A. System Overview

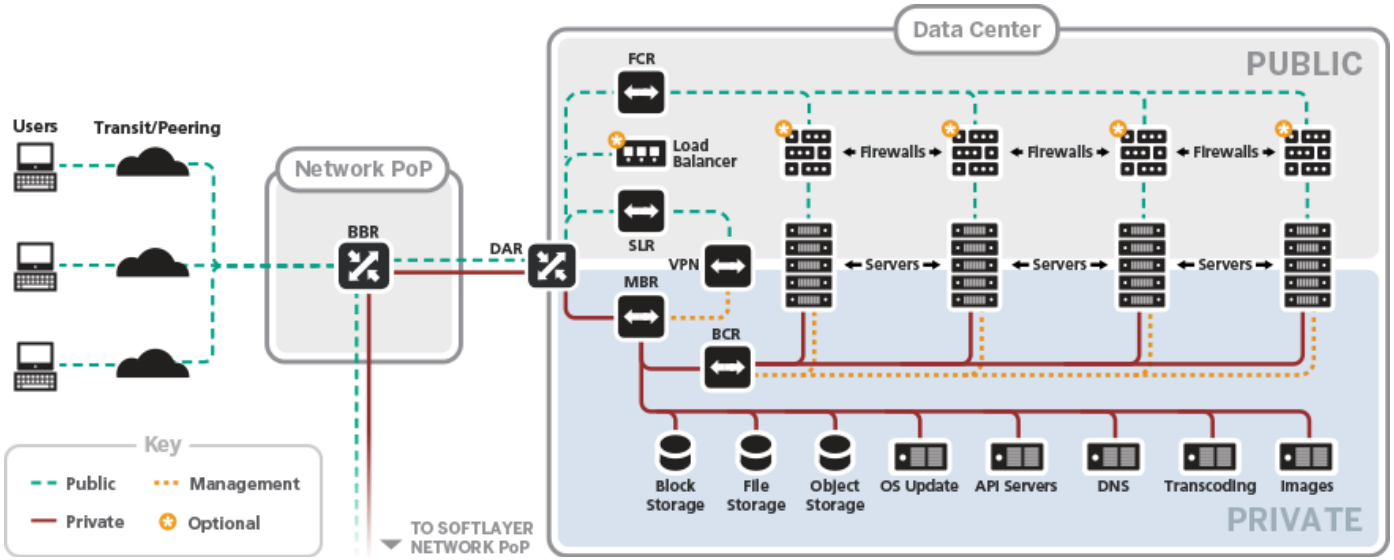
Background

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

SoftLayer’s 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. SoftLayer’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 SoftLayer 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 SoftLayer 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.

Public, Private and Management Network Diagram:



SoftLayer delivers its IaaS through the Internal Management System (IMS) customer relationship management (CRM) system, which is an internally developed customer relationship management 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 SoftLayer's IaaS. The Customer Portal allows customers to:

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

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

- Virtual servers are computing "instances" that are complete computing environments that include 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.

- Bare metal servers are dedicated physical servers. Bare metal servers allow direct access to physical hardware to support high demand and processor-intensive workloads.

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

Boundaries of the System

This report covers the services managed by SoftLayer, including global data center physical locations, the IMS portal and the supporting infrastructure devices. Additionally, this report includes network devices that are managed by SoftLayer supporting the IMS portal and infrastructure including hypervisors and network devices that support customer environments but are not provisioned/managed by customers within the SoftLayer IaaS. The report includes supporting services to the virtual and bare metal services, such as storage. These devices can be locally attached, accessible by API (such as Object Store), 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. Within each customer environment, servers, VMs and other systems/devices are managed by SoftLayer's customers and are not included within the boundaries of the system. This report does not extend to the workloads (data, files, information) sent by SoftLayer IaaS customers to the SoftLayer IaaS system. The integrity and conformity with regulatory requirements of such data are solely the responsibility of the applicable SoftLayer IaaS customer. Additionally, this report does not extend to business process controls, automated application controls, or key reports.

SoftLayer provides services to the Federal government and Department of Defense (DoD) via the FedRAMP and Defense Information Systems Agency (DISA)/DoD programs in two data centers (DAL08 and WDC03). A separate instance of IMS (FedIMS) provides provisioning functionality and infrastructure management. These data center facilities are included within the physical security 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 SoftLayer's IaaS and customers' hosting environments utilizing SoftLayer's IaaS, and does not include controls over other services. SoftLayer also provides enterprise-class tools to help mitigate potential security risks and ensure availability. Tools provided by SoftLayer 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 SoftLayer's other services and tools.

Components, infrastructure, network devices, software, and data center location system boundaries:

<table>
<tr><th>Service Offering</th><th>Data Center / Hardware Locations</th><th>Network</th><th>Operating System Infrastructure</th><th>System Software</th><th>Applications</th><th>Customer Data</th></tr>
<tr><td rowspan="3">IBM SoftLayer</td><td rowspan="3">30 data centers
(See Infrastructure section below)</td><td>Customer provisioned and managed network devices, firewalls and VPNs are solely the responsibility of the customer and are not within the boundaries of the system.</td><td colspan="3" rowspan="2">Customer environments (including the development and maintenance) provisioned and managed using the Customer Portal, including OS, system software, and applications are solely the responsibility of the customer and are not within the boundaries of the system.</td><td rowspan="3">Customer data is solely the responsibility of the customer and is not within the boundaries of the system.</td></tr>
<tr><td>Network devices supporting customer managed environments and managed by SoftLayer are within boundaries of the system including:
Routers, Switches, Firewalls, VPNs</td></tr>
<tr><td>Network devices directly in support of the IMS portal are within the boundaries of the system including:
Routers, Switches, Firewalls, VPNs</td><td>Operating systems directly in support of the IMS portal are within boundaries of the system including:
Linux, UNIX, Windows, CentOS</td><td>System software directly in support of the IMS portal are within boundaries of the system including:
Radius, Citrix, Active Directory</td><td>Internal Management System (IMS)/ Customer Portal</td></tr>
</table>

B. System Components

Infrastructure

SoftLayer provides the Infrastructure as a Service (IaaS) system using 33 locations, throughout the period May 1, 2016 to April 30, 2017, and uses multiple telecom service providers for backbone connectivity and multiple co-location management providers for data center facility management. Refer to the table below for a list of data center vendors that provide facility management services in the SoftLayer facilities included within the boundaries of the system.

Facility	Physical Location	Facility Manager
AMS01	Amsterdam, Netherlands	Digital Realty
AMS03	Almere, Netherlands	KPN
DAL01	Dallas, TX	ViaWest
DAL02	Dallas, TX	SoftLayer
DAL05	Dallas, TX	Digital Realty
DAL06	Dallas, TX	SoftLayer
DAL07	Plano, TX	SoftLayer
DAL08	Richardson, TX	Digital Realty
DAL09	Richardson, TX	Digital Realty
FRA02	Frankfurt, Germany	Zenium Technology
HKG02	Hong Kong, China	Digital Realty
HOU02	Houston, TX	SoftLayer
LON02	Chessington, London	Digital Realty
MEL01	Melbourne, Australia	Digital Realty
MEX01	Queretaro, Mexico	Alestra
MIL01	Milan, Italy	DATA4
MON01	Montreal, Canada	COLO-D
PAR01	Paris, France	Global Switch
SAO01	Sao Paulo, Brazil	Ascenty

Facility	Physical Location	Facility Manager
SEA01	Tukwila, WA	Internap
SJC01	Santa Clara, CA	Digital Realty
SJC03	Santa Clara, CA	Digital Realty
SNG01	Singapore	Digital Realty
SYD01	Sydney, Australia	Global Switch
TOK02	Tokyo, Japan	@Tokyo
TOR01	Ontario (Markham), Canada	Digital Realty
WDC01	Chantilly, VA	Digital Realty
WDC03	Ashburn, VA	Digital Realty
WDC04	Ashburn, VA	Digital Realty
CHE01	Chennai, India	TATA
DAL10	Dallas, TX	QTS
OSL10	Oslo, Norway	EVRY
SEO01	South Korea	SK

Customers with bare metal, virtual, or hybrid environments can access the servers remotely (electronically) from anywhere in the world. Certain facilities (i.e., DAL02, DAL07 and HOU02) house both co-location servers and Infrastructure as a Service (IaaS) related servers. Co-location customers do not have logical or physical access to the SoftLayer Infrastructure as a Service (IaaS) system. As such, co-location cages housing customers' servers are not included within the boundaries of the system.

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 all geographic locations, SoftLayer 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. All facilities except DAL02, DAL06, HOU02, PAR01 and SYD01 have two-factor authentication with a biometric system and require a key card. The facilities noted above are also restricted but only require key card authentication.

Each data center has a full-time SoftLayer site manager on-site. The site manager and members of the facility teams are responsible for monitoring the SoftLayer 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 SoftLayer site manager to any unauthorized access attempts. Major events are communicated by the SoftLayer site manager to the central SoftLayer 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. At each data center, failed access attempts are logged and available for follow-up as necessary. Security events are communicated to the SoftLayer site manager and to the central SoftLayer Facilities Team, as necessary.

SoftLayer 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 SoftLayer Facilities Team to provision access to SoftLayer 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 a SoftLayer employee is terminated, HR sends a notification to responsible personnel and access privileges are revoked by the Facilities Team for SoftLayer sites and the facility vendors for vendor owned sites within five (5) business days of 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). All 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 all 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.

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 at least an annual 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 SoftLayer and vendor managed facilities, SoftLayer 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 SoftLayer personnel to monitor various aspects of each facility. SoftLayer 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 quarterly frequency. Maintenance is performed at each data center facility, either by SoftLayer personnel for SoftLayer managed facilities or by certain vendors. Maintenance records are monitored and reviewed by SoftLayer site managers at each data center facility. Any deviations regarding scheduled maintenance activities are communicated to the central SoftLayer facilities team.

Software

Overview

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

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

SoftLayer Managed Component	Software Managed
IMS Database	• Oracle
IMS Infrastructure	• Various Unix OS • Windows
Customer Portal / IMS	• Proprietary Software Developed by SoftLayer

In addition, SoftLayer manages certain shared network devices that support customer environments. RADIUS software is used to manage customer's network devices.

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 all 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.

All 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. System such access is not within the scope of this report.

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 SoftLayer systems via the provided SoftLayer logins, including the mobile website and mobile applications, and the SoftLayer 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 SoftLayer Personnel

SoftLayer personnel access IMS to investigate customers' issues and to provide technical support. There are two primary mechanisms for a SoftLayer 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 SoftLayer is at the direction and sole discretion of the customer and not within the boundaries of the system.

Access to the SoftLayer environment by SoftLayer personnel requires unique user credentials authenticated through SoftLayer's Active Directory. Active Directory is the central user administration tool and provides access to the SoftLayer network. To access IMS, employees log in with their same credentials to the portal. 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.

SoftLayer has configured minimum requirements for Active Directory passwords, including minimum character length, complexity, password history, and expiration. If accessing the SoftLayer environment from outside a SoftLayer office location, SoftLayer employees are required to access the SoftLayer 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 SoftLayer network are authorized and access is granted based on job responsibilities. Certain privileges granted in Active Directory allow authorized SoftLayer employees to access the infrastructure and network devices supporting the IMS portal. A quarterly business need revalidation is performed over IMS and Active Directory in accordance with the revalidation policy to determine that SoftLayer 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.

Hard Drive Destruction

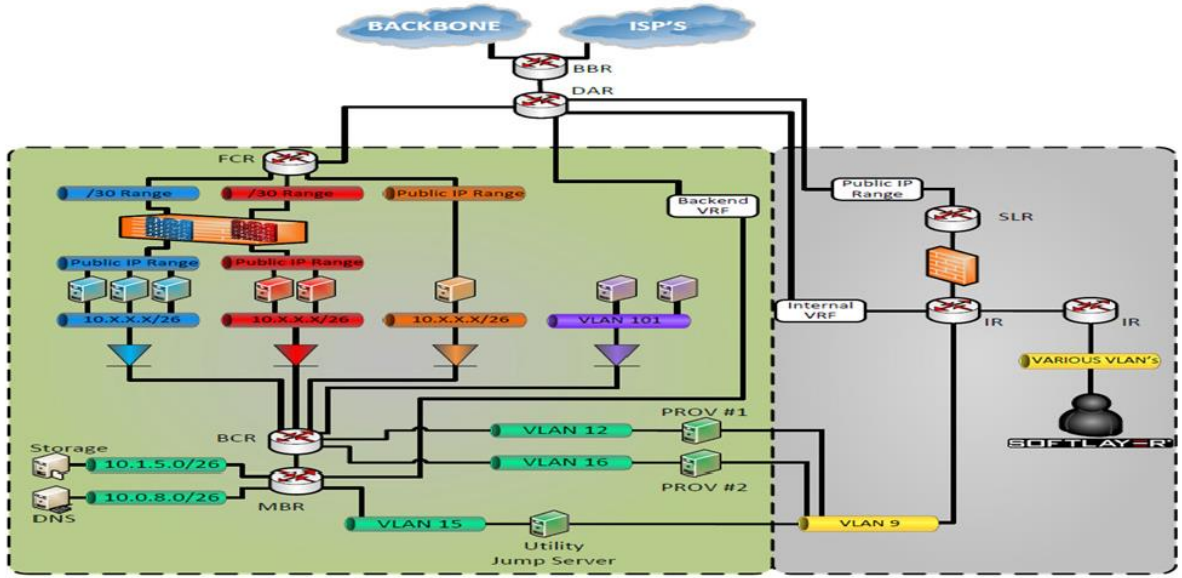
Once a drive is determined to be at the end of its functional life, the drive is requested to be physically destroyed. Upon completion, the drive is physically destroyed by bending and breaking its internal components, including the data platters. The end result of the process results in the inability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

Network Security

Network Segregation via VLANs

Internal boundaries are established and maintained through dedicated VLANs leveraging custom automated ACLs (Access Control Lists). To segregate customer traffic, SoftLayer 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 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 SoftLayer Management network.

SoftLayer VLAN Configuration:



External Vulnerability Scanning

Vulnerability scans are executed nightly against Internet facing devices within the SoftLayer environment. After the vulnerability scan is complete, a report is generated and any vulnerabilities identified are assigned severity levels based on the security policy.

Vulnerabilities identified are tracked and remediated based on severity levels, as necessary, per the requirements of the security policy. Implementation of corrective actions are administered through the change management process. Monitoring is performed to ensure the timely implementation of corrective actions.

Firewall Rule Revalidation
The SoftLayer Network Engineering team has identified the firewalls that are in place to protect the IaaS system and performs a firewall rule revalidation over the firewalls on a quarterly 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 approved by the VP of Risk Management. For any differences against the baseline configuration, the Network Engineering 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
Internal and external penetration tests are conducted on the SoftLayer 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 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. SoftLayer 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. SoftLayer 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.

Incident and Security Incident Management
SoftLayer'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 SoftLayer environment and manage the identification, response and resolution of incidents. Through the NOC and SOC, SoftLayer provides 24/7 monitoring of data centers. SoftLayer 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 Operations Center (NOC) and Security Operations Center (SOC)

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 telecom circuit providers, network engineers, customers, peering ISPs, transit providers, data center vendors or other internal groups at SoftLayer.
- Review of tickets escalated to the NOC/SOC through the "Network Operations" or "Security Operations" ticket queues.
- The NOC monitors alerts from network monitoring tools using a variety of tools, including PeakFlow, Netcool, 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 (NOC) or security incident (SOC) creates a ticket unless an existing ticket already exists. NOC tickets are documented in IMS as Unplanned Incidents in Progress (UIP) 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 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 customers are affected? Incident tickets are classified as Key Account Customer, Individual Data Center, Individual Regional/City Location or Global;
- Severity: How strongly affected those within the incident scope are, with emphasis given to actual incidents over changes made to working networks and services? Severity levels include Loss of Service, Intermittent or Degraded Service, Moderate Service Impact, Change to Service and No Impact; and
- Service: What is the actual service impacted? Services may include network or infrastructure devices, data centers, firewalls, network connectivity, DNS, Exchange Email, and/or web-based activities such as www.softlayer.com or manage.softlayer.com.

Once a UIP 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 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 Customer Portal.

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

- All 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 a NOC 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 SoftLayer's equipment, the NOC Technician also indicates what actions were applied to prevent future failure. This information is used if a Post-incident Review (PIR) is performed.

When an Unplanned Incident in Progress (UIP) or Security Incident in Progress (SIP) ticket is recorded, SoftLayer 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 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 SoftLayer 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.

System Capacity Monitoring
Capacity monitoring systems are managed by the NOC to monitor availability thresholds over the SoftLayer 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 NOC, network capacity, and network engineering teams. Upon receiving notification of a capacity breach, the NOC 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. SoftLayer 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. SoftLayer reviews and implements appropriate 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 that are not within the scope of Operations support or have no effect on services.

SoftLayer 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, 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.

Change Management Process

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

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

All 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 significant 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.

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

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

A Disaster Recovery Plan (DRP) has been designed to be used in the event of a disaster affecting SoftLayer. 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 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 SoftLayer'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 SoftLayer to help mitigate the risk of downtime.

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

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

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

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

Operations Teams	**Network Operations and Engineering Teams**	**Facilities Teams**	**Communications Teams**

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

Operations Teams	Network Operations and Engineering Teams	Facilities Teams	Communications Teams
environment and reassembled at the standby facilities, as appropriate.		○ Managing staff safety and welfare.	

People

Organization and Administration

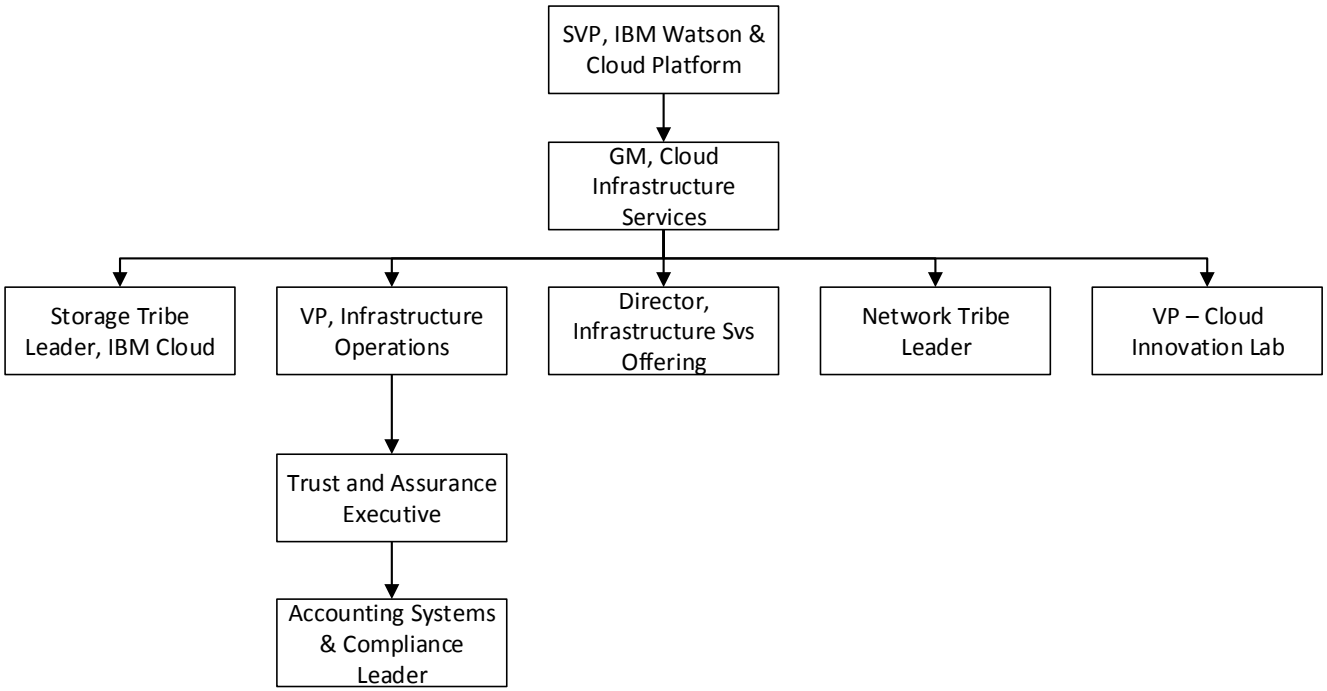
Key SoftLayer positions of authority and responsibility are documented in a formal organizational chart via IBM's BluePages, which evidences key organizational structures and reporting lines. The organizational chart is reviewed by HR and updated periodically for accuracy by managers.

Within the organization, roles and responsibilities are defined and communicated. SoftLayer leverages participation from multiple organizational levels, sites, locations, geographies and organizations are involved, as required, to perform the day-to-day oversight of service delivery related functions, matters, responsibilities and issues. Functional roles may be combined within management positions to deliver services in a cost effective manner.

The SoftLayer IaaS teams are diverse teams of development and operations professionals, which maintain and follow IBM's industry leading 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. The IBM General Manager, Cloud Services (GM) leads SoftLayer. The GM of Cloud Services for SoftLayer reports to the Senior Vice President of IBM Cloud.

The SoftLayer Chief Operating Officer oversees daily operations. Supporting the Chief Operating Officer are Senior Executives and Vice Presidents that manage and perform the daily operations of SoftLayer. These core competencies have been established to provide full capabilities to serve customers worldwide. Functional and administrative responsibilities are broadly defined and communicated through organizational charts, which are reviewed and updated regularly. The Vice Presidents guide the management of the business units.

SoftLayer Organizational Chart as of October 31, 2016


SVP, IBM Watson & Cloud Platform
GM, Cloud Infrastructure Services
Storage Tribe Leader, IBM Cloud
VP, Infrastructure Operations
Director, Infrastructure Svs Offering
Network Tribe Leader
VP – Cloud Innovation Lab
Trust and Assurance Executive
Accounting Systems & Compliance Leader

Human Resources (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. IBM has a long-standing commitment to equal opportunity due to its recognition that a diverse workforce is fundamental to its competitive success. IBM HR representatives support personnel requirements, including:

- Recruiting Employees and Engaging Contractors: Qualified applicants are selected based on business needs, job-related requirements as per stated job descriptions/postings, and each applicant's individual qualifications and skills.
- Talent Development and Training: 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 ensure minimum levels of training are being achieved.
- New Hire Orientation: New employees joining IBM participate in a new-employee orientation class, which includes such topics as IBM values, Business Conduct Guidelines, IBM tools, performance measurements, and the Concerns and Appeals Program.
- Job Training and Cross Training: 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.
- Employee Performance Management: Checkpoint is IBM's new performance management process for a high performance culture that is built on clear strategy and priorities and fueled by feedback. IBM employees set goals that are updated throughout the year to remain aligned to business priorities and the work they are doing. At year end, an employee is assessed against five dimensions (business results, client success, innovation, responsibility to others and skills). The core of Checkpoint is continual feedback to allow managers to help team members boost their performance by aligning goals and performance expectations throughout the year. By addressing performance concerns quickly, mangers can be more effective in course correcting and coaching.

Background Due Diligence (Verification)

SoftLayer's hiring practices mandate minimum criteria that each potential candidate must meet. SoftLayer is supported by IBM for background verifications. A key component of this hiring process is an established set of Global Employment Verification (GEVS) criteria applicable to regulars, non-regulars (fixed term, supplemental), and interns/students.

The following verification criteria are implemented as permitted by local law for candidates being considered for SoftLayer employment:

- Hiring government employees
- Restricted and Sensitive Hiring List
- Re-hire eligibility
- Non-Compete clause
- Denied Parties List
- Export Controls Regulation Review
- Criminal background check
- Work authorization/residence permit
- Proof of identity

- Confirmation of academic achievement

Codes of Conduct

IBM's Business Conduct Guidelines (BCG) define the standards of acceptable business conduct for all IBM employees worldwide, covering such topics as: intellectual property, gifts and entertainment, and competing fairly. IBM regularly reviews and updates the BCG content, as needed, in order to comply with IBM policies, laws, regulations, and external guidance. Employees certify their understanding of IBM's BCG as new employees and re-certify annually, thereafter. Employee certification is tracked by management.

Outside of the United States, SoftLayer employees are classified as IBM contractors. Guidelines have been set requiring that all contractors are certified through the procurement portal and tracking tool. Third party service providers are properly identified, and procedures exist for controlling the activities of contract personnel and protecting the organization's information assets.

IBM uses the Electronic Industry Citizenship Coalition (EICC) code of conduct as the code which establishes for procurement suppliers the minimum social responsibility standards expected from them as conditions for doing business with IBM. The EICC code establishes standards to ensure that working conditions are safe, that workers are treated with respect and dignity, and that business operations are environmentally responsible and conducted ethically.

Investigations

Internal Audit (IA) investigates alleged BCG violations related to financial recording and reporting, business processes or inappropriate use of IBM assets. Investigation requests can be submitted by line management, employees, Legal, Security, Human Resources, IA, and referrals from the internal appeals administrators (e.g., Confidentially Speaking or other reporting channels). Investigations may also be initiated in response to letters or complaints by customers, business partners, suppliers, and former employees. Quarterly reporting detailing the nature, status, and disposition of IA investigations (financial and BCG allegations) is provided to the Audit Committee.

Internal Audit investigation teams report directly to geography Internal Audit Directors and each Director reports to the General Auditor of the IBM Corporation. Disciplinary action recommendations from investigations associated with a financial statement impact or of a sensitive nature are brought forward and reviewed by the General Auditor, VP HR (Employee Relations and Engagement), and the Controller. Quarterly reports detailing the nature, status and disposition of Internal Audit investigations are reported to the Audit Committee.

Procedures

Customers are provided and required to agree to a Master Service Agreement (MSA)/Cloud Service Agreement (CSA) during the ordering process. The MSA/CSA acts as the formal contract and usage policy for customer users of the SoftLayer IaaS system. The MSA/CSA documents the contractual obligations of SoftLayer and the customers using SoftLayer IaaS. Any updates to the MSA/CSA are communicated to the existing customers through the Customer Portal.

The policies and procedures are a series of documents, which are used to describe the controls implemented within the SoftLayer IaaS 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 SoftLayer's commitments. These policies and procedures are available to all SoftLayer employees that support the SoftLayer IaaS system. Additionally, each of the policies and procedures are reviewed by SoftLayer management on a periodic basis, per the defined policy.

HR Policies and Procedures

IBM has a set of centralized HR policies and procedures for recruiting, developing, retaining and compensating personnel. IBM's documented Workforce Diversity Policy 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, disability, or age. Furthermore, IBM policy states that the workplace environment is free of harassment and affords reasonable accommodation for the disabled, in accordance with applicable laws.

Information Management Policies and Procedures

Information Management describes the programs, architecture framework, standards, and guidelines the IBM CIO organization has designed to achieve effective management of data as a corporation-wide asset that meets the needs of its external and internal customers. Policies governing customers are defined by each service offering management team.

IBM's IT security and availability 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 IBM's information technology services and assets. Information security and availability is managed through the following:

- Data Privacy: Standards and guidelines for collecting, using, disclosing, storing, accessing, transferring or otherwise processing of personal information are in place, allowing IBM to process information as necessary in executing a particular business purpose.
- Physical Security: Policies and procedures for managing physical access to IBM facilities, including user ID management and restricted access through the use of a badge access system.
- Logical Security: Policies and procedures for managing logical access to systems and devices, including user ID management, system health checking, patch management and vulnerability scanning.
- Network Security: Policies and procedures for managing and monitoring IMS network security, including firewall rule revalidations, network penetration testing, intrusion detection/prevention (IDS/IPS) monitoring, and secure transmission of information and data through secure file transfer protocol (FTP). SoftLayer implements these mechanisms for its internal assets and resources. SoftLayer offers a catalogue of these tools to customers but maintains no responsibility for configuration and implementation of customer's security tools and is not within the boundaries of the system.
- Incident and Security Incident Management: Policies and procedures for managing incident and security incident management, including both internally and externally reported problems and security incidents.

- Change Management: Policies and procedures for managing changes to system software and network components, including change approvals, testing and affected user communications.
- System Availability: Policies and procedures for managing system availability, including monitoring of system capacity, backing up of critical data, data restoration testing, management of environmental controls at data centers, and management and testing of the business continuity and disaster recovery plans (BCP and DRP).

IT Risk Assessment Process
SoftLayer's risk assessment process consists of the following elements:

- Assessing the sufficiency of corporate policies, procedures, systems, and other arrangements in place to control risk
- Identifying potential risks in SoftLayer's technology, products, security, and services
- Determining the level of severity for identified risk factors and evaluating the potential impact on the operating effectiveness of existing controls
- Identifying potential sources of risk and recommending areas for management to develop and implement policies and procedures to mitigate the identified risk areas
- Monitoring and evaluating the operating effectiveness of existing controls in light of changes resulting from new or renovated information systems, regulatory changes, new personnel and external security risk factors
- Monitoring the regulatory environment to determine the effect that proposed and new regulations may have on SoftLayer's service offering

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

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

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

Management Monitoring of Controls

Management Self-Assessment of Control
SoftLayer's Management Self-Assessment of Control (MSAC) is a formal and comprehensive approach of the on-going review and assessment of the internal controls that are in place to help achieve business objectives and guard against inherent risk. It includes an evaluation of the design and execution effectiveness of the internal controls that require inspection and validation to support the assessment and concludes with a documented Self-Assessment rating and corrective action plans for areas that require improvement.

Internal Audit

The IBM Internal Audit (IA) organization's authority to assess the control posture of the IBM Corporation, including SoftLayer, is formally established in a corporate directive. IBM's senior management and the Audit Committee support IA's mission by enabling the organization to be adequately staffed with the appropriate skills and audit engagements to be performed on an independent basis. Independence is addressed through its reporting structure. The General Auditor is accountable to the Audit Committee and reports administratively to the CFO.

IA 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 that is a prioritization of a defined audit universe. IA monitors and tracks line management's implementation of recommendations to address audit concerns (findings) until closure.

Internal Audit conducts an extensive training and education program to develop and maintain auditing skills.

Trust and Assurance Team

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

Controls

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

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

Data

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