# Building GxP Regulated Systems on IBM Cloud™

IBM **Cloud**

IBM

# Purpose of this document

This document has been compiled by the IBM Cloud Services group to provide transparency to clients planning to deploy regulated (GxP) systems in the IBM Cloud infrastructure.

GxP refers to the collective set of globally accepted current "good practices" with respect to quality. This includes good manufacturing practices (GMPs), good clinical practices (GCPs), good laboratory practices (GLPs), good pharmacovigilance practices (GPVPs), good engineering practices (GEPs) and other quality guidelines in regulated industries including food, drugs, medical devices and cosmetics. In addition to the GxPs, IBM recognizes that Healthcare and Life Science (HCLS) clients' business activities are regulated by global health authorities such as the U.S. Food and Drug Administration (FDA) and European Medicines Agency (EMA), and are subject to regulations such as Title 21 CFR Part 11 and Annex 11: Computerized Systems Validation. While the IBM Cloud is not directly regulated by these global entities, IBM, as an IT Service Provider, recognize that there are control tools and activities that IBM Cloud can provide in support of its clients' compliance with regulatory and good practice requirements. As such, this guide has been developed to provide:

- Information about IBM Cloud resources available to clients in support of client-owned regulatory and good practices
- Clarification with respect to IBM Cloud and client responsibilities regarding design, deployment, qualification, validation and maintenance of systems

# Table of Contents

# Document scope

The scope of this document covers:

- IBM Cloud infrastructure services managed by IBM, including global data center physical locations, the IBM Cloud client portal, and the supporting infrastructure devices.
- Network devices that are managed by IBM Cloud supporting the IBM Cloud portal and infrastructure as well as network devices that support client environments but are not provisioned/managed by clients within the IBM Cloud infrastructure as a service (IaaS).
- Compute offerings including virtual (including the hypervisor layer) and bare metal servers.
- Storage offerings such as Block, File, and Cloud Object Storage.
- IBM platform as a service (PaaS) and software as a service (SaaS) components are out of scope of this document.

As shown in Figure 1 below, the scope of this document is limited only to the infrastructure components that are available as IaaS services in the IBM Cloud environment. The major components of the IaaS layer are compute, storage and network. The storage devices (such as Block and File Storage) can either be locally attached, accessible via API (such as Cloud Object Storage), or accessible via a storage area network. The Storage Area Network (SAN) is architecture to attach remote computer storage devices to servers in such a way that, to the operating system, the devices appear as locally attached. Although IaaS processes and controls are available to be leveraged by both PaaS and SaaS layers, those services are out of scope of this document. IBM's intent is to provide a scalable, well managed IaaS layer in IBM Cloud on which Clients can build or host their solutions on top of.

IBM Cloud also provides enterprise-class tools designed to help monitor for potential security risks and mitigate availability problems. Tools provided by IBM Cloud include, but are not limited to, load balancing, intrusion detection and prevention, standard and dedicated hardware firewalls, anti-virus, anti-spyware, anti-malware, and VeriSign® and GeoTrust® SSL Certificates.

## GxP Client Considerations

In this document, potential considerations are identified for Client Standard Operating Procedures (SOPs) and GxP documentation that may be relevant to Clients that utilize IBM Cloud.

This document does not address GxP considerations related to:

– Systems or devices managed by a regulated company within the client IaaS infrastructure environment

– Workloads (data, files, information) built by regulated companies on IBM Cloud IaaS

– Where applicable, configuration of IBM tools used in the support of mitigating security risks

These callouts should be viewed as guidance and not as exhaustive content on GxP systems. For additional expertise on GxP, contact IBM Services.

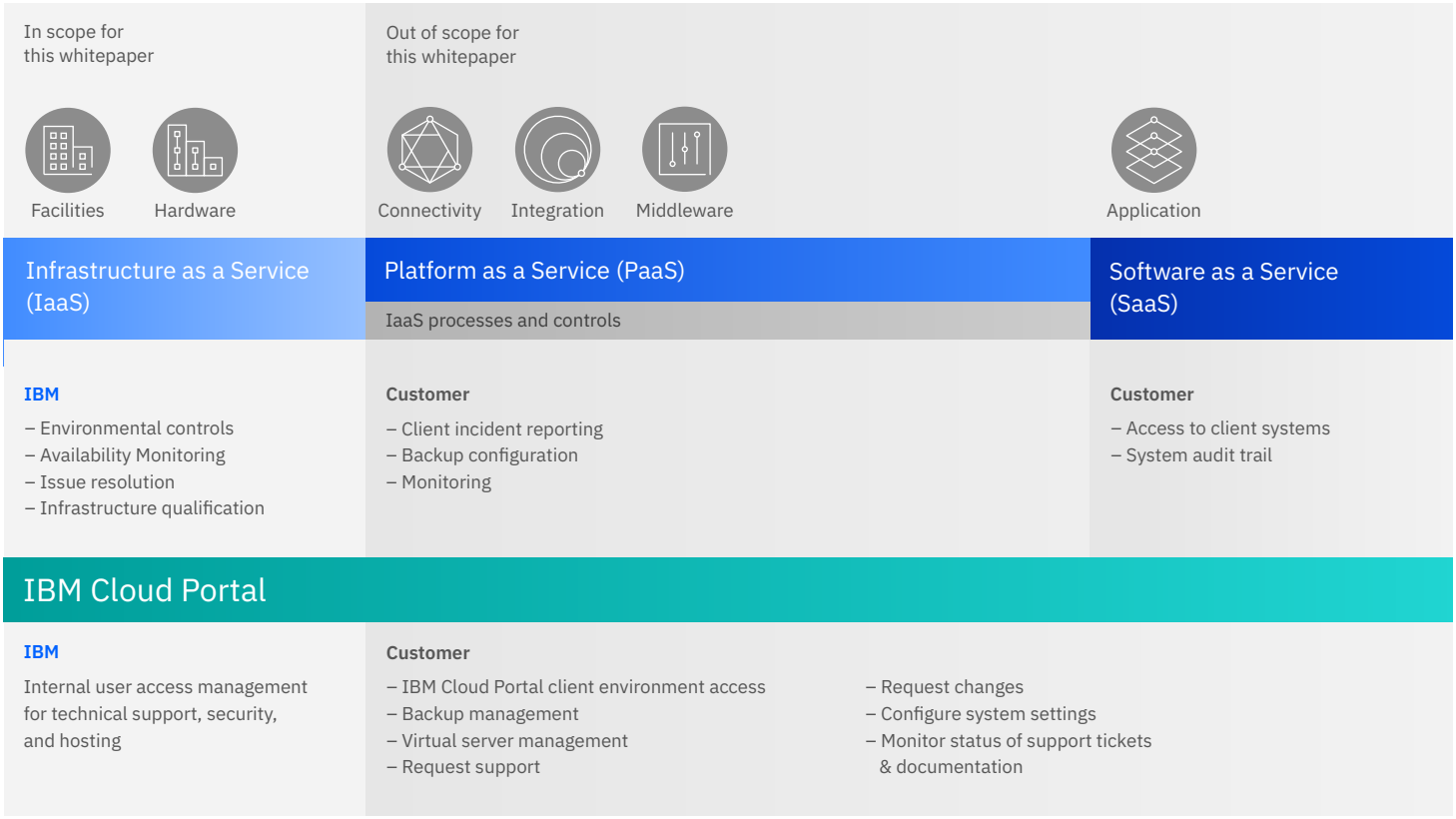



**Figure 1:** IaaS areas

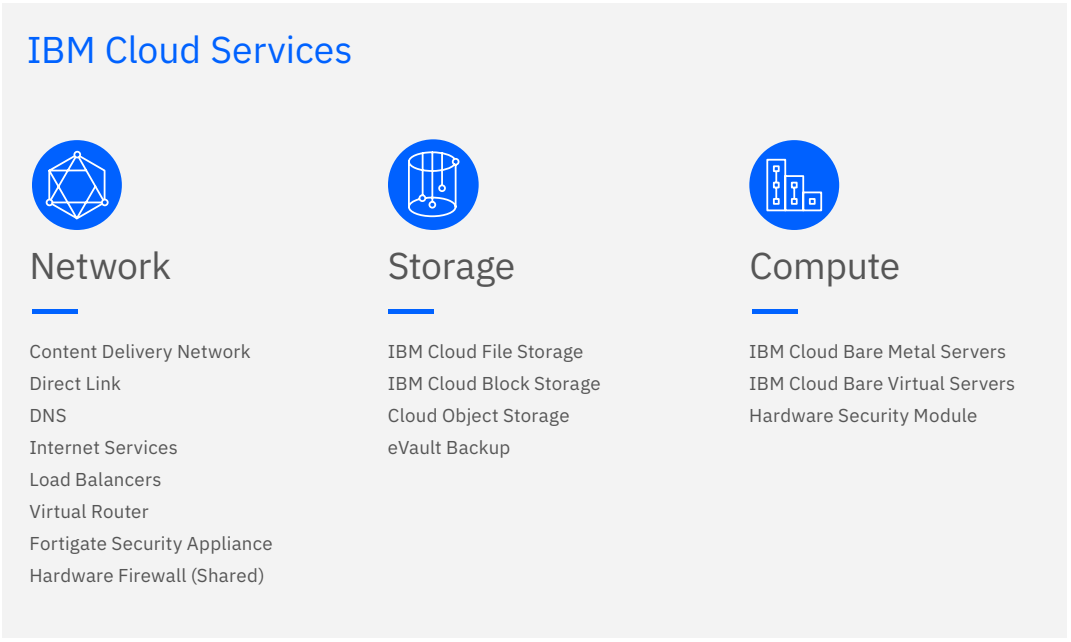



**Figure 2:** IBM Cloud Services

Further descriptions of each service can be found under the “Maintaining your Infrastructure” subsection of Section 2b: Infrastructure qualification.

# The IBM approach to securing and controlling Cloud Services

IBM Cloud delivers configuration requirements requested by clients, through application of automated test scripts, verification of installation activities and documented records to help secure and control cloud infrastructure components.

IBM Cloud demonstrates its ability to support administrative, physical and technical controls that align with client expectations through a combination of attestation reports (i.e. System and Organizational Controls (SOC) 1 and SOC 2), international standards certifications, and client-specific data captured within a client software portal.

**Service Organization Control (SOC) Reports Available**

IBM Cloud engages a third-party auditor to perform and execute SOC for Service Organizations Reports. The auditor expresses an opinion with relation to the results of the attestation and notes any findings. Currently a SOC 1 report and SOC 2 report are performed annually. It's a normal business practice for Cloud providers to provide security reports upon request by customers. The SOC 1 report focuses on the service organization controls that would be useful to user entities and their auditors for planning a financial statement audit of the user entity and evaluating internal control over financial reporting at the user entity. The SOC 2 report focuses on the service organization's system description and controls in accordance with specific criteria related to availability, security and confidentiality. Both the SOC 1 and SOC 2 reports include auditor testing, results, and an opinion.

Clients can use the SOC 2 report to review the controls maintained by IBM Cloud and their effectiveness. This is especially valuable to clients with regulated workloads because they can use this report to gain insight into the quality and reliability of the services they use. They can then use this information in their own qualification work to highlight the strengths of the infrastructure they use. This and other standards can be used by clients to help satisfy GxP and other regulatory requirements.

**Relevant certifications**

In addition to the controls attested to through SOC reports, IBM Cloud maintains a number of certifications that are relevant to its clients.

**ISO 9001**

ISO 9001 is the international standard that specifies requirements for a quality management system (QMS). Organizations use the standard to demonstrate the ability to consistently provide products and services that meet client and regulatory requirements.

The IBM Cloud infrastructure is certified (PDF, 412 KB) under the ISO 9001 standard. Additionally, IBM has maintained a Corporate wide certificate (PDF, 4.9MB) to the ISO 9001 standard since 2001 (current certificate expiring May 2022). A Corporate Policy on Quality was established in 2001 and a four-Tier Global Quality Framework model has been established that provides direction on quality system initiatives.

**ISO 27001**

ISO 27001 specifies the requirements for establishing, implementing, maintaining and continually improving an information security management system within the context of the organization. It also includes requirements for the assessment and treatment of information security risks tailored to the needs of the organization.

For more information on these and other compliance programs and certifications, see IBM Cloud compliance certifications.

Section 1:

# IBM Cloud Infrastructure

**General System Description**

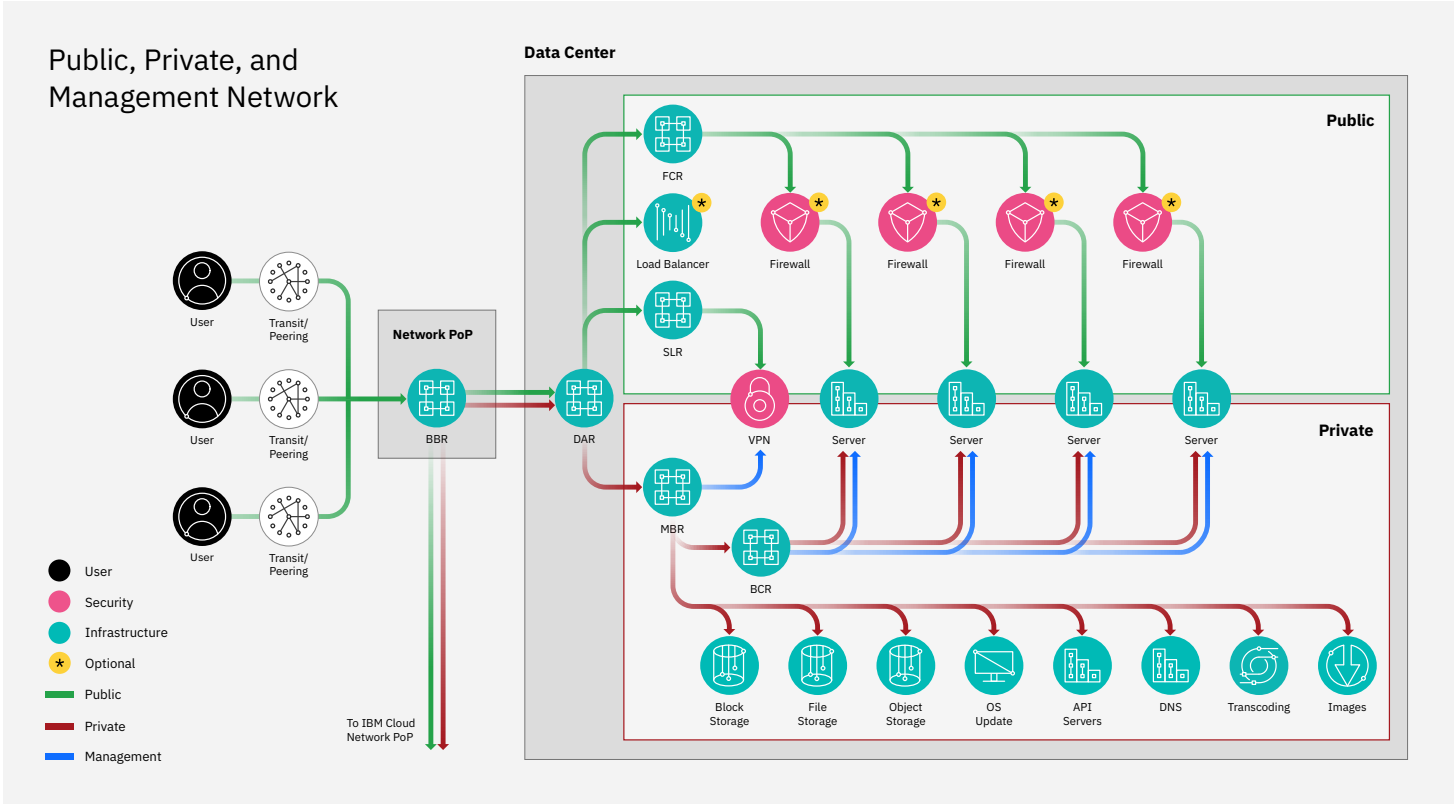
The IBM Cloud infrastructure provides on-demand cloud infrastructure as a service (IaaS) to its clients, allowing them to create scalable bare metal servers, virtual servers, or hybrid computing environments, via IBM Cloud's Client Portal, leveraging global data centers and points of presence (PoP). Refer to the IBM Cloud Portal section below.

IBM Cloud's IaaS is built using a Network-Within-A-Network topology that provides remote access to allow clients the ability to build and manage computing environments remotely. IBM Cloud'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 connects to the closest PoP and travels 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 client's servers (bare metal or virtual) in IBM Cloud data centers around the world. Data can be moved between servers through the private network. Clients 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 environment 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.



**IBM Cloud Portal**

IBM delivers its IaaS through the IBM Cloud Portal, which is an IBM Client Relationship Management (CRM) system used to track clients' hardware and services. It allows clients to manage and configure their cloud environments. Client capabilities include management of system and network devices provisioned by the client, account management, ordering and deployment, and client support.

IBM Cloud Portal has two components: (1) the internal management portal as viewed by IBM employees and (2) the Client Portal available to the users of IBM's IaaS. The Client Portal allows users to:

- Create and manage tickets, support requests and inquiries and resolution
- Review account information
- View logs and certain configuration data regarding their purchased solutions
- Maintain client provisioned firewall and DNS configurations that affect their base metal servers
- Perform functions such as OS reloads and access Rescue Layer. Rescue Layer is an innovative automated system for restoring and repairing servers after crashes or failures. Rescue Layer can be used to reboot a failed server into RAM-Disk Unix, Linux or Windows PE rescue kernel.
- Purchase or upgrade servers to initiate the automated provisioning process for new systems
- Scale computing resources on demand - adding or resizing instances as needed but without having to purchase physical systems. Public and private virtual nodes are available.

**Definitions**

- Bare Metal Servers are dedicated physical servers that allow direct access to physical hardware to support high demand and processor-intensive workloads.
- Virtual servers are computing "instances" that are complete computing environments that include a full hardware and software stack accessed and controlled over the Internet.

IBM Cloud personnel also have access to the IBM Cloud Portal to set up and configure purchased solutions, assist in troubleshooting issues, and respond to client requests.

## Client Access to Infrastructure

### IBM Cloud Portal

Clients use IBM Cloud Portal to track availability of hardware and services, as well as manageand configure network devices. Through this portal, clients can perform the following functions over their network devices:

- configure network devices
- manage account provisioning
- order and deploy new devices
- request IBM Client support (i.e. support requests and inquiries)

### IPMI Management Network

Secure connection to the Intelligent Platform Management Interface (IPMI) can be used for out-of-band management, server control, and server rescue through an encrypted VPN tunnel. Clients interact with their IBM Cloud devices through IPMI View, using a backend IPMI address.

### Private/Public Network

IBM's public network offers carrier grade Internet connectivity to multi-home backbone carriers. This network is capable of gigabit speeds from the server to the Internet.

The private network facilitates complete control over server management while adding convenient and secure services. There are three functional areas to the private network:

- Server-to-Server
- Server-to-Services
- VPN to VLAN

Section 2:

# IBM Cloud Infrastructure Quality Management System

IBM Cloud operates and maintains its IaaS under a quality management system that has been assessed and certified as described throughout this document. Documented control of its people, processes, data centers, suppliers, service management, change management, and incident response, enables IBM Cloud to deliver a secured, controlled global cloud infrastructure.

## Section 2a: Organization & Governance

**Personnel Hiring & Training**

IBM Cloud maintains personnel policies and procedures which are designed to recruit, develop, and retain competent and trustworthy personnel who facilitate an effective internal control system. IBM recruits employees and contractors who are qualified applicants and selected based on business needs, job-related requirements as per stated job descriptions/postings, and each applicant's individual qualifications and skills. After the prospective new hire is identified, background due diligence procedures are performed based on an established set of Global Employment Verification (GEVS) criteria applicable to regulars, non-regulars (fixed term, supplemental), and interns/students. New hires participate in a new-employee orientation class, which includes such topics as IBM values, Business Conduct Guidelines (BCG), IBM tools, performance measurements, and the Concerns and Appeals Program. The new hire must certify their understanding of IBM's BCG and re-certify annually thereafter. Employee certification is tracked by management.

IBM is dedicated to training and developing high performers through their talent development and training programs. IBM identifies and focuses employee development on skills that are relevant in the industries it serves. Employee skills development is accomplished through an array of educational and training opportunities, including traditional classroom and a variety of web-based, self-paced (e-Learning) courses. Employee skills development credits are monitored and tracked by management to help ensure minimum levels of training are being achieved. Additionally, as part of learning their job responsibilities, personnel increase organizational capabilities through "hands-on" training, utilizing documented functional guidance, corporate directives, and desk procedures. Personnel are cross-trained, as appropriate, to facilitate adequate backup coverage.

### GxP Client Considerations

IBM clients are responsible for ensuring their personnel have the education, training, and experience to perform their assigned job functions. When IBM Cloud services to configure infrastructure support of GxP systems, the experience level with IBM services, such as the IBM Cloud portal, should be taken into consideration when hiring and/or training personnel. Refer to section 2b for further information on client management of system configurations.

Clients should consider updating their own policies and procedures and/or any other organizational documents that cover the following areas:

- Personnel education and experience requirements
- Training curriculums management
- Training on Electronics records and electronic signatures (21 CFR Part 11)
- Access management
- Computer systems validation

**Client Management**

Service-level Agreements (SLAs) are used to define the support services provided by IBM through the IBM Cloud infrastructure to the IBM Client. SLAs are made up of the following:

1. **Primary Cloud Services Agreement** - The agreement under which clients order cloud services from IBM. The agreement details the scope of IBM support including a summary of services provided to the client, as well as the requirements when providing said services, such as content and data protection requirements, liability requirements, and governing laws/geographic scope requirements.
2. **Service Description (IBM Cloud Services Description)** - The Service Description describes IBM Cloud infrastructure services available to the client. The description includes explanations of the cloud services, specific SLA scenarios, charges, renewals, suspensions, terminations, etc.
3. **Detailed System Requirements** - Any additional requirements agreed between IBM and Client that are not covered in the aforementioned section contracts.

### GxP Client Considerations

Clients shoud use SLA documentation to define IBM areas and processes that impact client's GxP systems.

**Third Party Service Considerations**

IBM categorizes its subservice providers into one of three categories:

**IBM subservice providers – no client interaction:** suppliers who provide tools or services used by IBM Cloud that do not interact with the IBM Client (i.e. ticketing system software providers, change management software providers, etc.).

**IBM subservice providers – indirect client interaction:** suppliers who provide tools or services used by IBM Cloud to assist in support of the Client. IBM works with the supplier on behalf of the Client to make changes or configurations to the level of support and oversees vendor compliance and remediation of non-conformances. (i.e., tools such as Direct Link).

**IBM subservice providers – direct client interaction:** suppliers who provide tools or services used by Clients within the IBM Cloud infrastructure. IBM Clients interact directly with the supplier to make changes or configurations to the level of support or manage supplier non-conformances (i.e. Sysdig, LogDNA).

IBM maintains a consistent supplier qualification, control and management program to drive compliance by all IBM subservice suppliers. Suppliers must initially go through a rigorous process to ensure that they are able to provide the quality of service, maintain its availability, and meet the demands required. The first step in this process is a risk assessment of the process/product and in-depth review of the contract if one currently exists.

The contracting process includes discussions on services to be provided, as well as agreement to security and privacy standards by all parties. IBM and the supplier must agree on the responsibility of each aspect of the contract prior to execution. Any gaps must be addressed or a solution agreed upon to mitigate the risk. Post contract execution, the supplier management group within IBM regularly evaluates the supplier and acts if the supplier is found in non-compliance to agreed upon terms.

Although IBM Cloud contracts with a variety of data center suppliers to provide physical data center sites, IBM Cloud retains ownership of the physical and environmental controls and monitors each physical environment and the actions of each facilities supplier. The facility management suppliers are in constant contact with IBM Cloud infrastructure site managers through real estate managers and facility engineers. In addition, a portal is available for tracking tickets and issues between IBM and the facility management suppliers.

**Policies & Procedures Management**

IBM has a group of policies and procedures that define the Quality Management System. Policies are reviewed and updated on an ad hoc basis for any administrative changes or content modifications and on a biannual basis (at minimum) to ensure applicability to the IBM Cloud infrastructure environment. Policies are available to relevant IBM employees for viewing and any changes to a policy will be communicated to affected managers and stakeholders.

Policies and Procedures areas include, but are not limited to:

- Infrastructure maintenance
- System Information integrity
- Vulnerability and issues management
- System and services acquisition
- System and communication
- Audit and accountability
- Change management
- Configuration management
- Personnel hiring & training

### GxP Client Considerations

Clients should consider how to best incorporate IBM Cloud tools and approaches into their policies and procedures for:

- Supplier management
- Software Development Life Cycle (SDLC)
- Hardware qualification
- Document management

**Quality Assurance**

A quality assurance team exists within the IBM Cloud organization in order to assure compliance is maintained by IBM Cloud services. The team is an independent quality function and organizationally segregated from operational activities. Compliance priorities are identified and coordinated across senior management, Information Systems, networking, inventory, physical building management companies, and both internal and external auditors / assessors to ensure that compliance requirements are met, maintained and [as necessary] measured.

### GxP Client Considerations

A client quality strategy should be built upon the compounding value of:

- IBM Cloud attestations and certifications demonstrating quality and control
- IBM Cloud service technology and underlying functionality

## Section 2b: Infrastructure qualification

**New Client setup and infrastructure qualification**

Clients select the configuration and capacity of their bare metal and virtual servers, storage, and network capacity via the online portal, API, or via communication with IBM sales. The order is initiated as a ticket in the provisioning system. If the resources are available, they are automatically assigned to the client and displayed to them in the IBM Cloud Portal. Email confirmations are also sent to the client that confirm their order has been completed. If the resources are not available in their selected configuration, the ticket is assigned to the data center staff. The data center staff make the requested hardware changes and then return the server back to the control of the automation.

Infrastructure attributes and lifecycle are cataloged and tracked in the IBM Cloud Portal. IBM uses an additional automation to verify physical switch attributes and obtain MAC addresses of bare metal servers. These processes create logs that can be used as part of a client's GxP validation.

**Configuring infrastructure**

Changes to the network configurations are made through the console by IBM Network Engineers or via IBM Cloud Portal automation. Changes made through the IBM Cloud Portal tend to be common updates, such as VLAN or subnet modifications. Console based changes are performed by trained 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, network changes are tested 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 clients regarding any potential for outage and 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. Clients are notified of widespread service disruptions through the Client Portal via notification banners.

IBM uses a server configuration management tool that is used to automate the configuration and maintenance of every internal system within the IBM Corporation. The tool tracks all servers (virtual or bare metal) throughout the corporation for their entire lifecycle. Further, the tool keeps track of "recipes" which are the configurations of how a specific server should be set up. When a server first comes online, the server is bootstrapped with the automation so that it has the baseline recipe and can run in the background to monitor the integrity of the server as it relates

to the baseline recipe. The configuration tool runs a diagnostic check every 30 minutes and automatically corrects the server back to baseline if there is an irreconcilable variance. In the event that a server has unexpected deviations, the tool emails the administrative teams to investigate the issue.

**Maintaining your infrastructure**

The overall change management process addresses implementations that may potentially impact the environment and includes changes to infrastructure and systems. IBM's change management process does not include changes to client's virtual servers, bare metal servers or client managed network devices. Customers are able to configure and make changes to their systems and configurations through the IBM Cloud Portal, IPMI via the management network, and by directly interacting with their systems over the public or private networks.

IBM is responsible for implementing changes in the IT environment including changes to individual components (e.g., equipment, systems software 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 changes are facilitated by a management system governing implementation and auditing. Controls exist to covering the identification of changes, prioritization of changes, emergency procedures, impact assessment and change authorization.

Changes are subject to approval and testing prior to implementation. Testing and back out plans are required depending on the change type. Certain change types do not require testing or back out plans, as testing may not be deemed 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 record.

All changes 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.

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

**Changes to IBM Cloud Portal**

Changes to IBM Cloud Portal are subject to approval and testing prior to implementation. All changes require a formal change record. 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 record.

All changes 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. Changes to the infrastructure that do not have an impact on client service do not require approval.

All change windows/maintenance schedules are distributed via notifications in the IBM Cloud Portal to notify users of upcoming changes and outages. For individual changes that may impact/disrupt the production environment, ticket owners prepare client facing statements that are communicated to the NOC for distribution.

## GxP Client Considerations

**Software Validation**

IBM Cloud clients validating a GxP system typically must include hosting infrastructure in the validation. To help clients with their obligations, the IBM Cloud infrastructure and provisioning tools are qualified and certified with ISO 9001. IBM Cloud is responsible for ensuring IBM Cloud services conform to client requested specs, SLAs and commercial IT standards. However, IBM Cloud does not provision or configure client-specific infrastructure as part of this IaaS offering, and IBM Cloud cannot perform GxP validation of client software systems on behalf of clients.

**Maintaining and configuring IBM client infrastructure environment**

Clients use the IBM Cloud Portal to input and document their system design requirements (specifications), and verify that systems have been built/configured according to their specifications and/or any qualification is completed. Clients may need to update the following documentation to reflect how they utilize the IBM infrastructure and the IBM Cloud Portal:

- Change Control Procedure
- Configuration Management Procedure
- Production Release Procedure
- Audit and/or Monitoring Procedures
- Configuration documentation
- Application Source Code
- Installation qualification/Operation qualification (leveraging IMS portal documentation)

Visualized below are all IaaS components with defined roles and responsibilities over component change and design.

**Maintenance:** relates to any change to the physical and/or source code of an IaaS component (i.e. hardware changes, install of version upgrades and patches)

**Configurations:** relates to any modification of settings using menu options with no impact to source code (i.e. changes to backup frequency, opening a firewall port)


| Infrastructure Product | | Maintenance | Configurations |
|---|---|---|---|
| Storage | **IBM Cloud File Storage**<br>Persistent, high performance, network-attached storage accessed with NFS. Many features are included to support flexible architectures. |  |  |
| | **IBM Cloud Block Storage**<br>Persistent, high performance iSCSI storage that is provisioned and managed independently of compute instances. ISCSI-based Block Storage LUNs are connected to authorized devices through redundant multi-path I/O (MPIO) connections. |  |  |
| | **Cloud Object Storage**<br>Persistent object storage replicated across multiple geographies with encryption built-in. |  | |
| | **eVault Backup**<br>Automated agent-based backup system that is managed through the eVault WebCC browser-based management utility, providing users with a method to backup data between servers in one or more data centers on the IBM Cloud Network. |  | |
| Compute | **IBM Cloud Bare Metal Servers**<br>Bare Metal Servers that are hourly or monthly, single-tenant servers dedicated to each client. They are not shared in any part, including server resources, with other customers. Each client manages their own servers, which are provisioned without a hypervisor underneath. Servers can be deployed in one or more datacenters. |  |  |
| | **IBM Cloud Virtual Servers**<br>Scalable virtual servers that are purchased with dedicated cores and memory allocations. |  |  |
| | **Hardware Security Module**<br>State-of-the-art, dedicated storage for encryption keys. |  | |

IBM Customer

| Infrastructure Product | | Maintenance | Configurations |
|---|---|---|---|
| Network | **Content Delivery Network**<br>A collection of edge servers that are distributed through various parts of the country or the world. Web content is served from an edge server, which is located in the geographic area closest to the customer who requests the content. |  |  |
| | **Direct Link**<br>Allows client to connect directly to an IBM private network within the same geographical location of the physical cross-connect using fiber cross-connected patches. |  |  |
| | **DNS**<br>Resolves human-readable hostnames into machine-readable IP addresses. All manner of detail records can be captured, allowing any hostname to be assigned to a host. |  |  |
| | **Cloud Internet Services**<br>Enables the client to progress quickly by establishing defaults, which can be changed easily using the API or UI. |  |  |
| | **Cloud Load Balancer**<br>Helps clients improve availability of their business-critical applications by distributing traffic among multiple application server instances, and by forwarding traffic to healthy instances only. |  |  |
| | **Virtual Router Appliance**<br>Allows the user to selectively route private and public network traffic through a full-featured enterprise router with firewall, traffic shaping, policy-based routing, VPN and a host of other features. (Also known as Vyattas) |  |  |
| | **Fortigate Security Appliance**<br>A dedicated single-tenant network device connected upstream from a server that protects any or all servers on a public VLAN. |  |  |
| | **Hardware Firewall (Shared)**<br>Blocks unwanted traffic from a server before the traffic ever reaches the server. The Hardware Firewall (Shared) leverages a multi-tenant enterprise platform to protect an individual server. It delivers virtualized network security through its Virtual Domain (VDOM) technology, providing virtualized security domains that are separately provisioned and managed. |  |  |

## Section 2c:
## CAPA & Incident Reporting

**IBM Security and Incident Response**

IBM is responsible for monitoring, responding, and alerting clients to incident and security events that may affect the security or availability of the system.

IBM'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 Operations Center (NOC) and Security Operations Center (SOC) are responsible for monitoring the IBM environment and managing identification, response and resolution of incidents. Through the NOC and SOC, IBM provides 24/7 monitoring of in-scope data centers. IBM utilizes a variety of tools 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.

The NOC 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 NOC and SOC are notified of incidents in a variety of ways:

- E-mail received from public aliases or internal aliases.
- Phone calls from telecommunication circuit providers, network engineers, clients, peering ISPs, transit providers, data center suppliers or other internal groups at IBM.
- Review of tickets escalated to the NOC/SOC through the "Network Operations" or "Security Operations" ticket queues.
- Network monitoring alerts received from a variety of tools, including: PeakFlow, Netcool, IP Alert, Nagios, GROK (syslog parser), and Regex.
- Security monitoring alerts from a variety of Security Information and Event Management (SIEM), Endpoint Detection and Response (EDR) and Threat Intelligence Platform (TIP) tools.

The team member that identifies the issue or receives the initial notification of an incident (NOC) or security incident (SOC) creates a ticket unless an existing ticket already exists. NOC tickets are documented in the IBM Cloud Portal as Unplanned Incidents in Progress (UIP), and SOC tickets are documented in the incident management tool as Security Incidents in Progress (SIP). If a ticket regarding the same incident already exists, any new information is documented in the existing UIP or SIP notes. UIPs and SIPs are classified based on criticality. Each UIP 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, UIP and SIP ticket classification further defines the incident's importance and urgency. There are three elements involved in incident classification:

**Scope:** How many clients are affected?

**Severity:** How strongly affected those within the incident scope are, with emphasis given to actual incidents over changes made to working networks and services?

**Service:** What is the actual service impacted?

Once a UIP or SIP is created, assigned and classified, a structured and documented process engages until successful resolution. Incident escalation occurs as necessary at the end of each NOC or SOC shift and when incidents exceed the skill set of the UIP/SIP ticket owner. Internal communications are distributed, when required, by the NOC 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 Client Event Notification System (also known as Event Management).

Any vulnerabilities that are found, and are a direct result of a misconfiguration by IBM Cloud infrastructure, will require a root cause analysis. This information is presented to clients upon closure of the incident once requirements are met. IBM also uses this information to implement preventative measures. Closing a UIP/SIP ticket indicates that the incident has been resolved.

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

**Client Initiated Incident Reporting**

The incident management process defines the requirements for responding to client raised incidents within the required response time-frame, per the defined policy. Clients initiate support requests and inquiries via the IBM Cloud Portal. IBM personnel record each potential incident in the appropriate ticketing system and track the incident from identification to resolution. Additionally, an external facing resource (Abuse Team) is available for receiving incoming reporting of vulnerabilities, risks or incidents by external parties. Issues reported are routed to the Abuse team and analyzed. IBM Cloud Portal abuse tickets are created as required and monitored to resolution.

**Corrective Action Preventive Action Plans**

Corrective and Preventive Action (CAPA) plans are opened through escalation of client-initiated incidents or in response to findings from external audits, internal audits, and self-identified gaps. A CAPA identifies tasks that need to be accomplished in order to address an instance of non-compliance identified within the commercial operating environment. CAPAs track remediation activities that need to be completed in order to mitigate identified security weaknesses. The table below describes the typical CAPA process for IBM Cloud.

| IBM Cloud infrastructure CAPA process components | Operational CAPAs | Compliance CAPAs |
|---|---|---|
| | Opened through escalation of incidents identified through security monitoring by the SOC. These incidents are specific to IBM administered systems only and are not applicable to customer managed systems.<br><br>Opened through escalation of incidents identified through availability monitoring by network operations or third party publications (i.e. trade group bulletins, network vendor reports). | Opened as a result of internal audits, external audits, certification reviews and gap analysis reviews. |
| Root Cause Analysis | Performed by the internal system owner/administrator and reviewed and approved by Cyber Security Incident Response Team (CSIRT) after formal escalation driven by impact of incident.<br><br>Performed by technical team via UIP process. | Performed by IBM Cloud quality team via ticketing system software. |
| Remediation Plan & Approval | Remediation plan and approval recorded in the Incident management tool owned by the SOC.<br><br>IBM Cloud quality team records remediation plan and approval in ticketing management software. | IBM Cloud quality team records remediation plan and approval in ticketing management software. |
| Verification of Remediation | Performed by the IBM Cloud quality team as part of CAPA closure tracking. | Performed by the IBM Cloud quality team as part of CAPA closure tracking. |

### GxP Client Considerations

In order to receive, assess and rely upon incident reports and CAPA actions from IBM, clients should evaluate and update their SOPs as needed.

## Section 2d: Data Integrity

IBM categorizes client data as either:

**Content** - defined as all data, software and information that the Client or its authorized users provide, authorize access to, or input to the Cloud Services.

**Client Personal Data** - ent personal data that is processed by IBM on behalf of Client in order to provide Cloud Services and other services agreed in the SLA. Client

(a) is the sole Controller of Client Personal Data or (b) has been instructed by and obtained the authorization of the relevant Controller(s) to agree to the Processing of Client Personal Data by IBM.

**Account information** - Data about Client, such as Client name, account ID, Client history, etc. This data is considered non-Client owned data.

**Data retention**

IBM will return or remove client content from IBM computing resources upon the expiration or cancellation of the Cloud Service, or earlier upon Client's request. IBM does not archive content; however, some content may remain in Cloud Service backup files until expiration of such files as governed by IBM's backup retention practices.

**Backup and restore**

IBM provides back-up services in the form of the EVault product. EVault Backup is an automated agent-based backup system that is managed through the EVault WebCC browser-based management utility, providing users with a method to backup data between servers in one or more data centers on the IBM Cloud Network. Client administrators can set backups to follow an hourly, daily, weekly, or custom schedule that targets full systems, specific directories, or even individual files. Additional plug-ins allow for compatibility with software like Microsoft Exchange and Microsoft SQL, as well as other types of third-party software and enable users to perform a Bare Metal Restore, when necessary.

**Making backup configurations available**

IBM is responsible for the availability of the system and as such IBM Cloud Portal data is replicated to another geographically separate server to help ensure availability of the Client Portal and certain support services. The Client Portal and its internal functionality is provided via the portal's 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. IBM monitors the replication continuously to validate it is continuously running successfully.

On an annual basis, IBM performs a failover test of the IBM Cloud Portal from the primary location to the secondary location to verify that the portal 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.

### GxP Client Considerations

The IBM client is responsible for the data integrity of their proprietary data housed on the IBM infrastructure. This includes but is not limited to setting up, scheduling, and performing backups and backup recovery procedures.

Scheduling backup of Client bare metal and virtual servers hosted on the IBM Cloud infrastructure and performing restore tests on a periodic basis are not included within the responsibilities of IBM IaaS and falls to the Client to execute and maintain.

## Section 2e:
## 21 CFR Part 11 Considerations

**Activity Timestamps**

Clients are able to utilize “"time.service.networklayer.com" for time services. “Time.service.networklayer.com” is a NTP time service on the back-end private network which is offered as a convenience to clients. Time services are linked to “time.softlayer.local” via NTP. The server is synchronized with one of the following:

– server 3.us.pool.ntp.org

– server time.nist.gov

– server time-a.nist.gov

– server ntp-1.mcs.anl.gov

Currently IBM does not offer any Stratum level guarantee on this service. Currently, some of the time servers are at Stratum 3 while some are at Stratum 4.

**Considerations related to the security of the audit trail**

Several topics covered in this paper relate to the security and integrity of the audit trail, including user access management, audit log security, database security, server qualification, and monitoring of security events. Appropriate controls are in place to ensure that the activity logs on infrastructure components cannot be altered.

### GxP Client Considerations

The security and integrity of the audit trail of any software hosted in the IBM Cloud environment is the responsibility of the Client.

## Section 2f:
## Access Management

Two environments exist for access management processes:

**IBM Cloud environment** - Point-and-click Web-based solution for IBM account management. Within the IBM Cloud Portal, there are various categories that contain myriad related tools and features, from user details and billing to device management and load balancing.

**IBM environment** - All systems utilized by IBM in support of the IBM Cloud infrastructure

**Other access considerations**

IBM has configured minimum requirements for Active Directory passwords, including minimum character length, complexity, password history, and expiration. If accessing the IBM environment from outside an IBM office location, IBM employees are required to access the IBM 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 access to the IBM network are authorized and access is granted based on job responsibilities. Certain privileges granted in Active Directory allow authorized IBM employees to access the infrastructure and network devices supporting the IBM Cloud Portal. A quarterly employment revalidation is performed over IMS and a quarterly business need revalidation is performed over Active Directory in accordance with the revalidation policy to determine that IBM privileged user ID access is still required. 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 within five business days of termination.

| | Client | IBM |
|---|---|---|
| IBM Cloud Portal | Client interactions with the IBM Cloud Portal are restricted based on the authorization level requested by the user. If the user is a "master" (a user with all privileges granted to a Client using the Portal), that user can create other user accounts with varying levels of authorization. Within the portal, the Client manages the users within their respective organization and related permissions. | IBM personnel access the IBM Cloud Portal to investigate Client issues and to provide technical support. There are two primary mechanisms for an IBM employee to modify/update a Client's Bare Metal Server: through the IBM Cloud Portal and its functionality, or through directly accessing the Client's environment. Credentials associated with a Client's Bare Metal, Virtual, or Hybrid environment are stored in the portal to assist in troubleshooting issues. To access the portal, employees log in with their same credentials to the portal. |
| Bare Metal Servers & Virtual Servers | Clients are solely responsible for managing their Bare Metal and Virtual Servers. | Support personnel cannot directly access Client Virtual Servers, and in the rare instance where support is required, it is provided through the XenCenter management console. Bare Metal and Virtual Server technical support provided by IBM is at the direction and sole discretion of the Client and not within the boundaries of the system. |
| IBM Internal Environment | Clients cannot directly access the IBM environment. | Access to the IBM environment by IBM personnel requires unique user credentials authenticated through IBM's Active Directory. Active Directory is the central user administration tool and provides access to the IBM network. To access infrastructure systems, privileged employees two factor authenticate (credentials and token) to a bastion host through which they can then authenticate into other infrastructure devices in the environment. |

## GxP Client Considerations

Clients should maintain documentation in support of the following access areas:

- Managing and reviewing client access to IBM Cloud Portal;
- Verifying that only authorized and properly trained Client personnel are allowed direct logical access to virtual servers
- Client logins to the IBM Cloud Portal and virtual servers (including the mobile website and mobile applications), VPN, other Client portals, and IaaS component admin consoles are appropriately administered by user entities via the following controls:
  - Passwords are changed periodically
  - Passwords are kept confidential
  - Security violations are monitored and followed up as necessary
  - Provisioning of new Client users and granting of additional Client access permissions are properly authorized
  - Termination processes include timely notification and disabling of access rights

## Section 2g: Physical Security & Environmental Controls

The physical and environmental protection policy is part of enterprise-wide implementation of approved operating policies and is consistent with other company policies. This policy is intended to summarize how physical and environmental protection controls are implemented within IBM facilities.

IBM provides the following support for the physical security and environmental control of their data centers.

### GxP Client Considerations

IBM's policies and procedures are only applicable to the supporting infrastructure and the IBM Cloud portal. IBM Clients maintain sole control of their systems and workloads; IBM has limited visibility and no control over Client software systems. Development, documentation, and dissemination of Client site physical and environmental protection policies and procedures are Client responsibility.

## Facilities

### Physical Security

- Server rooms (SR) seperated 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
- Key card proximity systems at each facility and server room
- Full time on-site manager and facilities team
- Surveillance cameras
- Approved personnel based on their job responsibilities
- Monitoring and logging of key card access attempts
- Visitor protocol

### Environmental Controls

- Fire detection and suppression systems
- Backup power, including uninterruptible power supply (UPS) units and redundant generators
- Power distribution units (PDU) and electrical panels
- Heating and cooling (HVAC) mechanisms
- Periodic reviews and testing performed by specialized and trained security personnel, facility provider engineering personnel and IBM personnel to monitor various aspects of each facility

# Acronyms/Terms

**API:** Application Programming Interface

**BCG:** Business conduct guidelines

**CAPA:** Corrective Action Preventative Action

**CPU:** Central Processing Unit

**DNS:** Domain Name System

**EMA:** European Medicines Agency

**FDA:** U.S. Food and Drug Administration

**GCP:** Good clinical practices

**GEVS:** Global employment verification

**GLP:** Good laboratory practices

**GMP:** Good manufacturing practices

**GPVP:** Good pharmacovigilance practices

**GxP:** Collective set of globally accepted current "good practices" with respect to quality.

**HCLS:** Healthcare and Life Sciences

**IaaS:** Infrastructure as a service

**IMS:** Internal management system client portal

**MAC:** Media Access Control

**MOP:** Maintenance Operation Protocol

**NOC:** Network Operations Center

**NTP:** Network time protocol

**OS:** Operating System

**PoP:** Points of presence

**QMS:** Quality Management System

**SAN:** Storage Area Network

**SDLC:** Software development lifecycle

**SIP:** Security incidents in progress

**SLA:** Service Level Agreement

**SOC:** Security Operations Center

**SOC report:** Service Organization Control report

**Stratum:** reference clock source that relays UTC (Coordinated Universal Time) time

**TACACS**: Terminal Access Controller Access Control System

**UIP:** Incidents in progress

**VLAN:** Virtual local area network

**VPN:** Virtual private network

**Workload:** Amount of processing (data, files, information) used to execute computing tasks.

---


IBM Corporation
Route 100
Somers, NY 10589

Produced in the United States of America
August 2019