# *SoftLayer Technologies, Inc.*
## *IBM Cloud Infrastructure as a Service (IaaS)*

Report on SoftLayer Technologies, Inc.'s Description of its Information Technology General Controls System for IBM Cloud Infrastructure as a Service (IaaS) and on the Suitability of the Design and Operating Effectiveness of Controls

For the period November 1, 2021 to October 31, 2022

Prepared in Accordance with:

- American Institute of Certified Public Accountants AICPA AT-C 320*, Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting*
- International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*

## *Table of Contents*

**Section** **Page**

**Report of Independent Service Auditors**

To the Management of SoftLayer Technologies, Inc.

*Scope*

We have examined SoftLayer Technologies, Inc.'s (the "Service Organization") description of its information technology general controls system for IBM Cloud Infrastructure as a Service (IaaS) (the "system") entitled "SoftLayer Technologies, Inc.'s Description of its Information Technology General Controls System for IBM Cloud Infrastructure as a Service (IaaS)" throughout the period November 1, 2021 to October 31, 2022 (the "description") and the suitability of the design and operating effectiveness of the controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "SoftLayer Technologies, Inc.'s Assertion/Statement" (the "assertion"). The controls and control objectives included in the description are those that management of the Service Organization believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the system that are not likely to be relevant to user entities' internal control over financial reporting.

The description of the system does not include control objectives related to business process controls, automated application controls, or key reports produced by IBM Cloud Infrastructure as a Service (IaaS). Therefore, our examination did not extend to control objectives related to business process controls, automated application controls, or key reports produced by IBM Cloud Infrastructure as a Service (IaaS).

The information included in Section V "Other Information Provided by SoftLayer Technologies, Inc. That is Not Covered by the Service Auditors' Report" is presented by management of the Service Organization to provide additional information and is not a part of the description. Information about the Service Organization's management response to exceptions identified has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description.

*Service organization's responsibilities*

In Section II, the Service Organization has provided an assertion/statement about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The Service Organization is responsible for preparing the description and the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

*Service auditors' responsibilities*

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period November 1, 2021 to October 31, 2022. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description based on the criteria in management's assertion.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in the assertion in Section II.

*Service auditors' independence and quality control*

We have complied with the independence and other ethical requirements of the Code of Professional Conduct established by the AICPA.

We applied the quality control standards established by the AICPA and accordingly maintain a comprehensive system of quality control.

*Inherent limitations*

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization or a subservice organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions by the system. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization or a subservice organization may become ineffective.

*Description of tests of controls*

The specific controls tested and the nature, timing, and results of those tests are listed in Section IV.

*Opinion*

In our opinion, in all material respects, based on the criteria described in SoftLayer Technologies, Inc.'s Assertion/Statement in Section II,

*a.* the description fairly presents the system that was designed and implemented throughout the period November 1, 2021 to October 31, 2022.

*b.* the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period November 1, 2021 to October 31, 2022.

*c.* the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period November 1, 2021 to October 31, 2022.

*Restricted use*
This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of management of IBM Corporation, the ultimate parent company of SoftLayer Technologies, Inc., user entities of the system during some or all of the period November 1, 2021 to October 31, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties. If report recipients are not user entities that have contracted for services with SoftLayer Technologies, Inc. for the period November 1, 2021 to October 31, 2022 or their independent auditors (herein referred to as a "non-specified user") and have obtained this report, or have access to it, use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do

not acquire any rights against PricewaterhouseCoopers LLP as a result of such access. Further, PricewaterhouseCoopers LLP does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

PricewaterhouseCoopers LLP

January 13, 2023

SoftLayer Technologies, Inc.
14001 North Dallas Parkway,
Suite M100
Dallas, Texas 75240

## SoftLayer Technologies, Inc.'s Assertion/Statement

We have prepared the description of SoftLayer Technologies, Inc.'s information technology general controls system for IBM Cloud Infrastructure as a Service (IaaS) (the "system") entitled "SoftLayer Technologies, Inc.'s Description of its Information Technology General Controls System for IBM Cloud Infrastructure as a Service (IaaS)" throughout the period November 1, 2021 to October 31, 2022 (the "description") for user entities of the system during some or all of the period November 1, 2021 to October 31, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

The description of the system does not include control objectives related to business process controls, automated application controls, or key reports produced by IBM Cloud Infrastructure as a Service (IaaS). Therefore, the examination did not extend to control objectives related to business process controls, automated application controls, or key reports produced by IBM Cloud Infrastructure as a Service (IaaS).

We confirm, to the best of our knowledge and belief, that

*a.* the description fairly presents the system made available to user entities of the system during some or all of the period November 1, 2021 to October 31, 2022 as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion/statement were that the description

i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable,

(1) the types of services provided, including, as appropriate, the classes of transactions processed.

(2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

(3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

(4) how the system captures and addresses significant events and conditions other than transactions.

(5) the process used to prepare reports and other information for user entities.

SoftLayer Technologies, Inc.
14001 North Dallas Parkway,
Suite M100
Dallas, Texas 75240

(6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.

(7) the specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the service organization's controls.

(8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. includes relevant details of changes to the system during the period covered by the description.

iii. does not omit or distort information relevant to the system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the system that each individual user entity of the system and its auditor may consider important in its own particular environment.

*b.* the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period November 1, 2021 to October 31, 2022 to achieve those control objectives. The criteria we used in making this assertion/statement were that

i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of the service organization.

ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved.

iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

# *III. SoftLayer Technologies Inc.'s Description of its Information Technology General Controls System for IBM Cloud Infrastructure as a Service (IaaS)*

**Overview**

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

IBM Cloud IaaS is built using a Network-Within-A-Network topology that provides remote access to allow customers the ability to build and manage computing environments remotely. IBM Cloud IaaS's "Network-Within-A-Network" configuration includes three (3) network interfaces. Public, private, and management traffic travel across separate network interfaces, segregating and securing traffic while streamlining management functions.

- Public Network - Network traffic from anywhere in the world will connect to the closest network PoP, and it will travel directly across the network to its data center, minimizing the number of network hops and handoffs between providers.
- Private Network - Provides a connection to the customer's servers (bare metal or virtual) in IBM Cloud IaaS data centers around the world. Data can be moved between servers through the private network; and customers can utilize various services, update and patch servers, software repositories, and backend services, without interfering with public network traffic.
- Management Network - Each server within the IBM Cloud IaaS is connected to the management network. This out-of-band management network, accessible via VPN, allows access to each server for maintenance and administration, independent of its CPU and regardless of its firmware or operating system.

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

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

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

IMS has two components: IMS, as viewed by internal employees, and the Customer Portal, as available to users of IBM Cloud IaaS. The Customer Portal allows customers to:

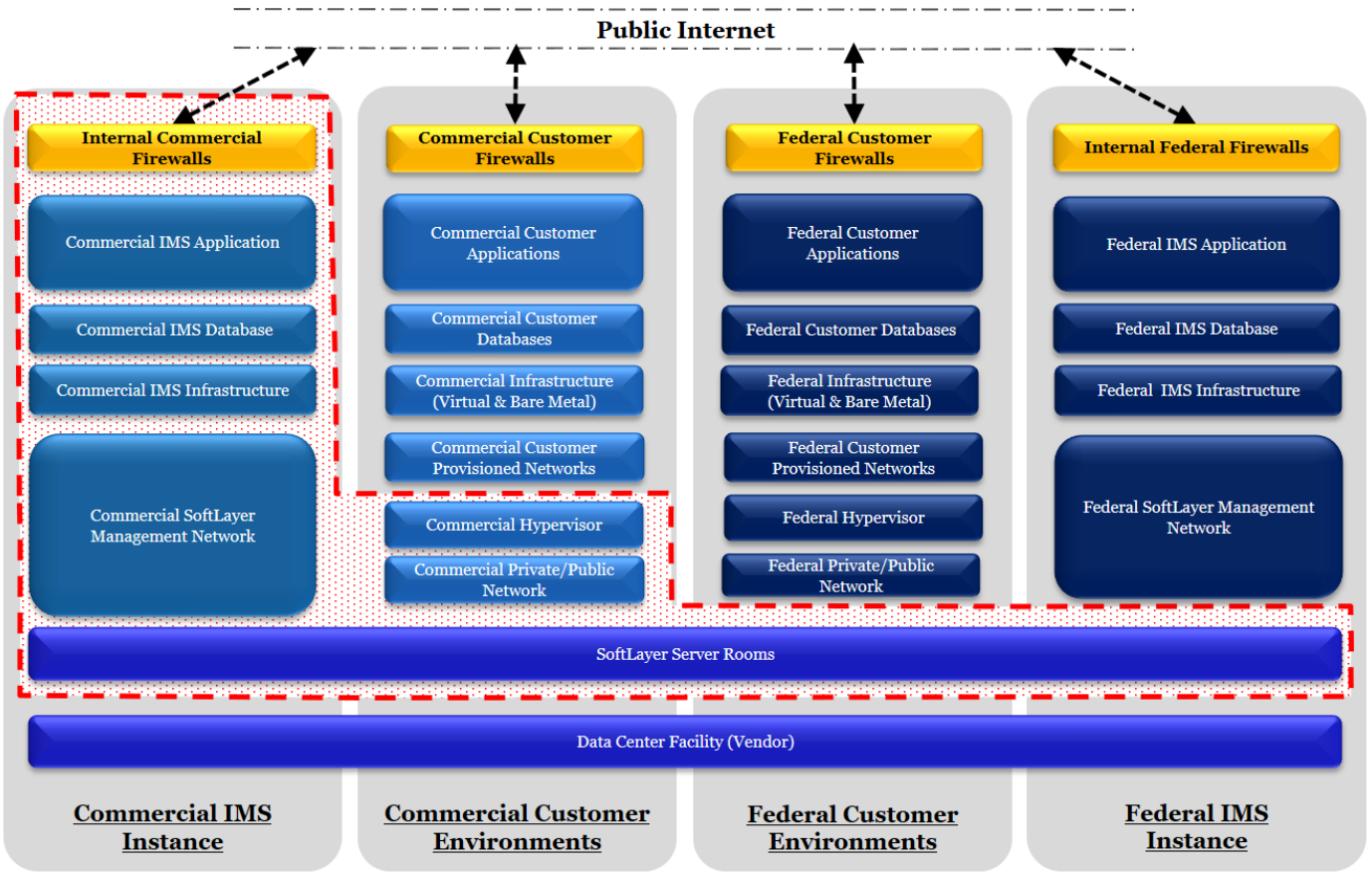
- Create and manage tickets for incident response and resolution
- Review account information
- View information and certain configuration data regarding their purchased solutions
- Perform functions such as OS reloads, and access RescueLayer
- Maintain customer provisioned firewall and DNS configurations that affect their bare metal servers
- Purchase or upgrade services to initiate the automated provisioning process for new systems

Customers build their environments using virtual servers and/or bare metal servers.

IBM Cloud IaaS personnel also have access to IMS to set up and configure purchased solutions, assist in troubleshooting technical issues, and respond to customer requests.

## Scoping

**IBM Cloud Infrastructure as a Service (IaaS) SOC 1 Scope**




***Area within the dashed line is within the scope of this report.*

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

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

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

***Networking***

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

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

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

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

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

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

***Storage***

- **IBM Cloud File Storage** is a flash-backed NFS-based file storage system that allows customers to increase storage capacity and adjust performance based on workload demands.
- **IBM Cloud Block Storage** is a persistent storage option available for Cloud Virtual and Bare Metal Servers.
- **IBM Cloud Backup** is a recovery system the customer manages, enabling customer to securely backup data between IBM servers in one or more IBM Cloud data centers.
- **IBM Cloud Object Storage (IaaS)** is a cross-regional, unstructured, scalable, and persistent data storage service designed to support exponential data growth.
- **Storage Area Network (SAN)** is architected to attach remote computer storage devices to servers in such a way that, to the operating system, the devices appear as locally attached.

***Compute***

- **IBM Cloud Bare Metal** is a dedicated physical server. Bare metal servers allow direct access to physical hardware to support high demand and processor-intensive workloads.
- **SAP-Certified Cloud Infrastructure** is a dedicated physical server purpose-built for SAP workloads.
- **IBM Cloud Virtual Servers** are computing "instances" that are a complete computing environment that includes a full hardware and software stack accessed and controlled over the Internet. The computing resources can be scaled on demand, adding or resizing instances as needed, but without having to purchase physical systems. Public and private virtual nodes are available.

***Security***

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

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

IBM Cloud IaaS provides services to the Federal government and Department of Defense (DoD) via the FedRAMP and Defense Information Systems Agency (DISA)/DoD programs in two data centers (DAL08 and WDC03). A separate instance of IMS (FedIMS) provides provisioning functionality and infrastructure management. These data center facilities are included within the physical security scope of the system, however, other aspects of the services including the FedIMS system and its processes, are not included within the scope of the report.

The accompanying description includes only those controls directly impacting IBM Cloud IaaS and customers' hosting environments utilizing IBM Cloud IaaS services detailed in this report. IBM Cloud IaaS also provides enterprise-class tools to help mitigate potential security risks and ensure availability. Tools provided by IBM Cloud IaaS include, but are not limited to, load balancing, intrusion detection and prevention, standard and dedicated hardware firewalls, anti-virus, anti-spyware, anti-malware, VeriSign® and GeoTrust® SSL Certificates. This report does not extend to controls over IBM Cloud IaaS's other services and tools.

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

<table>
<tr><th>Service Offering</th><th>Data Center / Hardware Locations</th><th>Network</th><th>Operating System Infrastructure</th><th>System Software</th><th>Applications</th><th>Customer Data</th></tr>
<tr><td rowspan="3">IBM Cloud IaaS</td><td rowspan="3">51 data centers<br>(See In-Scope Data Centers section below)</td><td>Customer provisioned and managed network devices, firewalls and VPNs are solely the responsibility of the customer and are not within the scope of the system.</td><td colspan="3" rowspan="2">Customer environments (including the development and maintenance) provisioned and managed using the Customer Portal, including OS, system software, and applications are solely the responsibility of the customer and are not within the scope of the system.</td><td rowspan="3">Customer data is solely the responsibility of the customer and is not within the scope of the system.</td></tr>
<tr><td>Network devices supporting customer managed environments and managed by IBM Cloud IaaS are within the scope of the system including:<br>Routers, Switches, Firewalls, VPNs</td></tr>
<tr><td>Network devices directly in support of the IMS portal are within the scope of the system including:<br>Routers, Switches, Firewalls, VPNs</td><td>Operating systems directly in support of the IMS portal are within the scope of the system including:<br>Linux, UNIX, Windows</td><td>System software directly in support of the IMS portal are within the scope of the system including:<br>Radius, Citrix, Active Directory</td><td>Internal Management System (IMS)/ Customer Portal</td></tr>
</table>

### *In-Scope Data Centers*

IBM Cloud IaaS provides infrastructure as a service using multiple telecom service providers for backbone connectivity and multiple co-location management providers for data center facility management. Refer to the table below for a list of data center vendors that provide facility management services in the IBM Cloud IaaS facilities included within the scope of the system.

| Facility | Physical Location | Facility Manager |
|---|---|---|
| AMS01 | Amsterdam, Netherlands | Capitaland |
| AMS03 | Almere, Netherlands | NL\|DC |
| CHE01 | Ambattur, India | TATA |
| DAL02 | Dallas, TX | SoftLayer |
| DAL05 | Dallas, TX | Digital Realty |
| DAL06 | Dallas, TX | SoftLayer |
| DAL08 | Richardson, TX | Digital Realty |
| DAL09 | Richardson, TX | Digital Realty |
| DAL10 | Irving, TX | QTS |
| DAL12 | Richardson, TX | Digital Realty |
| DAL13 | Carrollton, TX | Cyrus One |
| FRA02 | Frankfurt, Germany | Cyrus One |
| FRA04 | Frankfurt, Germany | E-Shelter |
| FRA05 | Frankfurt, Germany | Interxion |
| HKG02 | Hong Kong, China | Digital Realty |
| *HOU02 | Houston, TX | SoftLayer |
| LON02 | Chessington, London | Digital Realty |
| LON04 | Farnborough, UK | Ark Data Centres |
| LON05 | Hemel Hempsted, UK | NTT |
| LON06 | Slough, UK | Cyrus One |
| MEX01 | Queretaro, Mexico | Equinix |

| Facility | Physical Location | Facility Manager |
|---|---|---|
| MIL01 | Milan, Italy | DATA4 |
| MON01 | Montreal, Canada | COLO-D |
| OSA2X | Osaka, Japan | IDC Frontier |
| *OSL01 | Oslo, Norway | EVRY |
| PAR01 | Paris, France | Global Switch |
| PAR04 | Paris, France | Global Switch |
| PAR05 | Paris, France | BNPP |
| PAR06 | Paris, France | BNPP |
| SAO01 | Sao Paulo, Brazil | Ascenty |
| SAO04 | Santana de Parnaíba, Brazil | Odata |
| SAO05 | Sao Paulo, Brazil | Acenty |
| SEO01 | Gyeonggi-do, South Korea | SK C&C |
| SJC01 | Santa Clara, CA | Digital Realty |
| SJC03 | Santa Clara, CA | Digital Realty |
| SJC04 | San Jose, CA | Stack Infrastructure |
| SNG01 | Jurong East, Singapore | Digital Realty |
| SYD01 | Sydney, Australia | Global Switch |
| SYD04 | Erskine Park, Australia | Digital Realty |
| SYD05 | Sydney, Australia | Equinix |
| TOK02 | Tokyo, Japan | @Tokyo |
| TOK04 | Saitama, Japan | Softbank |
| TOK05 | Tokyo, Japan | NTT |
| TOR01 | Ontario (Markham), Canada | Digital Realty |
| TOR04 | Ontario, Canada | ServerFarm |
| TOR05 | Ontario, Canada | Digital Realty |
| WDC01 | Chantilly, VA | Digital Realty |

| Facility | Physical Location | Facility Manager |
|---|---|---|
| WDC03 | Ashburn, VA | Digital Realty |
| WDC04 | Ashburn, VA | Digital Realty |
| WDC06 | Ashburn, VA | Raging Wire |
| WDC07 | Ashburn, VA | Sabey |

** Note: For purposes of the reporting period 11/1/2021 - 10/31/2022, there were 51 data centers. However, two (2) were decommissioned during the period (HOU02 and OSL01).*

Customers with bare metal, virtual, or hybrid environments can access the servers remotely (electronically) from anywhere in the world. Certain facilities (i.e., DAL02 and and HOU02) house both co-location servers and IaaS related servers. Co-location customers do not have logical or physical access to the IBM Cloud IaaS system. As such, co-location cages housing customers' servers are not included within the scope of the report.

**Relevant Aspects of the Internal Control Framework**

IBM's Framework of Internal Control (FIC) is based on the 2013 COSO (Committee of Sponsoring Organizations of the Treadway Commission) Framework which is comprised of Entity Level Controls (ELCs) that are enterprise wide and have a pervasive effect toward the achievement of IBM's operating, reporting, and compliance objectives while guarding against inherent risks.

IBM's ELCs have been mapped to components and principles of COSO 2013. Each of the five components and relevant principles must be present and functioning.

Examples of ELCs are Board of Directors, Codes of Conduct, Background Due Diligence, HR Policies to Recruit, Develop, Compensate & Separate, Reporting Channels & Investigations, Management Self-Assessment of Control, and Internal Audit.

## *A. Control Environment*

### *Board of Directors (Executive Management Oversight)*

IBM's Board of Directors is responsible for the supervision of the overall affairs of the Company. The Board holds periodic meetings during the year.

The Board adheres to governance principles, as specified in a set of Corporate Governance Guidelines. Board members are selected based on their business or professional experience, the diversity of their background, and their array of talent and perspectives. The Board is composed of a majority of independent members who are elected by the company's shareholders.

The Board has delegated certain authority to three key committees (Audit Committee, Directors and Corporate Governance Committee, Executive Compensation and Management Resources Committee), which are composed entirely of independent directors. Each committee has a written charter and reports regularly to the Board.

IBM's Audit Committee assists the Board with oversight of the integrity of the Company's financial statements, compliance with legal and regulatory requirements, the independent accountant's qualifications and independence, and the performance of the internal audit function and IBM's independent accountant. In addition, the Committee periodically reviews IBM's enterprise risk management framework. Members of the Committee are non-management directors who, in the opinion of the Board, satisfy the independence criteria established by the Board and the standards of the SEC and the NYSE. The Committee reports directly to IBM's Board of Directors and includes at least one Financial Expert, as defined by the rules of the SEC.

The Committee reviews the scope of the audit plan, as well as the summary of the results, and the adequacy of the system of internal control.

The Committee reviews the implementation of IBM's Business Conduct Guidelines and the process to monitor compliance through education and employee certification.

***Background Due Diligence***

Hiring qualified candidates, who also meet high standards of business integrity, is fundamental to IBM's workforce quality and performance, and ultimately its success. To support this objective of consistent resource quality worldwide, IBM's hiring practices mandate minimum criteria that each potential candidate must meet. A key component of IBM's hiring process is an established set of Global Employment Verification Standard (GEVS) criteria applicable to regulars, non-regulars (fixed term, supplemental) and interns / students. A reduced set of criteria is applicable to transitioning employees from acquisitions and outsourcing deals.

The following verification criteria are mandatory for candidates being considered for IBM employment:

- Government Relationships (prior to offer)
- Restricted and Sensitive Hiring List (prior to offer)
- Rehire Eligibility (prior to offer)
- Non-Compete Clause (prior to offer)
- Denied Parties List (prior to offer)
- Export Regulations Control Review (prior to start date)
- Criminal Background Check (prior to start date), where legally permissible

- Proof of identity (prior to or on start date)
- Work authorization / Residence Permit (prior to or on start date)
- Confirmation of Academic Achievement for Early Professional Hires

IBM's offer of employment is conditional upon successfully meeting these verification criteria. There may be specific country-level verification and exception criteria that must also be assessed based on local statutory requirements, inherent country risk factors, industry practices or known contractual requirements.

Contractors:

Similar to background checks for IBM employees, suppliers that provide contract personnel are required by procurement contract terms to perform background checks prior to providing the contractor to IBM.

### *HR Policies to Recruit, Develop, Compensate, and Separate*

IBM's centralized personnel policies and procedures are designed to recruit, develop and retain competent and trustworthy employees who facilitate an effective internal control system and support competitive success. The Human Resources (HR) function manages global HR design and strategy, delivers HR programs and provides support across all HR-related specialties. Global Administration provides administrative support on a global basis to executives, management and staff.

IBM has a long-standing commitment to equal opportunity due to its recognition that a diverse workforce is fundamental to its competitive success. IBM's documented Workforce Diversity and Inclusion Policy (Corporate Policy 117) requires that activities such as hiring, promotion and compensation be conducted without regard to race, color, religion, gender, gender identity or expression, sexual orientation, national origin, genetics, pregnancy, disability, age, veteran status, or other characteristics. Furthermore, IBM policy states that the workplace environment is to be free of harassment and reasonable workplace accommodations are to be made for the disabled, in accordance with applicable laws.

Talent Acquisition

IBM selects appropriately qualified applicants based on business needs, job-related requirements as per stated job descriptions/positions, and assessment of each applicant's individual qualifications and skills.

Talent Development and Training

IBM offers a compelling and transparent career experience where employees know the career options available to them, and how to accelerate their career growth and progression. IBM identifies and focuses employee development on skills that are most relevant and valued by the market. Employees have access to insight into the skills most valued and are actively encouraged to gain skills of the future to grow and advance. Cultivating these market-valued skills supports IBM staying competitive in the market.

As part of learning their job responsibilities, employees improve their organizational capabilities through “hands-on” training, utilizing documented functional guidance, corporate directives and desk procedures. Employees are cross-trained, as appropriate, to facilitate adequate back-up coverage.

The IBM "Your Learning" platform provides employees with a centralized digital learning platform by aggregating learning from across multiple internal and external sources. The platform provides personalized learning recommendations based on the learner's profile and learning transcript history, while at the same time allowing them to customize the space by choosing what learning is most relevant for their performance, development needs and continuous career building.

New Hire Orientation

As part of the on-boarding process, new hires attend an induction session (Start at IBM) that gives them an understanding of IBM’s culture, values, an organization overview, and what it means to be an IBMer. The session also covers the importance of one’s career and the tools and resources available to support their career journey.

Performance Based Compensation

Checkpoint is IBM's performance management process that favors speed and innovation and cultivates a high-performance culture. The program is based on three (3) key actions: Create Goals, Exchange of Feedback, and Annual Assessment.

The process aligns all employees globally with IBM's strategy and values based on the principle that IBM's success depends on employee’s achievement of Checkpoint goals that link directly to IBM’s business objectives. Employees are empowered to be in control of their goals which reflect their work, business direction and the five (5) dimensions (Business Results, Client Success, Innovation, Responsibility to Others, and Skills), which are built on the foundation of IBM’s Values and Practices.

The core of Checkpoint is ongoing feedback, including updating goals as necessary, which gives managers meaningful insights into IBMers’ work and enables alignment.

Managers perform a year-end assessment using a three-point rating scale for each dimension (Exceeds, Achieves, Expects More) based on expectations for the role and band.

Separation

The Global HR Separation Standard establishes a process for separation procedures for all employee categories (Regular and Complementary including Executives) and specifies adherence to corporate security instructions and standards.

### *IT Security*

IBM IT Security requirements align with the roles and responsibilities of the IBM Chief Information Security Office (CISO) and the Business Information Security Officers (BISOs), and the Cybersecurity Advisory Committee (CAC). IBM's IT Security requirements are intended to mitigate risk, to minimize or eliminate the loss or misuse of information critical to IBM's business, and to prevent the disruption of IBM's business operations due to unauthorized or excessive access to our information technology services and assets.

IBM's IT Security Standard (ITSS) establishes the principles and requirements for the protection of IBM worldwide IT systems and the information they contain. The standard applies to all IBM operating units, corporate staffs and subsidiaries, without exceptions; however, IT assets, including infrastructure, that are dedicated to a single IBM customer are outside the scope of this standard when the protection requirements are established by the customer.

Workstation Security

IBM has a policy governing workstation security compliance. IBM workstations employ diagnostic tools that check for core workstation security features which automatically correct issues or notify employees of non-compliance to drive manual corrections. These checks include: hard drive security (password protection or full disk encryption); screen saver; antivirus; firewall; database encryption, if required based on data sensitivity; user account passwords; service pack level and security patch currency; as well as verification that certain features are not enabled such as file-sharing capabilities.

Data Privacy & Tech Ethics

The Chief Privacy Office oversees IBM's overall privacy strategy and tech ethics governance. Corporate Policies and guidelines that address data privacy, including the collection and processing of personal information, and tech ethics are in place.

Privacy Advisory Committee (PAC) is a board-level senior executive committee that coordinates IBM's actions to address strategic and operational issues relating to privacy and tech ethics. The PAC serves as an accelerant for privacy-related policy-level decision-making within IBM and is governed by a charter, that is maintained by the Chief Privacy Office.

Physical Security

Access to IBM facilities is generally restricted through the use of a badge access system.

### *Codes of Conduct*

IBM's Business Conduct Guidelines (BCG) define the standards of acceptable business conduct for all IBM employees worldwide, including but not limited to topics such as: anti-bribery, gifts and amenities, competition, conflict of interest, intellectual property, books and records, working with third parties, etc.

IBM reviews and updates the BCG content annually in order to comply with IBM policies, regional laws and regulations, and external guidance. Employees certify that they have read and will comply with the IBM BCG as new employees and re-certify annually thereafter. The certification process, including completion of a BCG education course, is tracked by both Trust & Compliance Office and the employee's manager.

IBM endorses the Responsible Business Alliance (RBA) Code of Conduct for its own operations and extends a requirement for RBA code conformance to its direct suppliers of goods and services. The Code encourages participants to go beyond legal compliance, drawing upon internationally recognized standards, in order to advance social and environmental responsibility and business ethics in the areas of Labor, Health and Safety, Environment, Ethics, and Management Systems. The RBA Code represents the minimum social responsibility standards IBM expects of their suppliers as a condition of doing business with them.

IBM requires all suppliers to sign an RBA Letter Agreement demonstrating their commitment to adhere to the RBA Code.

### *Reporting Channels and Investigations*

IBM's Employee Concerns is the place to raise a concern regarding non-inclusive or inappropriate behaviors, report a violation of the IBM Business Conduct Guidelines, or give your point of view about an IBM policy, practice or program which is impacting the broader IBM population. The following issues can be raised through Employee Concerns: 1) An issue or decision which affects an employee personally, or where they feel they have been unfairly or inappropriately treated, or if they have witnessed inappropriate treatment of an individual in the IBM workplace. 2) Reporting a violation (or suspected violation) of the IBM Business Conduct Guidelines involving financial reporting, compliance and controls, or other unethical or unlawful conduct; 3) A point of view about a workplace policy, practice or program in IBM which is impacting the broader IBM population. The process allows for an employee to raise concerns anonymously.

The "Talk it Over@IBM" channel is available to anyone who works in an IBM workplace to discuss their concerns with an HR professional about situations related to non-inclusive behaviors - such as harassment, discrimination, bullying and other inappropriate behaviors.
The geography investigations manager submits allegations for review to the Allegation Review Board (ARB), which is composed of CA&AS, HR and Legal. The ARB is responsible for reviewing each allegation it receives to determine the appropriate course of action.

Corporate Assurance and Advisory Services (CA&AS) is responsible for investigating matters involving alleged violations of IBM's Business Conduct Guidelines related to financial recording and reporting, business processes and inappropriate use of assets.

The geography investigations manager submits allegations for review to the Allegation Review Board (ARB), which is composed of CA&AS, HR and Trust & Compliance (T&C). The ARB is responsible for reviewing each allegation it receives to determine the appropriate course of action.

If an investigation identifies a financial statement impact or involves matters of a sensitive nature, the resulting disciplinary action recommendation must also be reviewed by a CHQ panel whose members include: the Vice President, HR Services; the Chief Auditor; and Legal. Senior line management, in concert with the appropriate staff functions, retains responsibility for recommending, formulating, implementing and communicating the status of any disciplinary actions.

On a quarterly basis, as part of CA&AS' centralized investigations program, the Audit Committee is provided a report detailing the nature, status and disposition of substantiated CA&AS investigations that have a financial statement impact.

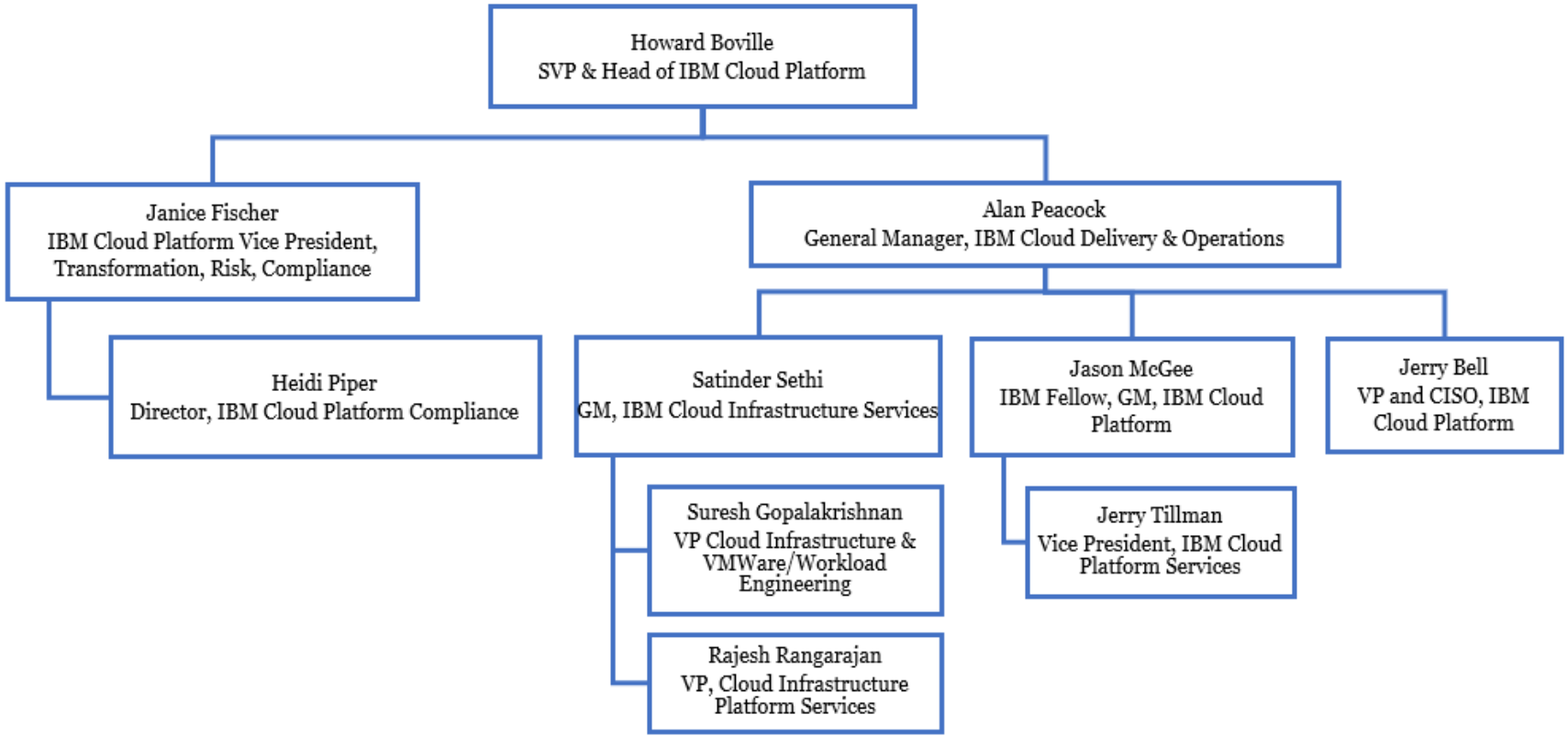
### *Organization and Administration*

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 IaaS leverages participation from multiple organizational levels, sites, locations, and geographies, and organizations are involved, as required, to perform the day-to-day oversight of service delivery related functions, matters, responsibilities and issues. Functional roles may be combined within management positions to deliver contracted services in a cost-effective manner. IBM Cloud IaaS may distribute some portion of its development and operations processes to IBM locations around the world, when permissible.

The IBM Cloud IaaS 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 controls, as a part of the Security Steering Committee.

***IBM Cloud Organizational Chart as of October 31, 2022***



## *B. Risk Assessment*

IBM Cloud IaaS performs IT risk assessments on a periodic basis to ensure system risks related to security and availability are identified, tracked, and addressed as necessary.

IT risk assessments over the system are documented, reviewed, and approved on an annual basis, and include the following information:

- Determining business objectives including security commitments
- Evaluating the effect of environmental, regulatory, and technological changes on IBM's security
- Identifying threats to operations, including security threats, using information technology asset records
- Analyzing risks associated with the threats
- Determining a risk mitigation strategy that contemplates the risk of fraud, including the incentives, opportunities, and potential rationalizations
- Developing or modifying and deploying controls consistent with the risk mitigation strategy

IBM Cloud IaaS maintains a Risk Assessment Policy, which documents the Risk Management Life Cycle (RMLC) that IBM Cloud IaaS follows to identify, assess, mitigate, and monitor risk for its IaaS. The RMLC consists of a Risk Assessment that includes Risk Acceptance Criteria, Risk Treatment, and Reporting and Monitoring.

On an annual basis, the VP of Risk Management coordinates the RMLC. Designated Risk Assessors complete the Risk Assessment by documenting assets (documents, applications, databases, people, equipment, infrastructure, external services, etc.) and their associated threats and vulnerabilities. Asset owners are responsible for alerting the Trust and Assurance team to any identified risks during the course of operation. Each asset is assigned a score based on the criteria of consequence severity and probability of the risk occurring. Based on the final score, each associated risk is determined to be either acceptable or unacceptable. Unacceptable risks go through the Risk Treatment process to identify options to either transfer or avoid the risk. If neither option is feasible, a Risk Acceptance is documented.

All existing Risk Acceptances are reviewed on an annual basis to determine if the risk can be mitigated. The Risk Assessors are responsible for monitoring the progress of implementation against the Risk Treatment plan and reporting the results to the VP of Risk Management. The Risk Assessment does not extend to routine development initiatives classified as standard or custodial that maintain the Company's operations.

### *Vendor Risk Assessment and Management Process*

Contracts with vendors and business partners must be documented via formal legal agreements between IBM Cloud IaaS and the service provider. Vendors include the data center facility providers for the in scope physical locations, as IBM Cloud IaaS contracts with a variety of data center vendors to provide the physical data center sites where hardware is located.

As IBM Cloud IaaS retains ownership of the physical controls within the scope of this report through monitoring each physical environment and the actions of each facilities management vendor, the vendors are not considered subservice organizations necessary, within the scope of the IBM Cloud IaaS system, to achieve the related control objectives. IBM Cloud IaaS employed site managers are assigned for in-scope data centers. The facility management vendors are in continuous contact with the IBM Cloud IaaS Site Managers through the real estate managers and facility engineers communicating via the Portal and e-mail notifications.

## *C. Information and Communication*

### *IBM Communications Management*

IBM Cloud IaaS executives are responsible for setting the tone at the top. Messages are reinforced through periodic town hall meetings, which are conducted by senior IBM Cloud IaaS executives for the benefit of all employees.

Various direct and indirect methods of communication are implemented by management to ensure employees understand the policies, procedures, standards, and guidelines developed and their individual roles and responsibilities. Examples of these methods include orientation and training for new employees, e-mails, ongoing training, distribution of policies and procedures, and on-the-job training. Monthly management meetings are also utilized as a communication means to the company.

The facility management vendors are in constant contact with the IBM Cloud IaaS Site Managers through the real estate managers and facility engineers. In addition, a portal is available for tickets and issues between IBM Cloud IaaS and the facility management vendors. The facility management vendor communicates with IBM Cloud IaaS through the Portal and e-mail notifications.

## *D. Monitoring of Controls*

### *Management Self-Assessment of Control*

IBM's Management Self-Assessment of Control (MSAC) is a formal and comprehensive approach to identify, monitor and manage potential control risk. As part of the control assessment, management validates the design and effectiveness of internal controls, promoting early identification of emerging or changing risks.

### *Corporate Assurance and Advisory Services*

An IBM Corporate Directive defines the mission and responsibility of Corporate Assurance and Advisory Services (CA&AS), and grants CA&AS the authority necessary to assess the control posture of IBM. IBM's senior management and the Audit Committee support CA&AS' mission by enabling the organization to be adequately staffed with the appropriate skills and engagements to be performed on an independent basis. Independence is assured through CA&AS' reporting structure. The Chief Auditor reports administratively to the Chief Financial Officer but is accountable to the Audit Committee.

CA&AS uses a planning methodology comprised of both a risk model which includes fraud risk considerations and a coverage operating model resulting in an annual plan which is a prioritization of a well-defined audit universe. For all engagement types, CA&AS monitors and tracks line management's implementation of recommendations to address audit concerns (findings) until closure.

A Risk Taxonomy was developed with input from those functions representing the three lines model adapted from The Institute of Internal Auditors (IIA): 1) Global Process Owners; 2) Business Controls and Enterprise Risk Management; and 3) CA&AS. The taxonomy, which is owned and managed by CA&AS, identifies risk areas for IBM's business processes and assigns a high, medium or low risk level for each area. CA&AS Programs are aligned with the defined taxonomy risk areas.

CA&AS conducts an extensive training and education program to develop and maintain auditing skills to provide CA&AS personnel with the necessary education and expertise to execute their responsibilities.

### *Trust and Assurance Team*

The Trust and Assurance team is a part of IBM Cloud IaaS's Risk Management Department and supports the IBM Cloud IaaS-wide compliance efforts by monitoring compliance and conducting communication, training, and awareness initiatives in response to contractual and regulatory requirements. The Trust and Assurance team develops and maintains IBM Cloud IaaS-wide policies and makes them available to IBM Cloud IaaS personnel. Additionally, the Trust and Assurance team monitors non-compliance issues and remediation efforts to ensure issues are resolved according to an approved plan.

### *Controls*

IBM Cloud IaaS has adopted the Key Controls over Operations (KCO) methodology in order to improve the effectiveness of IBM Cloud IaaS's controls system through standardization and identification of common key control points with established testing criteria. This process utilizes established frequency and sample size requirements for the testing of each control point. This was adopted to streamline and improve the efficiency of IBM Cloud IaaS's controls system and to model the Sarbanes-Oxley approach for key operational controls for IBM Cloud IaaS.

Results of the KCO testing are reported to IBM Cloud IaaS management and entered into the Worldwide Controls Database managed by IBM Corporate Headquarters. The controllable units tested receive a report of findings from the KCO testing and are responsible for developing and implementing an action plan to address the findings.

## *E. IBM Cloud IaaS's Control Activities*

The description that follows outlines the processes and controls that are performed by IBM Cloud IaaS for its customers. This should be read in conjunction with the detailed control objectives and control activities described in Section IV that are intended to be incorporated herein by reference.

**Transaction Flow Diagram**

| | *Initiated* | *Authorized* | *Recorded* | *Processed* | *Corrected* |
|---|---|---|---|---|---|
| ***Access Administration*** *Physical and Logical* | User access request initiated by IBM Cloud IaaS (e.g., a standardized request form for employee, visitor, or contractor). | Required authorization(s) obtained from IBM Cloud IaaS in accordance with the defined security policy. | Request recorded in Human Resources Distribution email or IMS. | Request processed by IBM Cloud IaaS and notification is sent. | Corrective action is performed by IBM Cloud IaaS (e.g., addition or removal of privileges requires a new request to be initiated, authorized, recorded and processed). |
| ***Logical Security*** *Passwords* | Password parameters are set in accordance with the defined security policy. | Required password parameters and settings are defined and authorized. | Parameter configurations are recorded in a common toolset (e.g., Active Directory, IMS). | Parameter configurations are pushed to devices at a defined interval (e.g., AGPO, Chef, etc.). | Corrective action is performed by IBM Cloud IaaS (e.g., settings updated every 5 mins, etc.). |
| ***Logical Security*** *User ID Revalidations* | Revalidation initiated in accordance with the defined security policy (e.g., periodic continuous business need). | Obtain current authorized user listing (e.g., provided manually or extracted via a script). | User IDs are recorded in common toolset (e.g., Active Directory, IMS, etc.). | Revalidation processed (e.g., comparison of listings, confirmation). | Corrective action is performed by IBM Cloud IaaS (e.g., request for removal of access). |
| ***Change Management, Incident Management,*** *and* ***Computer Operations*** | Request initiated by IBM Cloud IaaS or customer (e.g., change ticket, incident ticket). | Required authorization(s) obtained from IBM Cloud IaaS in accordance with the defined security policy. | Request recorded in a common toolset (e.g., IMS, JIRA, etc.). | Request processed by IBM Cloud IaaS in accordance with the defined security policy. | Corrective action is performed by IBM Cloud IaaS (e.g., subsequent approval of ticket). |

**Physical Security**

Each data center building may contain multiple server rooms (SR), which are designated as separate areas of the data center, whether separated by a cage or through a room enclosure. Each server room is typically made up of one pod and built to the same specifications to support up to 5,000 servers. Leveraging this standardization across geographic locations, IBM Cloud IaaS optimizes key data center performance variables including: space, power, network, personnel, and internal infrastructure.

Physical access is controlled through key card proximity systems at each facility and server room. Access to and throughout each facility, including sensitive areas, such as electrical, generator, UPS, batteries, fire riser/sprinkler, and HVAC equipment is restricted and server room access is limited to authorized personnel. Each facility except DAL02, DAL06, HOU02, PAR01 and SYD01 has two-factor authentication with a biometric system and require a key card. The facilities noted above are also restricted but only require key card authentication.

Each data center has a full-time IBM Cloud IaaS site manager on-site. The site manager and members of the facility teams are responsible for monitoring the IBM Cloud IaaS server rooms on a daily basis and reporting any compromised access or environmental issues to the facility vendor for remediation. The vendors monitor the physical access systems centrally at each location and will alert the IBM Cloud IaaS site manager to any unauthorized access attempts. Major events are communicated by the IBM Cloud IaaS site manager to the central IBM Cloud IaaS Facilities Team.

Surveillance cameras are strategically located within in each data center to deter unauthorized access. Security personnel monitor key card access throughout the building in real time and address any issues, such as emergency doors ajar, doors left open, and failed access attempts. Security events are communicated to the IBM Cloud IaaS site manager and to the central IBM Cloud IaaS Facilities Team, as necessary.

IBM Cloud IaaS personnel are provided physical access based on their job responsibilities. Access to data centers for new hires and transfers is formally requested and requires approval based on job responsibility and location. Approved new hire access requests are sent to the IBM Cloud IaaS Facilities Team to provision access to IBM Cloud IaaS managed facilities. For vendor owned sites, approved requests are sent to the respective vendors to provision access. Physical access privileges are reviewed on a quarterly basis to verify access is appropriate. When an IBM Cloud IaaS employee is terminated, HR sends a notification to responsible personnel and access privileges are revoked by the Facilities Team for IBM Cloud IaaS sites and the facility vendors for vendor owned sites upon termination.

Individuals requiring access to the data center without an authorized key card, such as visitors, customers, contractors, or vendors must sign in at the security desk or with the Data Center Control Room (DCR). Visitors are required to be escorted by authorized personnel. The individual must provide a valid government issued photo identification card for identity verification. Visitors at data centers are required to wear identification cards to distinguish the person as a visitor. Temporary key cards are disabled after a predefined time, typically a 24-hour period.

**Change Management**

The overall change management process addresses implementations that may potentially impact the environment and includes changes to infrastructure and systems. The change management process does not include changes to customers' virtual servers, bare metal servers or customer managed network devices.

IBM Cloud IaaS is responsible for implementing changes in the IT environment including changes to individual components (e.g., equipment, systems and applications software, procedures and environmental facilities) and coordination of changes across all components (collectively, "Change Management").

To minimize the likelihood of disruption, unauthorized alterations and errors, control over the IT process of managing changes is facilitated by a management system that provides for analysis, implementation, and follow-up of all changes requested and made to the existing IT infrastructure. Existing controls take into consideration the identification, and prioritization of changes, emergency procedures, impact assessment, and change authorization.

***Changes to IMS and IMS Infrastructure Devices***

Changes are subject to approval and testing prior to implementation. Both disruptive and non-disruptive changes require a formal change record, which is managed via the JIRA tool. Testing and back out plans are required for the majority of changes depending on the change type. Certain change types do not require testing or back out plans as testing may not be feasible or relevant. For change types that are subject to testing, each change passes through the dev/staging environment for testing, and will not progress to production deployment until testing is approved. Where applicable, back out plans are documented within the JIRA record.

Changes in JIRA are assigned through an automated workflow that prevents the change from progressing until each required step is completed. Depending on the change type and impacted environment, the number and level of required reviewers and approvers may differ. Verbal approval from management prior to implementation is acceptable for emergency/expedited changes. However, documented approval must be provided after implementation. Routine changes to the infrastructure that do not have an impact on customer service are pre-approved therefore do not require approval within the change record.

Change windows/maintenance schedules are distributed via notifications in the Customer Portal to notify users of upcoming changes and outages. For individual changes that may impact/disrupt the production environment, JIRA ticket owners prepare customer facing statements that are communicated to the Network Operations Center (NOC) for distribution.

### *Changes to Network Devices*

Changes to the network are made through the console by Network Engineers or via IMS automation. Changes made through IMS tend to be common updates, such as VLAN or subnet modifications.

Console based changes are performed by Network Engineers for non-routine maintenance, configuration, and upgrades. The configurations of these devices are controlled by the Network Engineering Group. Console based changes are documented using Maintenance Operation Protocol (MOP) documents, that include the requested change and the configuration modifications. Changes to the device are made programmatically and change control is monitored by review of the Terminal Access Controller Access Control System (TACACS) log files, a remote authentication protocol.

Depending on the risk and impact of the console-based change, the change management process may vary. Prior to console changes being pushed to production, testing of network changes is performed in a virtual lab environment. Significant network changes are approved before implementation to the production environment. Console based changes are logged via the respective device's logging functionality. Configuration changes are tracked via a Git repository with a versioning history to allow simple views into the changes that were made and back-out, if necessary. Emergency changes for network devices follow a similar process as standard network changes discussed above; the changes are documented, logged, and approved.

When required, maintenance window notifications are distributed internally and to customers regarding an outage and potential for disruption. The network engineer assigned to the project or issue determines the necessity for a notification based on the risk to the security and/or availability of the network device and/or the overall network. Customers are notified of widespread service disruptions through the Customer Portal via notification banners.

## Incident Management

IBM Cloud IaaS's incident response policy covers threat events, threat sources, and scenarios that may affect the security and availability of the company's information assets. The Network Reliability Engineering (NRE) and Security Operations Center (SOC) are responsible for monitoring the IBM Cloud IaaS environment and manage the identification, response, and resolution of incidents. Through the NRE and SOC, IBM Cloud IaaS provides 24/7 monitoring of data centers. IBM Cloud IaaS utilizes a variety of tools, in combination, to monitor, mitigate, and resolve potential issues. Each data center also has its own local Data Center Control Room (DCR), which is used to monitor and resolve potential issues locally.

### *Network Reliability Engineering (NRE) and Security Operations Center (SOC)*

The NRE and SOC are responsible for maintaining the overall operation of the IBM Cloud IaaS environment, involving two broad classes of activities, problem resolution, and coordination. Problem resolution entails being the single point of contact for infrastructure problems, and coordination occurs when third parties engage with IBM Cloud IaaS regarding operational issues (i.e., scheduled maintenance, interacting with

transit and telecom providers about service, circuit problems, breaches, breaking Master Service Agreement and other unauthorized actions on the system).

The NRE monitors network traffic and operations metrics to identify potential network issues that may disrupt service and impact security. The SOC monitors security alerts to identify potential security issues that may disrupt service and impact security. The NRE and SOC are notified of incidents in a variety of ways:

- E-mail received from public aliases or internal aliases.
- Phone calls from telecom circuit providers, network engineers, customers, peering ISPs, transit providers, data center vendors or other internal groups at IBM Cloud IaaS.
- Review of tickets escalated to the NRE/SOC through the "Network Operations" or "Security Operations" ticket queues.
- The NRE monitors alerts from network monitoring tools using a variety of tools, including PeakFlow, Netcool, Oculus, IP Alert, Nagios, GROK (syslog parser), and Regex. Additionally, the SOC monitors alerts using a variety of tools, including QRadar and FireEye.

The team member that identifies the issue or receives the initial notification of an incident (NRE) or security incident (SOC) creates a ticket unless an existing ticket already exists. NRE tickets are documented in IMS or in ServiceNow as Customer Impacting Events (CIE) and SOC tickets are documented in JIRA as Security Incidents in Progress (SIP). If a ticket regarding the same incident already exists, any new information is documented in the existing CIE or SIP notes. CIEs and SIPs are classified based on criticality. Each CIE and SIP has a clearly defined owner responsible for resolving the incident according to the defined policies.

In addition to documenting the incident and applying standard solutions, CIE and SIP ticket classification further defines the incident's importance and urgency. There are three elements involved in incident classification:

- Scope: How many customers are affected? Incident tickets are classified as Key Account Customer, Individual Data Center, Individual Regional/City Location or Global;
- Severity: How strongly affected those within the incident scope are, with emphasis given to actual incidents over changes made to working networks and services? Severity levels include Loss of Service, Intermittent or Degraded Service, Moderate Service Impact, Change to Service and No Impact; and
- Service: What is the actual service impacted? Services may include network or infrastructure devices, data centers, firewalls, network connectivity, DNS, Exchange Email, and/or web-based activities such as www.softlayer.com or manage.softlayer.com.

Once a CIE or SIP is created, assigned, and classified, the ticket is worked until a resolution is achieved. Incident escalation occurs as necessary at the end of each NRE or SOC shift and when incidents exceed the skill set of the CIE/SIP ticket owner. Internal communications are distributed, when required, by the NRE or SOC for changes that affect system security and availability. Communication of issues or changes affecting security and availability for users are distributed as needed through the Customer Portal.

Closing a CIE/SIP ticket indicates that the incident has been resolved. The following conditions are confirmed by the CIE/SIP owner before a ticket is closed and an issue is deemed resolved:

- Telecom tickets resulting from an outage are confirmed closed with the provider.
- If possible, the problem owner demonstrates and documents in the ticket that the symptoms of the problem can no longer be reproduced.
- The problem owner confirms with an affected party that the problem is resolved. For example, when an NRE technician closes a ticket, a note is placed in the ticket indicating the specific root cause of the outage and the specific action taken to resolve the root cause. In cases that involve a failure in the IBM Cloud IaaS equipment, the NRE Technician also indicates what actions were applied to prevent future failure. This information is used if a Post-incident Review (PIR) is performed.

When a CIE or SIP ticket is recorded, IBM Cloud IaaS notifies and escalates the issue to the relevant affected customers and internal stakeholders, convenes technical and management conference bridges, and brings the appropriate technical skills to bear to resolve the incident.

**Computer Operations**

IMS data is replicated to another geographically separate server to help ensure availability of the Customer Portal (IMS) and certain support services. The Customer Portal and internal IMS functionality is provided via the IMS database. This database uses live replication over a dedicated connection between two geographically redundant sites. In case of a disruption at one site, the other site continues uninterrupted functionality. The IBM Cloud IaaS data engineering team monitors the replication continuously reviewing the GoldenGate replication settings to validate replication is continuously running successfully.

In the event that IMS or the Customer Portal is unavailable, customer systems will be unaffected and continue to operate. Users can continue to operate their existing servers. However, the features of IMS and the Customer Portal would be unavailable, such as the ability to view information or provision additional server instances.

On an annual basis, IBM Cloud IaaS performs a failover test of IMS from the primary location to the secondary location to verify that IMS would still operate in the event the primary site failed. Any necessary remediation over the replication settings is made based on the result of the failover test.

Backing up hosted bare metal and virtual servers and performing restore tests on a periodic basis is not included within the scope of this report.

***Disaster Recovery***

Based on the configuration of IBM Cloud IaaS's "Network-Within-A-Network", with 3 network interfaces, if an outage occurs at a data center on the public network, the traffic will be routed and can traverse through the other established networks to provide continued availability of the server, by routing traffic to another data center and then utilizing the other networks to reach the server.

Also, based on IBM Cloud IaaS's design of the environment, IMS is connected to the customers' bare metal and virtual servers. However, any IMS outage that may occur will not have an impact on the customers' environments. IMS is set up separately from the customers' environments, such that public and private traffic will continue to route if IMS becomes unavailable.

A Disaster Recovery Plan (DRP) has been designed to be used in the event of a disaster affecting IBM Cloud IaaS. A disaster can result from a number of accidental, malicious or environmental events such as fire, flood, terrorist attack, human error, and software or hardware failures. The DRP provides for the identification and response to threats, notification and intercommunication for data center employees and management, procedures to follow during a disaster, damage assessment, and team member roles and responsibilities. The risk assessment includes risks that could impact availability and noted mitigations. The DRP is reviewed at least annually and changes to the procedures are approved.

The decision to initiate disaster recovery procedures will be taken by executive management after assessing the situation following a disaster or crisis. If management decides to initiate IBM Cloud IaaS's disaster recovery procedures, members of the recovery teams are required to follow the procedures contained within the DRP until recovery is complete. A hot-site facility is maintained by IBM Cloud IaaS to help mitigate the risk of downtime.

Specific goals of the plan include, but are not limited to, the following:

- To be operational at the standby facility, as soon as possible, after DR Plan invocation
- To operate at the standby facility until cutback is possible
- To minimize the disruption to core functionality

Two recovery scenarios are developed based on the severity of the damage incurred, minor damage affecting part of the environment or major damage affecting the entire or majority of the environment.

During a recovery, certain teams are deployed including an Operations Team, Network Operations and Engineering Teams, Facilities Teams, and Communications Teams, each with specific responsibilities including the following:

| Operations Teams | Network Operations and Engineering Teams | Facilities Teams | Communications Teams |
|---|---|---|---|
| • Ensuring that the standby equipment meets the recovery schedules.<br>• Providing the appropriate management and staffing of the standby data center, data control, and help desk in order to meet the defined level of user requirements.<br>• Working with the Network Team to restore local and wide area data communications services to meet the minimum processing requirements.<br>• Initiating operations at the standby facility.<br>• Providing sufficient personnel to support operations at the standby facility.<br>• Managing the standby facilities to meet users' requirements.<br>• Establishing processing schedule and inform user contacts.<br>• Arranging for acquisition and/or availability of necessary computer supplies.<br>• Ensuring that documentation for standards, operations, vital records maintenance, application programs etc. are stored in a secure/safe environment and reassembled at the standby facilities, as appropriate. | • Evaluating the extent of damage to the voice and data network and discuss alternate communications arrangements with telecoms service providers.<br>• Establishing the network at the standby facilities in order to bring up the required operations.<br>• Defining the priorities for restoring the network in the user areas.<br>• Ordering the voice/data communications and equipment as required.<br>• Supervising the line and equipment installation for the new network.<br>• Providing necessary network documentation.<br>• Providing ongoing support of the networks at the standby facility.<br>• Reestablishing the networks at the primary site when the post disaster restoration is complete. | • In conjunction with the Information Systems, evaluating the damage and identifying equipment that can be salvaged.<br>• Working with the Networking Team to have lines ready for rapid activation.<br>• As soon as the standby site is occupied, cleaning up the disaster site and securing that site to prevent further damage.<br>• Supplying information for initiating insurance claims. Ensuring that insurance arrangements are appropriate for the prevailing circumstances (i.e., any replacement equipment is immediately covered etc.).<br>• Preparing the original data center for re-occupation.<br>• Maintaining current configuration schematics of the Data Center (stored off site) This should include:<br>o Air conditioning,<br>o Power distribution,<br>o Electrical supplies and connections,<br>o Specifications and floor layouts,<br>o Controlling security within the disaster area,<br>o Arranging for necessary office support services, and<br>o Managing staff safety and welfare. | • Working with Management to obtain directives on the messages to communicate.<br>• Making statements to local, national and international media, as appropriate.<br>• Informing suppliers and customers of any potential delays.<br>• Informing employees of the recovery progress of the schedules.<br>• Ensuring that there are no miscommunications that could damage the image of the company.<br>• Any other public relations. |

## Logical Security

### *Security Policy Definition*

The Sr. Director, Trust and Assurance develops and maintains enterprise-wide policies and communicates policy updates to IBM Cloud IaaS personnel responsible for implementing such policies via monthly Management Meetings. Management has approved policies regarding security and availability. Senior Management approves policies prior to release. Policies are reviewed and updated on an annual basis by the Compliance team or the responsible business unit.

Customers are responsible for implementing any additional measures to ensure security beyond what is noted in the Cloud Services Agreement (CSA).

### *Customers Access to Customer Portal (IMS)*

Customer interactions with the Customer Portal (IMS) are restricted based on the authorization level required by the user. If the user is a "master" (a user with privileges granted to a customer using the Portal), that user can create other user accounts with varying levels of authorization. This includes the creation of other master users based on the customer's requirements.

Customer users are required to have a unique login and password. Minimum password parameters exist for customer access to the Customer Portal. Within IMS, the customer manages the users within their respective organization and related permissions.

Specifically, the following controls are not within the scope of the report:

- Managing and reviewing customer access to IMS;
- Verifying that only authorized and properly trained customer personnel are allowed logical access to IBM Cloud IaaS systems via the provided IBM Cloud IaaS logins, including the mobile website and mobile applications, and the IBM Cloud IaaS provided VPN; and
- System access to the Customer Portal and hosted equipment (servers) is appropriately administered by user entities:
    - Passwords are changed periodically,
    - Passwords are kept confidential,
    - Security violations are monitored and followed up as necessary,
    - Provisioning of new customer users and granting of additional customer access permissions are properly authorized, and
    - Termination processes include timely notification and disabling of access rights.

### *Access to IMS, IMS Infrastructure and Network Devices by IBM Cloud IaaS Personnel*

IBM Cloud IaaS personnel access IMS to investigate customers' issues and to provide technical support. There are two primary mechanisms for an IBM Cloud IaaS employee to modify/update customers' bare metal server: through IMS and its functionality, or through directly accessing customers' environments. Credentials associated with customers' bare metal, virtual, or hybrid environments are stored in IMS to assist in troubleshooting issues. Support personnel cannot directly access customers' virtual servers, and in the rare instance where support is required, it is provided through the XenCenter management console. Customers are solely responsible for managing their bare metal and virtual servers. As a result, bare metal and virtual server technical support provided by IBM Cloud IaaS is at the direction and sole discretion of the customer and not within the scope of the system.

Access to the IBM Cloud IaaS production environment, including IMS, IMS infrastructure and network devices, by IBM Cloud IaaS personnel requires unique user credentials authenticated through the IBM Cloud IaaS Active Directory. Active Directory is the central user access administration tool used to provide access to the IBM Cloud IaaS production environment. IBM Cloud IaaS has configured minimum requirements for Active Directory passwords, including minimum character length, complexity, password history, and expiration. If accessing the IBM Cloud IaaS environment from outside an IBM Cloud IaaS office location, IBM Cloud IaaS employees are required to access the IBM Cloud IaaS network via VPN utilizing token-based, two-factor authentication that enforces the established minimum password parameters. Additionally, the token requires a six-digit security code that changes every 30 seconds.

New hires that require IBM Cloud IaaS production access are authorized and access is granted based on job responsibilities. An annual continued business need revalidation is performed over Active Directory user IDs with access to the IBM Cloud IaaS production environment to determine that continued access is still required. Additionally, a quarterly business need revalidation is performed over Active Directory groups/users with privileged access to determine that IBM Cloud IaaS privileged user ID access is still required. Active Directory groups/users with privileged access is defined as users with administrator access to the bastion hosts controlling access to the IaaS production environment. Administrator access to the bastion hosts allows authorized IBM Cloud IaaS employees to add/modify/delete access to the IBM Cloud IaaS production environment, including IMS, IMS infrastructure and network devices. Exceptions identified during the revalidation process are remediated.

In the event that an employee resigns, is terminated or transfers, the user's logical access is revoked upon termination. A quarterly employment verification is performed over Active Directory user IDs with access to the IBM Cloud IaaS production environment, in accordance with the defined security policy, to determine that the owner of a user ID is still employed. Exceptions identified during the verification process are remediated prior to the completion of the quarterly employment verification, in accordance with the defined security policy.

### *Network Segregation via VLANs*

Internal boundaries are established and maintained through dedicated VLANs leveraging custom automated ACLs (Access Control Lists) or VRFs (Virtual Routing and Forwarding). To segregate customer traffic, IBM Cloud IaaS utilizes 802.1Q VLAN tagging for traffic within its data centers. Each bare metal server or virtual server will be automatically assigned a dedicated VLAN secured with custom ACLs or VRFs within the

environment and only traffic tagged with that VLAN ID will be routed to or from systems authorized to send or receive on the VLAN. Specifically, VLAN tagging is configured to segment individual customers from other customer environments and the IBM Cloud IaaS Management network.

### *Vulnerability Scanning*

Vulnerability scans are executed against all production devices within the IBM Cloud IaaS system. Vulnerability scans are executed based on the frequency defined within the policy for each device type. After the vulnerability scan is complete, a report is generated and any vulnerabilities identified are assigned severity levels based on the defined security policy.

Vulnerabilities identified are tracked and remediated based on severity levels, as necessary, per the requirements of the defined security policy. Implementation of corrective actions are administered through the change management process.

### *Device Destruction*

Once a hard drive is determined to be at the end of its functional life, the drive is requested to be physically destroyed. Upon completion, the drive is physically destroyed by bending and breaking its internal components, including the data platters. This results in the inability to "spin" or use the hard drive. The physical destruction process is tracked using the serial number on the hard drive. Details of physical destruction are maintained in IMS.

## Significant Events and Conditions other than Transactions

No significant events or changes to the design of controls have occurred that impact the information technology general controls system for IBM Cloud IaaS during the period November 1, 2021 to October 31, 2022.

# *IV. SoftLayer Technologies Inc.'s Control Objectives and Controls, and PricewaterhouseCoopers' Tests of Operating Effectiveness and Results of Tests*

The control objectives and the accompanying description of controls, which were provided by IBM Cloud IaaS management, cover the following areas of information systems controls:

A. Physical Security

B. Change Management

C. Incident Management

D. Computer Operations

E. Logical Security

Tests of the control environment, risk assessment, monitoring, and information and communication included inquiry of appropriate management, supervisory and staff personnel, observation of IBM Cloud IaaS's activities and operations, and inspection of IBM Cloud IaaS's documents and records. The results of these tests were considered in planning the nature, timing and extent of our testing of the controls designed to achieve the control objectives described on the following pages. As inquiries were performed for substantially all of IBM Cloud IaaS's control activities, this test was not listed individually for each control activity listed in the tables in Section IV. Additionally, observation and inspection procedures were performed as it relates to system generated reports, queries, and listings to assess the completeness and accuracy (reliability) of the information utilized in the performance of our testing of the control activities.

## A. Physical Security

**Control Objective:** Controls provide reasonable assurance that physical access to server rooms where customer systems reside is restricted to authorized individuals.[1]

| Control Reference | Control Activity | PricewaterhouseCoopers' Tests | Results of Tests |
|---|---|---|---|
| A1 | Physical access to server rooms where customer systems reside is restricted (e.g., through the use of a card access or biometric systems) to authorized personnel only and requires documented approval from management.<br>Individuals without authorized access to the server rooms must sign in and be escorted by an individual with approved controlled area access. | 1) Observed the server rooms where customer systems reside for a sample of data centers to determine whether access to server rooms is restricted through an access system.<br>2) Observed evidence for a sample of data centers to determine whether visitors and contractors to the data centers are signed in and escorted by authorized personnel.<br>3) Inspected evidence for a sample of new access to server rooms where customer systems reside to determine whether new access requests were documented and approved in accordance with the defined policy. | No exceptions noted. |
| A2 | Access rights to server rooms where customer systems reside are revalidated on a quarterly basis. A quarterly revalidation is performed to determine that a business need for access still exists. Exceptions identified during the revalidation process are remediated in accordance with the defined policy. | 1) Inspected evidence for a sample of data centers to determine whether access revalidations were performed on a quarterly basis. Where identified, inspected evidence to determine whether corrective action was performed in accordance with the defined policy.<br>2) Inspected evidence for a sample of data centers to determine whether all active access was included in an access revalidation performed on a quarterly basis. | No exceptions noted. |

1 The physical security control objective only applies to IBM Cloud IaaS systems located at the specified data centers described in section III of this report.

| Control Reference | Control Activity | PricewaterhouseCoopers' Tests | Results of Tests |
|---|---|---|---|
| A3 | Terminated access to server rooms where customer systems reside is revoked within upon termination. | 1) Inspected the current active access list for a sample of data centers and the list of terminations during the period to determine whether terminated access was deleted or re-assigned to a new owner in accordance with the defined policy.<br>2) Inspected a sample of physical access removal requests to data centers during the period to determine whether management action was taken in accordance with the defined policy. | No exceptions noted. |
| A4 | Surveillance cameras are located at strategic locations at the data center as a deterrent to unauthorized access. | 1) Observed evidence for a sample of data centers to determine whether surveillance cameras are located at controlled areas within the data center. | No exceptions noted. |

## B. Change Management:

**Control Objective:** Controls provide reasonable assurance that changes to the system software and network components are documented and approved.

| Control Reference | Control Activity | PricewaterhouseCoopers' Tests | Results of Tests |
|---|---|---|---|
| B1 | Change approvals are obtained prior to implementation into the production environment, if applicable. Verbal approval from management prior to implementation is acceptable for emergency changes. However, documented approval must be provided after implementation. | 1) Inspected change tickets for a sample of system changes to determine whether the following was performed:<br>• Required approvals, if applicable, based on the risk categorization, were obtained prior to implementation, in accordance with the defined change management procedures; or<br>• Verbal approvals, for emergency/expedited changes, were obtained prior to implementation with documented approvals provided after implementation, in accordance with the defined change management procedures. | No exceptions noted. |
| B2 | Changes are tested successfully, when applicable, prior to implementation into the production environment. | 1) Inspected change tickets for a sample of system changes to determine whether the following was performed;<br>• Testing, when applicable, is completed successfully prior to implementation into the production environment. | No exceptions noted. |

| Control Reference | Control Activity | PricewaterhouseCoopers' Tests | Results of Tests |
|---|---|---|---|
| B3 | A formal, documented change management process exists, including the change approval process and procedures to handle routine, expedited, emergency, and business as usual changes. The change management process is reviewed periodically and changes to the procedure are approved.<br><br>Changes are documented prior to implementation into the production environment and documentation includes the following:<br>• Categorization of the change risk. Change risk categories are used to determine approval requirements in accordance with the defined change management process. Changes which have been categorized as 'Minor' or 'Business as Usual' in accordance with the defined change management procedures may not require approval prior to implementation;<br>• A back out plan, as applicable; and<br>• Communication to the affected users in accordance with the defined change management procedures, as applicable. | 1) Observed the IBM change management procedures to determine whether periodic review and approval was performed.<br>2) Observed the IBM change management procedures to determine whether it includes procedures to handle routine, expedited, emergency, and business as usual changes.<br>3) Inspected a sample of system changes for the following:<br>• Categorization of change risk;<br>• A back out plan was documented, as applicable; and<br>• Communication to affected users, as applicable. | No exceptions noted. |

## C. Incident Management

**Control Objective:** Controls provide reasonable assurance that system and network processing issues (once input into the incident management tool) are responded to in a timely manner.

| Control Reference | Control Activity | PricewaterhouseCoopers' Tests | Results of Tests |
|---|---|---|---|
| C1 | A formal, documented incident management process exists. The incident management process document is reviewed and approved on a periodic basis. | 1) Inspected the incident management procedures to determine whether periodic review and approval was performed. | No exceptions noted. |
| C2 | IBM provides customers with a reporting channel to notify IBM management of incidents identified.<br>Externally reported and internally identified customer impacting incidents are tracked through an incident management tool and are responded to in accordance with the published customer impacting incident response times. The following information is populated in the incident tickets:<br>• Incident severity;<br>• Date and time the incident was identified; and<br>• Date and time of first response to the incident. | 1) Observed the tool / system used for customer incident reporting to determine whether customers are provided a channel for reporting incidents.<br>2) Inspected customer impacting incident tickets for a sample of incidents to determine whether the following was populated:<br>• Incident severity;<br>• Date and time the incident was identified; and<br>• Date and time of first response to the incident.<br>3) Inspected customer impacting incident tickets for a sample of incidents to determine whether the incidents were responded to in accordance with the published incident customer impacting response times. | No exceptions noted. |

| Control Reference | Control Activity | PricewaterhouseCoopers' Tests | Results of Tests |
|---|---|---|---|
| C3 | Internal security incidents are tracked through an incident management tool and are responded to in accordance with the published internal security incident response times. The following information is populated in the incident tickets:<br>• Incident severity;<br>• Date and time the incident was identified; and<br>• Date and time of first response to the incident. | 1) Inspected internal security incident tickets for a sample of incidents to determine whether the following was populated:<br>• Incident severity;<br>• Date and time the incident was identified; and<br>• Date and time of first response to the incident.<br>2) Inspected incident security tickets for a sample of incidents to determine whether the incidents were responded to in accordance with the published incident response times. | From a sample of 45 internal security incidents, the following exceptions were noted:<br>• Two (2) internal security incidents were not responded to in accordance with the published incident response times. |
| C4 | Automated tools identify security and availability incidents, which are tracked by the SOC and/or NOC groups where necessary. | 1) Observed evidence to determine whether incident monitoring tools are configured to generate alerts to the SOC/NOC groups. | No exceptions noted. |

| Control Reference | Control Activity | PricewaterhouseCoopers' Tests | Results of Tests |
|---|---|---|---|
| C5 | Reporting channels exist to notify the cybersecurity incident response team (CSIRT) of potential cybersecurity breaches or other incidents.<br><br>Cybersecurity incidents are tracked through a cybersecurity incident management tool and are responded to in accordance with the documented cybersecurity incident management process. The following information is populated in the incident tickets:<br>• Cybersecurity incident severity;<br>• Date and time the cybersecurity incident was created; and<br>• Response with actions to resolve the cybersecurity incident. | 1) Observed evidence to determine whether customers and employees are provided with reporting channels to notify the cybersecurity incident response team (CSIRT) of potential cybersecurity breaches or other incidents.<br>2) Inspected cybersecurity incident tickets for a sample of cybersecurity incident to determine whether the following was populated:<br>• Cybersecurity incident severity;<br>• Date and time the cybersecurity incident was created; and<br>• Response with actions to resolve the cybersecurity incident.<br>3) Inspected cybersecurity incident tickets for a sample of cybersecurity incidents to determine whether the cybersecurity incidents were responded to in accordance with the documented cybersecurity incident response management process. | No exceptions noted. |

## D. Computer Operations

**Control Objective:** Controls provide reasonable assurance that failover systems are monitored.

| Control Reference | Control Activity | PricewaterhouseCoopers' Tests | Results of Tests |
|---|---|---|---|
| D1 | IMS and IMS infrastructure data is replicated on a continuous basis to another geographically separate server. | 1) Inspected evidence of the replication settings within IMS to determine whether data is replicated to a geographically separate server. | No exceptions noted. |
| D2 | A formal, documented disaster recovery plan exists. The disaster recovery plan is reviewed periodically and changes to the procedures are approved. The disaster recovery plan includes an identification of the risks, corresponding risk mitigation strategies and procedures to test the feasibility of the plan. The disaster recovery plan is tested at least annually. | 1) Inspected evidence for the disaster recovery plan to determine whether periodic review and approval was performed.<br>2) Inspected evidence for the disaster recovery plan to determine whether the disaster recovery plan includes an identification of the risks, corresponding risk mitigation strategies and procedures to test the feasibility of the plan.<br>3) Inspected evidence for the disaster recovery plan to determine whether the disaster recovery plan was tested at least annually. | No exceptions noted. |

## E. Logical Security

**Control Objective:** Controls provide reasonable assurance that logical security over systems is implemented and maintained as defined in the security policy.

| Control Reference | Control Activity | PricewaterhouseCoopers' Tests | Results of Tests |
|---|---|---|---|
| E1 | Policies related to security and availability requirements are periodically reviewed in accordance with the required review timeframe and communicated to authorized users. | 1) Inspected the current security and availability policies to determine whether periodic review and approval was performed.<br>2) Inspected the current security and availability policies to determine whether the policies have been communicated / made available to authorized users. | No exceptions noted. |
| E2 | Access to systems is granted based upon a documented, approved request, in accordance with the defined policy. | 1) Inspected evidence for a sample of new user IDs to determine whether the new user access request was documented and approved in accordance with the defined policy. | No exceptions noted. |
| E3 | A periodic continued business need revalidation is performed over Active Directory user IDs with access to the IBM Cloud IaaS environment, in accordance with the defined policy to determine that continued access is still required. Exceptions identified during the revalidation process are remediated in accordance with the defined policy. | 1) Inspected evidence for a sample of periodic continued business need revalidations over Active Directory user IDs with access to the IBM Cloud IaaS environment to determine whether the revalidations were performed in accordance with the defined policy. Where identified, inspected evidence to determine whether corrective action was performed in accordance with the defined policy.<br>2) Inspected evidence for a sample of Active Directory user IDs with access to the IBM Cloud IaaS environment to determine whether all active user IDs were included in a periodic continued business need revalidation. | No exceptions noted. |

| Control Reference | Control Activity | PricewaterhouseCoopers' Tests | Results of Tests |
|---|---|---|---|
| E4 | A periodic continued business need revalidation is performed over Active Directory groups/users with privileged access, in accordance with the defined policy to determine that continued access is still required. Exceptions identified during the revalidation process are remediated in accordance with the defined policy. | 1) Inspected evidence for a sample of periodic continued business need revalidations over Active Directory groups/users with privileged access to determine whether the revalidations were performed in accordance with the defined policy. Where identified, inspected evidence to determine whether corrective action was performed in accordance with the defined policy.<br>2) Inspected evidence for a sample of Active Directory groups/users with privileged access to determine whether they were included in a periodic continued business need revalidation. | No exceptions noted. |
| E5 | IBM user access is revoked in accordance with the defined policy. In the absence of documented timeframe requirements, IBM user access is revoked within five business days of termination. | 1) Inspected the current active user ID list for a sample of devices and the list of terminations during the period to determine whether terminated access was deleted or re-assigned to a new owner in accordance with the defined policy. Where user IDs were not deleted or re-assigned in accordance with the defined policy, inspected evidence to determine whether network or both remote and physical access was removed timely, in accordance with the defined policy. | No exceptions noted. |
| E6 | Vulnerability scans are performed in accordance with the defined policy. Any vulnerabilities identified are tracked and remediated in accordance with the defined policy. | 1) Inspected evidence for a sample of vulnerability scans to determine whether the vulnerability scans were executed in accordance with the defined policy. Where identified, inspected evidence to determine whether deviations were documented, tracked and remediated in accordance with the defined policy. | No exceptions noted. |

| Control Reference | Control Activity | PricewaterhouseCoopers' Tests | Results of Tests |
|---|---|---|---|
| E7 | Active Directory credentials and token-based two-factor authentication with minimum password parameters are required for IBM personnel to access IMS, IMS infrastructure devices and in-scope network devices. | 1) Observed evidence to determine whether token-based two-factor authentication is required for IBM personnel to access the environment.<br>2) Inspected evidence of the Group Policy Object (GPO) in Active Directory to determine whether password parameters are set in accordance with the defined security policy. | No exceptions noted. |
| E8 | Minimum password parameters are enforced by the system for customer access to IMS. | 1) Inspected evidence of the enforced password requirements upon creation of a customer ID to determine whether password parameters are set in accordance with the defined security policy. | No exceptions noted. |
| E9 | Customers can only access their data in IMS. Logical access between customers is configured, via VLAN, to restrict access to only that customer's data. | 1) Inspected evidence for a sample network switch configuration to determine whether switches are configured with VLAN tagging to tag and route traffic between switches to enforce segregation of customer data in accordance with the defined policy.<br>2) Inspected evidence for a sample IMS VLAN configurations to determine whether access between customer VLANs is restricted through unique VLAN IDs and associated Access Control Lists (ACLs) or Virtual Routing and Forwarding (VRF). | No exceptions noted. |
| E10 | Physical destruction of devices is performed and evidence, via certificate of destruction or other documentation, is retained in accordance with the defined policy. | 1) Inspected supporting device destruction certificates for a sample of devices identified for physical destruction to determine whether the devices were destroyed in accordance with defined policy. Where a certificate does not exist, inspected additional documented evidence to determine whether the devices were destroyed in accordance with the defined policy. | No exceptions noted. |

## *V. Other Information Provided by SoftLayer Technologies, Inc. That is Not Covered by the Service Auditors' Report*

The following information is provided by IBM Cloud IaaS management to communicate a response to exceptions identified. The responses are not included within the scope of this report and have not been subjected to the procedures applied in the PricewaterhouseCoopers LLP examination of IBM SoftLayer Technologies, Inc.'s description of its information technology general controls system for the IBM Cloud Infrastructure as a Service (IaaS) throughout the period November 1, 2021 to October 31, 2022, and accordingly, PricewaterhouseCoopers LLP expresses no opinion on them:

| IBM Control Activity | PricewaterhouseCoopers' Test Results | IBM Management Response |
|---|---|---|
| C3. Internal security incidents are tracked through an incident management tool and are responded to in accordance with the published internal security incident response times. The following information is populated in the incident tickets:<br>• Incident severity;<br>• Date and time the incident was identified; and<br>• Date and time of first response to the incident. | From a sample of 45 internal security incidents, the following exceptions were noted:<br>• Two (2) internal security incidents were not responded to in accordance with the published incident response times. | The impacted Operational Team has provided additional training on incident response management and required response timelines to ensure all incidents are responded to in a timely manner. |