physically segregated from other dedicated or public customers. The Dedicated Platform is not within the scope of this report.
- **IBM SoftLayer** provides on-demand cloud IaaS. SoftLayer offers bare metal, virtual server, or hybrid computing environments, leveraging global data centers and points of presence (PoP).

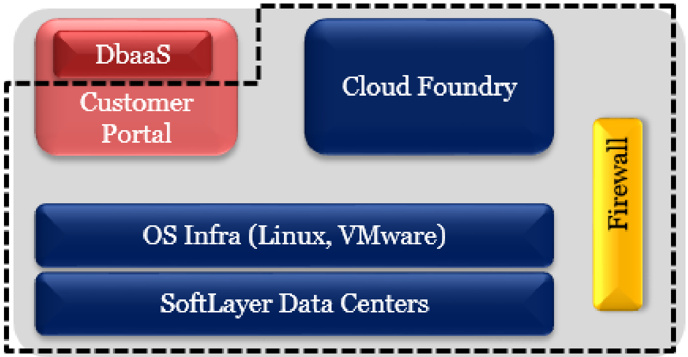
Boundaries of the System

This report covers the components, infrastructure, network devices and software for IBM Cloud's PaaS system for the IBM Cloud Foundry Public Environment, as documented in Table 1 of this report.

IBM Cloud Foundry also uses IBM SoftLayer's IaaS for physical hosting facilities, including physical security access management. The diagram below shows the scope of IBM Cloud's PaaS system for the IBM Cloud Foundry Public Environment.

Within each customer environment, applications 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 Foundry. 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.

IBM Cloud PaaS System for the IBM Cloud Foundry Public Environment SOC 3 Scope



**All components within the dotted border represent the scope of the IBM Cloud PaaS system for the IBM Cloud Foundry Public Environment.

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

Component	Datacenter / Hardware Locations	Network	Operating System Infrastructure	System Software	Applications	Customer Data
Cloud Public Platform	In-scope components reside at SoftLayer datacenter locations. Refer to in-scope locations below.	Vyatta Fortigate DataPower	Linux VMware	Ubuntu CentOS Redhat	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.

B. System Components

Infrastructure

IBM Cloud Foundry uses IBM SoftLayer's IaaS for computer hosting facilities, including physical security access management, the supply of power, data connectivity, and secured space for the physical infrastructure.

SoftLayer provided its IaaS using multiple locations listed below, throughout the period covered by this report, and 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 SoftLayer facilities included within the scope of the system.

Facility	Physical Location	Facility Manager
DAL05	Dallas, TX	Digital Realty
DAL06	Dallas, TX	SoftLayer
DAL09	Richardson, TX	Digital Realty
DAL1o	Irving, TX	QTS
DAL12	Richardson, TX	Digital Realty
DAL13	Carrollton, TX	Cyrus One
FRA02	Frankfurt, Germany	Zenium Technology
FRA04	Frankfurt, Germany	E-Shelter
FRA05	Frankfurt, Germany	Interxion
LON02	Chessington, London	Digital Realty
LON04	Farnborough, UK	Ark Data Centres
LON05	Hemel Hempstead, London	Gyron
LON06	Farnborough, UK	Ark Data Centres
MEL01	Melbourne, Australia	Digital Realty
SJC01	Santa Clara, CA	Digital Realty
SJC03	Santa Clara, CA	Digital Realty
SYD01	Sydney, Australia	Global Switch
SYD04	Erskine Park, Australia	Digital Realty
SYD05	Sydney, Australia	Equinix
TOR01	Ontario (Markham), Canada	Digital Realty
WDC04	Ashburn, VA	Digital Realty

Facility	Physical Location	Facility Manager
WDC06	Ashburn, VA	Sabey
WDC07	Ashburn, VA	Raging Wire

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 SoftLayer IaaS. As such, co-location cages housing customers' servers are not included within the boundaries of the system.

Software

Overview

Software systems are managed globally by IBM using consistent controls and processes. The following systems are managed by IBM Cloud PaaS for the IBM Cloud Foundry Public Environment:

- Operating Systems (RedHat, CentOS, Ubuntu, ESXi)
- Network Devices (Vyatta, Fortigate, DataPower)

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 industry leading 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 policies and procedures are a series of documents, which are used to describe the controls implemented within the IBM Cloud PaaS system for the IBM Cloud Foundry Public Environment. 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 Cloud PaaS system for the IBM Cloud Foundry Public Environment. 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 Cloud PaaS system for the IBM Cloud Foundry Public Environment are solely the responsibility of the customers of the IBM Cloud PaaS system for the IBM Cloud Foundry Public Environment. IBM Cloud Foundry 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 IBM Cloud Foundry. The CSA documents the contractual obligations of IBM Cloud and the customers using IBM Cloud Foundry, including principle service commitments and system requirements. Any updates to the CSA are communicated to the existing customers through the Customer Portal.

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

1. Cloud Services
2. Content and Data Protection

   Included within item c. of the Content and Data Protection section of the CSA 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

Attachment C – AICPA Trust Services Criteria

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

Security Category

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

Criteria

Category	Criteria
CC1.0 Control Environment	CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
	CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
	CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
	CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
	CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC2.0 Communication and Information	CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
	CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
	CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.

Category	Criteria
CC3.0 Risk Assessment	CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
	CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
	CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.
	CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.
CC4.0 Monitoring Activities	CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
	CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
CC5.0 Control Activities	CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
	CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
	CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC6.0 Logical and Physical Access Controls	CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.

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

Category	Criteria
	CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.
CC8.0 Change Management	CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
CC9.0 Risk Mitigation	CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
	CC9.2 The entity assesses and manages risks associated with vendors and business partners.