

### **III. SoftLayer Technologies, Inc.'s Description of its IBM Cloud Infrastructure as a Service (IaaS) System**

#### **A. System Overview**

##### **Background**

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 boundaries:

- 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, IBM Hardware Security Module (HSM), SAP-Certified Cloud Infrastructure, IBM Cloud Virtual Servers

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

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.

### **Service Commitments and System Requirements**

Customers are provided and required to agree to a Cloud Services Agreement (CSA) during the account creation process. The CSA is available to customers through the customer portal and acts as the formal contract and usage policy for customer users of the IBM Cloud IaaS system. The CSA documents the contractual obligations of IBM Cloud and the customers using IBM Cloud IaaS, including principal service commitments and system requirements. Any updates to the CSA are communicated to the existing customers through the customer portal.

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

- 1. Cloud Services
- 2. Content and Data Protection
  - Included within paragraph d. of the Content and Data Protection section is a link to IBM's Data Security and Privacy Principles for IBM Cloud Services (DSP). Relevant service commitments and system requirements are included within the following sections of the DSP:
    - Data Protection
    - Security Policies
    - Security Incidents
    - Physical Security and Entry Control

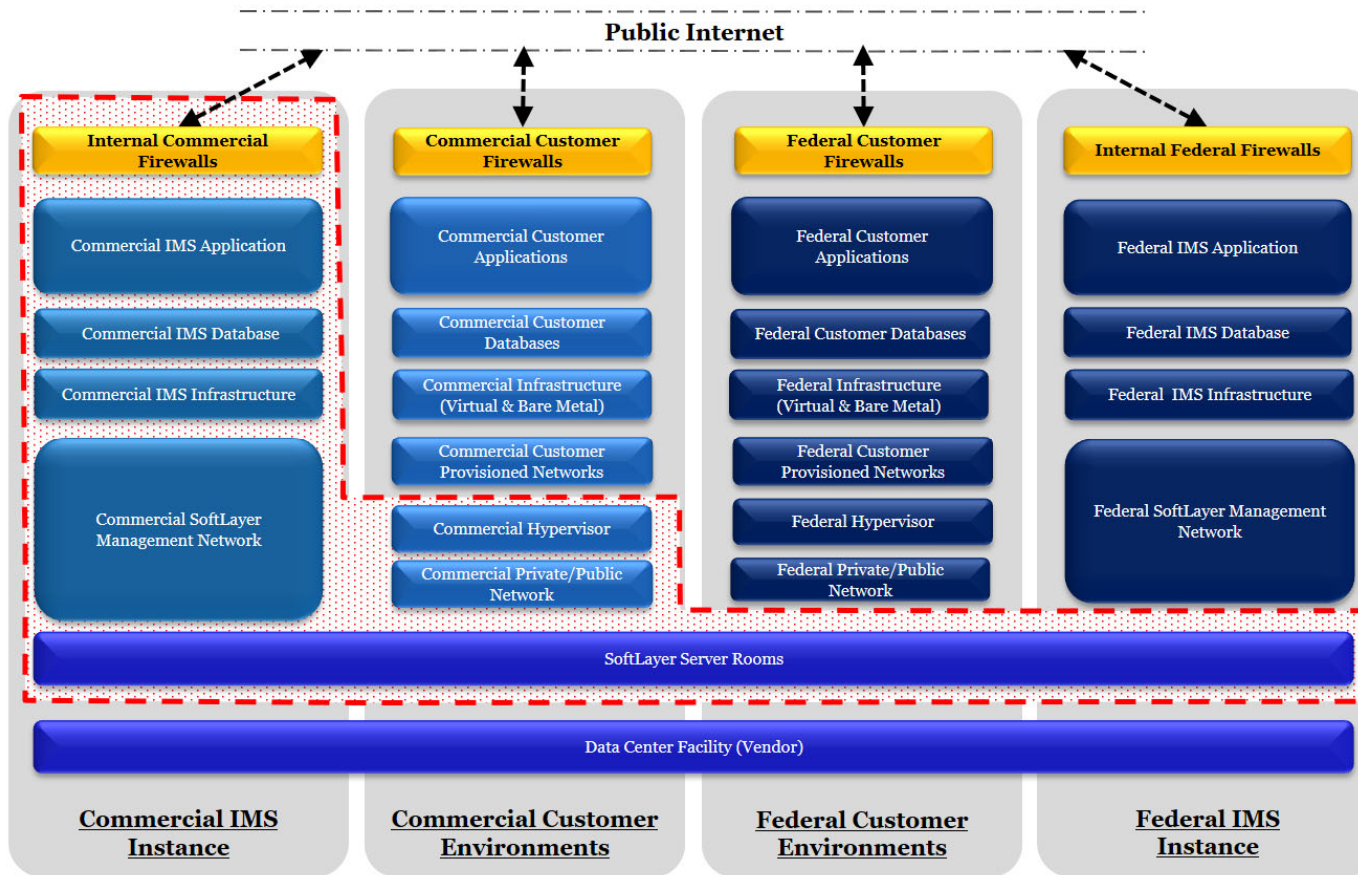
- Access, Intervention, Transfer and Separation Control
- Service Integrity and Availability Control
- 9. General

The CSA encompasses the full list of service commitments and system requirements delivered to IBM Cloud customers which may include services outside the scope of the report. As such, the CSA should be read in conjunction with the system boundaries and applicable trust services criteria. All other service commitments and system requirements described within the CSA are not in scope for this report.

Principal service commitments and system requirements within the boundaries of the system are outlined further in the sections below.

**Boundaries of the System**

**IBM Cloud Infrastructure as a Service (IaaS) SOC 2 Scope**



*Note: Area within the dashed line is within the boundaries of the system.*

The boundaries of the system 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 (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 routers. 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 vRouters or a Juniper vSRX device 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.
- **IBM Hardware Security Module (HSM)** is a standalone appliance that provides dedicated single-tenant encryption and key management.
- **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.

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 boundaries of the system do 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 (DALo8 and WDCo3). A separate instance of IMS (FedIMS) provides provisioning

functionality and infrastructure management. These data center facilities are included within the physical security boundaries of the system, however, other aspects of the services including the FedIMS system and its processes, are not included within the boundaries of the system.

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 boundaries of the system:**

Service Offering	Data Center / Hardware Locations	Network	Operating System Infrastructure	System Software	Applications	Customer Data
IBM Cloud IaaS	48 data centers (Refer to the Infrastructure section below)	Customer provisioned and managed network devices, firewalls and VPNs are solely the responsibility of the customer and are not within the boundaries of the system.	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 boundaries of the system.			Customer data is solely the responsibility of the customer and is not within the boundaries of the system.
		Network devices supporting customer managed environments and managed by IBM Cloud IaaS are within the boundaries of the system including: Routers, Switches, Firewalls, VPNs				
		Network devices directly in support of the IMS portal are within the boundaries of the system including: Routers, Switches, Firewalls, VPNs	Operating systems directly in support of the IMS portal are within the boundaries of the system including: Linux, UNIX, Windows	System software directly in support of the IMS portal are within the boundaries of the system including: Radius, Citrix, Active Directory	Internal Management System (IMS)/ Customer Portal	

## ***B. Relevant Aspects of the Internal Control Framework***

IBM's Framework of Internal Control (FIC) is based on COSO's Internal Control - Integrated Framework (COSO 2013 Framework), a construct designed to help improve the quality of reporting through focus on corporate governance, ethical practices and effective internal controls. The Framework 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 Corporate Assurance and Advisory Services (CA&AS).

### **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, the performance of the internal audit function (known at IBM as "Corporate Assurance and Advisory Services"), 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 meet this objective and promote 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 offer date for sanctioned countries, otherwise 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 passing the 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 that access IBM or our customer's site or systems are required by Procurement contract terms to perform background checks prior to providing the contractor to IBM. This requirement is included in the code of conduct and ethical integrity guidelines for suppliers, for which IBM monitors their business partners' and suppliers' adherence to on a periodic basis.

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

IBM's personnel policies and procedures are designed to recruit, develop and retain competent and trustworthy employees who facilitate an effective internal control system and promote 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 information and tooling enables employees to 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 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 enables IBM to stay competitive in the market.

As part of learning their job responsibilities, employees improve organizational capabilities through formal training (facilitator led or self-paced digital training) as well as "hands-on" training, utilizing documented functional guidance. 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 Twice-Yearly Reflections.

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. To promote marketplace leadership, IBM focuses on employee growth and driving high performance through building new skills. Employees are empowered to be in control of their goals which reflect their work, business direction and two core dimensions (Business Outcomes 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 insights into IBMers' work and ensure alignment.

IBMers complete a reflection twice-yearly: at the end of first half (1H) and the end of second half (2H). For each Reflection, managers provide feedback and at least annually, a rating.

### 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.

### ***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.

The IBM Trust & Compliance (T&C) group reviews and updates the BCG content annually in order to comply with IBM policies, regional laws and regulations, and external guidance. Upon onboarding, new employees certify that they have read and will comply with the IBM BCG policy. Annually, all employees re-certify their compliance with the IBM BCG. The certification process, including completion of an annual BCG education course, is tracked by both T&C 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 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 required of suppliers as a condition of doing business with IBM.

Suppliers must sign an RBA Letter Agreement demonstrating their commitment to adhere to the RBA Code. IBM monitors suppliers' compliance to the code as well as initiating 3rd-party audits of selected suppliers on an annual basis.

### ***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 a 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.

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.

Allegations can be submitted by line management, employees, Legal, Security, HR or CA&AS to the appropriate geography investigations manager. Additional allegation sources can include anonymous letters, complaints by customers, business partners, suppliers, former employees or referrals from the Employee Concerns focals received via the Confidentially Speaking reporting channel. All submissions are reviewed 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 may also be reviewed by a CHQ panel whose members include: the Vice President, HR Services; the Chief Auditor; and Legal. The appropriate line management representative, 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.

## **Risk Assessment**

### **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. Through CA&AS' focal point structure, audit management is responsible for understanding particular processes and organizations, including risks perceived by the business units and process owners. CA&AS continually monitors their plan, making adjustments as necessary, based on changing risks. Audit plan changes are approved by the appropriate CA&AS Director and the Chief Auditor. Significant changes to the audit plan are approved by the Audit Committee.

Findings are communicated to relevant parties, including IBM's external auditors. For all engagement types, CA&AS monitors, and tracks line management's implementation of recommendations to address audit findings until closure. The Chief Auditor provides the Audit Committee with a summary of results as well as an assessment of the Company's system of internal control.

CA&AS conducts continuous training and education programs to develop and maintain auditing skills. In addition, CA&AS sponsors certifications and memberships to professional organizations directly related to CA&AS' mission, for example: Certified Internal Auditor (CIA) offered by the Institute of Internal Auditors (IIA), Certified Information Systems Auditor (CISA) offered by ISACA, and Certified Fraud Examiner (CFE) offered by the Association for Certified Fraud Examiners.

### **Vendor Management**

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 boundaries of the IBM Cloud IaaS system, to achieve the related service commitments and system requirements. 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 email notifications.

### ***IT Risk Assessment Process***

IBM Cloud IaaS performs IT risk assessments on a periodic basis to ensure system risks related to security 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

High priority items identified during the periodic risk assessment are documented, assigned an owner, assigned an action plan, and tracked through to resolution in accordance with the defined risk assessment policy.

### **Information and Communication**

#### ***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.

Cybersecurity Threat Detection and Response: IBM deploys numerous mechanisms across the company designed to monitor and detect anomalous activity or security incidents, leverage AI, threat intelligence and forensic tools. Additionally, IBM runs various scans across the network to identify any vulnerability within the network.

IBM's IT Security Standard establishes the IT Security Control requirement for all systems and applications, and includes requirements for:

- Data and Asset Classification and Protection
- Asset Management
- Access Control
- Use of Encryption
- Operations Security
- Network Security
- Physical and Environmental Security
- Security Incidents
- Regulatory Request Handbook
- Risk Management
- End User Device Management and Configuration Requirements and End User Acceptable Use Requirements
- Supply Chain Security
- Security and Privacy by Design

Workstation Security: IBM has an enterprise IT security policy and a number of standards designed to protect IT assets. These are developed with influence from a number of industry best practices, including but not limited to, National Institute of Standards and Technology (NIST) and International Organization for Standardization (ISO). Workstations are governed by this policy that includes practices such as: strong password use, inactivity time intervals, encryption protection, data transfer restrictions, and patch management.

Data Privacy & Tech Ethics: The Chief Privacy Officer (CPO) oversees IBM's privacy and tech ethics vision, compliance strategy, and governance processes. 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):** 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.

### **Control Activities**

The control activities relevant to the IBM Cloud IaaS system are outlined further in the "System Components" section below.

### **Monitoring of Controls**

#### ***Internal Service Reporting Programs***

IBM conducts regular internal service reviews that span data center organizational structures. These programs are designed for management visibility and focus at an organizational level. IBM scorecard reviews are conducted on a regular basis. The executive level meeting reviews open issues in a scorecard format that typically include tracked issues from compliance review activities.

Controls and management reporting are in place and are designed so that customer internal control deficiencies are reported to management. IT incidents and issues are identified, reported, escalated, and tracked through resolution, and corrective measures have been established and are designed to reduce the likelihood of similar incidents re-occurring. In addition, controls have been established that are designed to highlight processing errors and inconsistencies promptly. Whenever possible, errors are corrected before they impact production and delivery. Information regarding errors, inconsistencies and exceptions are tracked, managed, and systematically reported to management.

#### ***Compliance Monitoring***

For the independent monitoring of controls, the IBM Cloud teams regularly engage the security experts from IBM's Information Security Services group to perform testing and certain remediation support activities, as necessary. In addition, external auditors are regularly engaged to provide assurance services over various information security related standards and practices.

IBM Cloud IaaS conducts regular compliance management and monitoring activities for security related risks. Executive VP interlocks and General Manager operational reviews, focused on the holistic compliance posture of the IBM Cloud, occur on a periodic basis through a compliance dashboard and drive accountability at the senior leadership level across business units. The compliance dashboard presents each control's risk and compliance aspects to ensure that the security and compliance team operate within key security risk and compliance metrics.



## **C. System Components**

### **Infrastructure**

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 boundaries of the system.

<b>Facility</b>	<b>Physical Location</b>	<b>Facility Manager</b>
*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
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
MIL01	Milan, Italy	DATA4
MON01	Montreal, Canada	COLO-D
OSA2X	Osaka, Japan	IDC Frontier
PAR01	Paris, France	Global Switch
PAR04	Paris, France	Global Switch
PAR05	Paris, France	BNPP

Facility	Physical Location	Facility Manager
PAR06	Paris, France	BNPP
SAO01	Sao Paulo, Brazil	Ascenty
SAO04	Santana de Parnaíba, Brazil	Odata
SAO05	Sao Paulo, Brazil	Ascenty
*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
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 November 1, 2022 to October 31, 2023, there were 48 data centers included in the scope of the report. However, five (5) were decommissioned during the period (AMSo1, DALo2, DALo6, MEXo1, and SEOo1).*

Customers with bare metal, virtual, or hybrid environments can access the servers remotely (electronically) from anywhere in the world.

### ***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 has two-factor authentication with a biometric system and require a key card.

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.

## **Software**

### **Overview**

IBM Cloud IaaS customers are solely responsible for customer owned and managed software and applications as these components are not within the boundaries of the system. IBM Cloud IaaS does not maintain responsibility for customer software and applications that IBM Cloud IaaS customers run on their bare metal, virtual, or hybrid environment; the software and applications are the responsibility of IBM Cloud IaaS customers.

For components of the environment managed by IBM Cloud IaaS, software systems are managed centrally by IBM Cloud IaaS using consistent controls and processes. IBM Cloud IaaS manages the Customer Portal (IMS), IMS infrastructure and operating systems, network devices supporting IMS and certain network devices supporting customer environments within the IBM Cloud IaaS environment.

<b>IBM Cloud IaaS Managed Component</b>	<b>Software Managed</b>
IMS Database	<ul style="list-style-type: none"><li>• Oracle</li></ul>
IMS Infrastructure	<ul style="list-style-type: none"><li>• Various UNIX OS</li><li>• Linux</li><li>• Windows</li></ul>
Customer Portal / IMS	<ul style="list-style-type: none"><li>• Proprietary Software Developed by IBM Cloud IaaS</li></ul>
Shared network devices supporting customer environments	<ul style="list-style-type: none"><li>• RADIUS</li></ul>

## **People**

### **Organization and Administration**

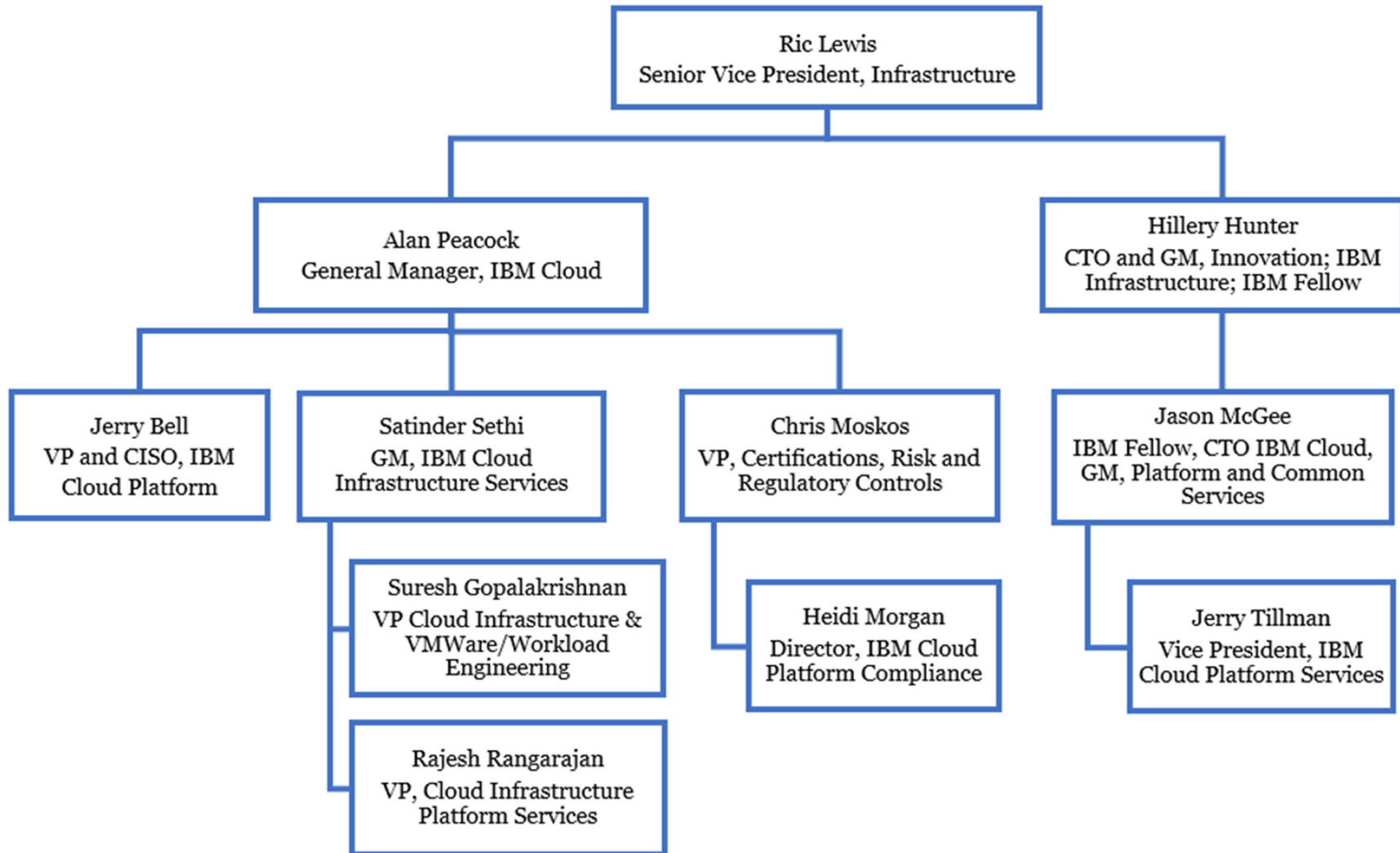
Key security positions of authority and responsibility are documented in a formal organizational chart, which evidences key organizational structures and reporting lines. The organizational chart is reviewed and updated periodically for accuracy.

Within the organization, roles and responsibilities are defined and communicated. IBM Cloud 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 may distribute some portion of its development and operations processes to IBM locations around the world, when permissible.

The IBM Cloud teams are comprised of diverse development and operations professionals, who maintain and follow IBM's processes, standards and procedures in the execution of their work. Security and availability requirements are generated from senior management. These requirements are distributed to the operational management leaders. These leaders are responsible for the implementation and monitoring of security controls.

**IBM Cloud Organizational Chart**



## **Data**

The integrity and conformity with regulatory requirements of workloads sent to the IBM Cloud IaaS system are solely the responsibility of IBM Cloud IaaS customers. IBM Cloud IaaS does not maintain responsibility for the data IBM Cloud IaaS customers store on their bare metal, virtual, or hybrid environment. The data is the responsibility of IBM Cloud IaaS customers.

## **Processes and Procedures**

### ***Policies and Procedures***

The IBM Cloud IaaS policies and procedures are a series of documents, which are used to describe the controls implemented within the system. The purpose of the policies and procedures is to describe the environment and define the practices performed on behalf of the customer. The policies and procedures include diagrams and descriptions of the network, infrastructure, environment and IBM's commitments. These policies and procedures are available to all IBM employees that support IBM Cloud IaaS. Additionally, each of the policies and procedures is reviewed by IBM management on a periodic basis, in accordance with the defined security policy.

### ***HR***

IBM's personnel policies and procedures are designed to recruit, develop and retain competent and trustworthy employees who facilitate an effective internal control system and promote 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.

### ***Communication***

IBM Cloud IaaS employees are kept informed of the corporate and individual responsibilities through a variety of channels of communication. A corporate intranet website has been established to provide timely announcements of corporate news. Employees can access a wide range of information that includes, but is not limited to, corporate news, corporate policies, organization charts, phone listings, internal education opportunities, security and safety guidance, and incident response procedures.

IBM Cloud IaaS maintains a line of communication with clients from the provisioning process through continued support of on-going operations. IBM Cloud IaaS communicates the procedures for handling operational failures, incidents, problems, concerns, and complaints to clients and how clients can alert IBM Cloud IaaS of any issues with their applicable systems.

### ***Logical Security***

#### ***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 boundaries of the system within this 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 boundaries 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 IBM Cloud IaaS's 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. The token requires a six-digit security code that changes every 30 seconds. Additionally, infrastructure devices on the control plane cannot be accessed without first authenticating through the bastion host devices included within the IBM Cloud IaaS environment.

The security configurations of the bastion hosts are governed by either Chef or Group Policy Object (GPO) policies. These policies are implemented on the bastion hosts and the system is configured to automatically remediate any policy deviations that occur. If an unauthorized change were to be made to a governed policies implemented on a bastion host, the configuration of the system would automatically revert the policy back to the required state.

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 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.

### ***Device Sanitization***

Once it is determined that a returned device should be repurposed or reused, the device is cleansed of any existing data by the IBM Cloud IaaS Inventory team through either 1) a standard reclaim process or 2) an ad hoc manual process.

- 1) The standard reclaim process occurs when a server is still useable but no longer needed by the customer (i.e., server upgrade). When a server is marked for reclaim, drives within that server at the time of the reclaim are required to undergo device sanitization. Reclaims

occur at the server level by wiping (i.e., reformatting) the drives and entering back into IBM Cloud IaaS inventory upon completion. A majority of devices in the environment are sanitized through the standard reclaim process.

- 2) The ad hoc process is invoked when a particular drive on a given server needs to be replaced due to a drive upgrade or corruption. In the ad hoc process, the drives are stored in a small parts bin and held for a least seven days in the event that the customer requires the drive to be physically returned. After the seven day waiting period, the drive is entered into the format server where a manual wipe sanitizes the drive of any existing data.

### ***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.

### ***Workstation Security***

IBM Cloud IaaS workstations employ a diagnostic tool that checks for core workstation security features, which automatically correct issues, or notifies workstation users of noncompliance. These checks include: hard drive security (password protection or full disk encryption); screen saver; antivirus; firewall; database encryption, if required based on data sensitivity; workstation user account passwords; operating system pack level and security patch is current; as well as checks to verify certain features are not enabled such as file sharing capabilities.

When non-compliance issues are identified, email notifications are sent to the registered user of each workstation requiring remediation. If not resolved, escalations via email are sent to managers of the employees that are not in compliance with the workstation policy, until the issue is resolved.

### ***Network Security***

#### ***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.

### ***Intrusion Detection***

IBM Cloud IaaS network ports are protected with firewalls, specifically Palo Alto firewalls, which serve as the intrusion detection (IDS) and intrusion prevention (IPS) agents, and GlobalProtect gateways that govern remote access activity. IBM Cloud IaaS traffic in and out of the network must pass through both the Palo Alto and GlobalProtect gateways. IBM Cloud IaaS uses the IBM QRadar tool, an enterprise security information and event management (SIEM) product, to monitor this traffic and events. GlobalProtect gateways and Palo Alto firewalls are configured to define which activity is logged and sent to the syslog server. The syslog server sends logged events within the syslog to QRadar, which monitors production IDS activity logs. Based on the nature, frequency, severity, and other activity log characteristics, a series of pre-defined rules enabled in QRadar will automatically flag events (or a combination thereof) as Offenses. The Security Operations Center (SOC) team monitors Offenses real-time and analyses to determine if the offense is a false positive or, whether the incident responses process should be invoked. If the offense is deemed to need further action, the SOC team will open a resilient (SIP) ticket to remediate the offense. The Security Incident in Progress (SIP) ticket will follow the standard incident management process.

### ***Firewall Rule Revalidation***

The IBM Cloud IaaS Network Engineering team has identified the firewalls that are in place to protect the IaaS system and the Security Operations team performs a firewall rule revalidation over the firewalls on a semi-annual basis. For each firewall, the team reviews the rules that allow open ports and traffic and compares the rules against the baseline configuration that was previously approved. For any differences against the baseline configuration, the Security Operations team will ensure that an approved change ticket exists to document the need for a firewall rule. If an approved change ticket cannot be found, the team will determine if the rule should exist and submit a change ticket to get the rule installed. If it is determined the rule should not be in place, the rule will be removed, and the Network Engineering team will investigate how the rule was created.

### ***Penetration Testing***

External penetration tests are conducted on the IBM Cloud IaaS. The penetration tests are designed to discover IT security flaws that could be exploited by a malicious attacker to compromise internal systems and data. The assessments are conducted in three phases: Reconnaissance, Exploitation, and Post-Exploitation. As an outcome of the review, recommended solutions are proposed to mitigate or remediate the flaws identified.

### **Secure Data Transmissions**

Customer interactions with the portal (IMS) are encrypted end-to-end utilizing 128 bit or 256 bit Secure Sockets Layer (SSL) protocols including manage.softlayer.com, control.softlayer.com, and the mobile applications' API URL as each website utilizes a TLS 1.2 encrypted connection. IBM Cloud IaaS requires external facing certificates to be signed by a well-known Certificate Authority, such as GeoTrust EV.

In addition to the primary Customer Portal, the customer can also utilize a mobile application on an Apple iOS or Google Android device. IBM Cloud IaaS mobile application communications require the use of HTTPS secure socket protocol accessible via <https://api.softlayer.com/> and <https://api.softlayer.com/mobile/v3/>. Interactions with the mobile-ready website and mobile applications are encrypted end-to-end utilizing 128 bit Secure Sockets Layer (SSL) protocol. Additionally, remote access mechanisms to the Customer Portal are encrypted.

### **Data at Rest Encryption**

Systems that store IMS data are subject to data at rest encryption requirements. IBM Cloud IaaS IMS data is stored within the primary Oracle databases at the DAL10 and WDC04 data center facilities. IBM Cloud IaaS enforces data at rest encryption at the database level utilizing Advanced Encryption Standard (AES) encryption and key management systems separating encryption keys from the data they encrypt.

IBM Cloud Object Storage (COS) is a scalable storage service with various deployment options available in order to meet customer requirements. COS provides security to customers through processing information into slices. As part of that transformation, data is encrypted using both information dispersal algorithm (IDA) and all or nothing transformation (AONT) encryption to an advanced Encryption Standard (AES) 256-bit encryption.

Network-attached storage (NAS) and Internet Small Computer Systems Interface (iSCSI) storage solutions, such as IBM Cloud File Storage and IBM Cloud Block Storage, store customer data utilizing Advanced Encryption Standard (AES) 256-bit encryption. Keys are protected using key management systems with industry standard Key Management Interoperability Protocol (KMIP).

### **Incident and Security 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 Cloud Services 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:

- Email 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, 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](http://www.softlayer.com) or [manage.softlayer.com](http://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.

### ***Customer Initiated Incident Reporting***

The incident management process defines the requirements for responding to customer raised incidents within the required response timeframe, per the defined policy. Customers initiate incident tickets via the Customer Portal. IBM Cloud IaaS personnel record each incident in an IMS ticket and track the incident from identification to resolution.

Additionally, an external facing resource is available on the IBM Cloud IaaS website for reporting vulnerabilities, risks or incidents by external parties. Issues reported are routed to the Abuse team and analyzed. Abuse or SIP tickets are created as required and monitored to resolution.

### ***Security Incident Management***

IBM Cloud IaaS security incidents are handled in accordance with the IBM Cloud IaaS incident response procedures, taking into account any data breach notification requirements under applicable law. IBM Cloud IaaS personnel have the ability to report security incidents via the IBM Cloud IaaS Help Desk. If the IBM Cloud IaaS SOC team identifies that a Customer Impacting Event (CIE) in ServiceNow or Security Incident in Progress (SIP) in JIRA has an IBM-wide/Corporate impact, they will create a Resilient ticket for IBM's Computer Security Incident Response Team (CSIRT) to address. Additionally, IBM Cloud IaaS customers can report security incidents directly through their project executives or engagement team,

who then communicates them to IBM's CSIRT Team via the IBM Help Desk. Incidents are rated based on severity level (severity levels 1-4). When IBM CSIRT receives a report of a potential security incident from a third party, IBM CSIRT logs the issue with the supporting details in Resilient and provides the tracking number to the party who reported the incident. Security incidents that have either already occurred or are identified in progress are logged with IBM CSIRT. Upon receiving notification of a security incident, the IBM CSIRT team takes ownership of investigating and resolving the reported security incident, with no further action required of the service offering unless otherwise instructed by the CSIRT team.

### ***System Capacity Monitoring***

Capacity monitoring systems are managed by the NRE to monitor availability thresholds over the IBM Cloud IaaS network. Network capacity is continuously monitored, 24x7. Low capacity thresholds are defined within the availability policy and upon breach of such thresholds, alerts are automatically reported to a central mailbox that is monitored by the NRE, network capacity, and network engineering teams. Upon receiving notification of a capacity breach, the NRE team raises a JIRA ticket to record, track, and resolve the capacity breach. Capacity breaches are remediated in accordance with the requirements outlined in the defined availability policy.

Redundant network infrastructure devices for the routing of critical functions exist at each data center. IBM Cloud IaaS maintains critical network devices in pairs to provide redundancy and the devices are both maintained as active. Both devices in a pair have traffic and activity processed through the devices and are monitored to ensure that the devices do not reach greater than 70% utilization. If one of the devices in a pair becomes unavailable, the standing device would be able to handle the network traffic. Capacity monitoring reports are generated and reviewed on weekly basis. The reports are used to review the utilization and check for devices that surpass the 70% utilization threshold. IBM Cloud IaaS reviews and implements remediation strategies to reduce the utilization to an acceptable level.

### ***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 customer's 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 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.

### **Availability**

#### ***Environmental Controls***

Data center facilities are managed and maintained to ensure adequate environmental controls are in place for the protection of equipment and the availability of customer data and services provided. Management reviews maintenance reports performed on a periodic basis to determine and schedule additional maintenance, where necessary. The following environmental controls exist at each center:

- Fire detection and suppression systems, including pre-action dry pipe, hand-held fire extinguishers, smoke detectors, and fire alarms;
- Backup power, including uninterruptable power supply (UPS) units and redundant generators (Global Switch Paris, Global Switch Australia and Ascenty Brazil utilize diesel rotary UPS (DRUPS) units);
- Power distribution units (PDU) and electrical panels; and
- Heating and cooling (HVAC) mechanisms, such as computer room air conditioning (CRAC) units, computer room air handlers (CRAH), chillers, and temperature and humidity monitoring and control.

At IBM Cloud IaaS and vendor managed facilities, IBM Cloud IaaS and Data Center Operations personnel perform an inspection of the data center during each shift to monitor temperature and humidity and to verify that environmental controls are operating as intended. Physical walkthroughs are performed by specialized and trained security personnel, facility provider engineering personnel and IBM Cloud IaaS personnel to monitor various aspects of each facility. IBM Cloud IaaS site managers monitor the maintenance records as evidence of continuous monitoring of each data center site.

The environmental protection systems are inspected and/or tested, as necessary, by approved vendors in accordance with local, city and state regulations. UPS/DRUPS units are located in dedicated areas. The primary UPS (providing backup power to the servers) is tested on a periodic basis under load conditions and performance results are monitored. Additionally, each data center facility is equipped with generators that automatically supply power to the facility in the event of outside power failure. Maintenance contracts are in place to ensure the equipment is maintained to certain specifications. The fire detection and suppression systems are tested on an annual basis. HVAC equipment, depending on the type, is maintained on a periodic basis. Maintenance is performed at each data center facility, either by IBM Cloud IaaS personnel or certain vendors. Maintenance records are monitored and reviewed by IBM Cloud IaaS site managers at each data center facility. Any deviations regarding scheduled maintenance activities are communicated to the central IBM Cloud IaaS facilities team.

### **Computer Operations**

Computer operations procedures have been defined and documented. Employees are periodically monitored for adherence to the policy and to facilitate any required amendments or changes to procedures.

### **IMS Replication and Failover**

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 in lieu of the unavailable services. 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 boundaries of the system or the scope of this report.

### **Disaster Recovery**

Based on the configuration of the IBM Cloud IaaS's "Network-Within-A-Network", with three 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 the IBM Cloud IaaS 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
<ul style="list-style-type: none"> <li>• Ensuring that the standby equipment meets the recovery schedules.</li> <li>• 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.</li> <li>• Working with the Network Team to restore local and wide area data communications services to meet the minimum processing requirements.</li> <li>• Initiating operations at the standby facility.</li> <li>• Providing sufficient personnel to support operations at the standby facility.</li> <li>• Managing the standby facilities to meet users' requirements.</li> <li>• Establishing processing schedule and inform user contacts.</li> <li>• Arranging for acquisition and/or availability of necessary computer supplies.</li> <li>• 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.</li> </ul>	<ul style="list-style-type: none"> <li>• Evaluating the extent of damage to the voice and data network and discuss alternate communications arrangements with telecoms service providers.</li> <li>• Establishing the network at the standby facilities in order to bring up the required operations.</li> <li>• Defining the priorities for restoring the network in the user areas.</li> <li>• Ordering the voice/data communications and equipment as required.</li> <li>• Supervising the line and equipment installation for the new network.</li> <li>• Providing necessary network documentation.</li> <li>• Providing ongoing support of the networks at the standby facility.</li> <li>• Reestablishing the networks at the primary site when the post disaster restoration is complete.</li> </ul>	<ul style="list-style-type: none"> <li>• In conjunction with the Information Systems, evaluating the damage and identifying equipment that can be salvaged.</li> <li>• Working with the Networking Team to have lines ready for rapid activation.</li> <li>• As soon as the standby site is occupied, cleaning up the disaster site and securing that site to prevent further damage.</li> <li>• 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.).</li> <li>• Preparing the original data center for re-occupation.</li> <li>• Maintaining current configuration schematics of the Data Center (stored off site) This should include:               <ul style="list-style-type: none"> <li>○ Air conditioning,</li> <li>○ Power distribution,</li> <li>○ Electrical supplies and connections,</li> <li>○ Specifications and floor layouts,</li> <li>○ Controlling security within the disaster area,</li> <li>○ Arranging for necessary office support services, and</li> <li>○ Managing staff safety and welfare.</li> </ul> </li> </ul>	<ul style="list-style-type: none"> <li>• Working with Management to obtain directives on the messages to communicate.</li> <li>• Making statements to local, national and international media, as appropriate.</li> <li>• Informing suppliers and customers of any potential delays.</li> <li>• Informing employees of the recovery progress of the schedules.</li> <li>• Ensuring that there are no miscommunications that could damage the image of the company.</li> <li>• Any other public relations.</li> </ul>