IBM Services for Managed Applications

Service Guide

November 2018

Z126-8130-WW-4 11/2018

Contents

IBM Services for Managed Applications Service Guide

IBM Services for Managed Applications provides hosting and cloud services Client orders as described in this Service Guide at IBM Cloud or Extended data centers (CDCs) using IBM-provided equipment, software and applications (Services). Client can run and manage enterprise business applications from a hosted cloud environment and IBM will manage to the level of Service Client orders.

Upon acceptance of the Order and Pricing Schedule (Schedule), IBM will enable the ordered Services. Additional terms in a Schedule may modify this Service Guide.

IBM may revise this Service Guide, including rules, policies and guidelines for use of the Services, at any time. The most recent version of the Service Guide including all updates is available at the following link IBM Services for Managed Applications Guide. The latest dated Service Guide will prevail over an earlier version, except as may be expressly specified otherwise. If, however, a revision has a materially adverse impact on Client, Client can notify IBM of the impact within 30 days of the notice of the change. If IBM does not remedy the specific impacted activity within 30 days after receipt of notice from Client, Client may terminate the affected Service Component by providing IBM 30 days' notice. Materially adverse impacts do not include changes required by governmental authority or assessment of or changes to additional charges such as surcharges or taxes.

Client is responsible to comply with the policies and guidelines described in this Service Guide, and other policies published or identified to Client by IBM.

SD-1. Portal

Client is provided with access to a portal via user id and password. Client can request moves, adds, and changes to IBM-managed Service Components and enables Client to get summarized views of their deployed Services and Service Components.

SD-2. Service Infrastructure

SD-2.1. Service Location

IBM Services for Managed Applications provides service at one or more CDCs in the following locations. Service definition availability is dependent upon location as defined in the applicable Schedule.

IBM Cloud Data Centers
Primary IBM Cloud Locations
Dallas, TX, USA
Ashburn, VA, USA
London, England, United Kingdom
Frankfurt, Germany
Sydney, Australia
Tokyo, Japan

Extended Locations
Poughkeepsie NY, USA
Dallas TX, USA

SD-2.2 Service Enablement Infrastructure

Service Enablement Infrastructure (SEI) includes facilities, power, network connectivity, IBM management infrastructure and the Client hosted infrastructure and applications on an as-available basis in the data center location specified in the Schedule. Facilities include data center conditioned space (raised-floor space), including the monitored environmental infrastructure necessary to support such use.

IBM will provision the equipment, software and services for the Service infrastructure to support the services ordered by the Client in the specified data center. IBM will:

- Provide project planning and coordination to design and provide the required infrastructure and application architecture
- Install, configure and test infrastructure and IBM-managed equipment, software, and services.
- Apply IBM security policy
- Provide acceptance of Client-owned equipment shipped to an Extended CDC to support an IBM Services for Managed Applications solution
- Rack, stack and cable such equipment per the design

SD-2.2.1. Maintenance

Maintenance is performed during scheduled maintenance windows or on an as needed basis. Scheduled maintenance includes system upgrades, enhancements or routine maintenance which is announced on the Portal at least two days in advance. Maintenance determined by IBM to be an emergency will have notice announced through the Portal. Scheduled maintenance windows are excluded from SLA calculations and remedies.

SD-2.3. Support for IBM-Managed Infrastructure, Equipment and Software

IBM will notify Client within 45 calendar days after IBM becomes aware that the maintenance of any IBM-provided equipment or software is no longer supported by its manufacturer or vendor, or that repair parts and/or patches or upgrades cannot be reasonably obtained for the equipment or software, or that another reasonably satisfactory maintenance provider is not available to maintain the equipment or software ("Support Discontinuance"). IBM will inform Client if the Service will be impaired by the Support Discontinuance and advise Client of alternatives to the continued use of the affected equipment or software. If Client does not authorize IBM to replace such equipment or software after notice of Support Discontinuance or otherwise make reasonable alternative arrangements within 60 calendar days following IBM's notice, IBM shall not be liable for failure to meet applicable service level agreements arising from the failure of equipment or software subject to the Support Discontinuance.

Client will use supported versions of Client software or will purchase extended support from the applicable vendor. Should Client cease making maintenance payments or fail to purchase extended support from the applicable vendor, thereby resulting in use of unsupported versions of Client software ("Unsupported Versions"), then (a) all necessary patches, fixes, and upgrades will be performed by IBM on a time and materials basis and billed to the Client; (b) any issues under the SLA that were caused by any Unsupported Version will be excluded from the calculation of Availability; and (c) additionally, to the extent that security patches are no longer made available for any Unsupported Versions, IBM reserves the right to take any necessary action to protect IBM's network from associated vulnerabilities.

IBM may provide update/migration custom services with respect to Support Discontinuance or Unsupported Versions for an additional charge to Client.

SD-2.4. Client Managed Equipment in IBM Managed Space

The Service includes the amount of space and power to support a Client Terminated Circuit as defined in Section SD-4.2. in increments defined in the Schedule. and up to thirty minutes of Move Add Change (MAC) (as defined herein) per month. Client will have no physical access to Client-managed equipment in IBM managed space. Client-managed equipment in IBM managed space is available only in Extended CDC locations.

IBM is not responsible for, and the Service does not include, care for Client-owned materials or equipment shipped to or installed at an Extended CDC.

Prior to shipping any materials or equipment to a CDC or causing a third party to ship any materials or equipment to a CDC, Client shall notify IBM by opening a ticket using the portal or by contacting the help desk. Client will provide IBM with:

- Cabling diagram defining purpose, interfaces, ports and IPs
- List of all Client-owned materials or equipment to be located in IBM managed space, including specifications to determine rack/space/power requirements

All Client shipments to a CDC shall be identified by Client name and Client ID on the shipping label. IBM is not responsible for, and Client assumes all risk of loss for, Client-shipped materials delivered to a CDC.

SD-3. Security

IBM operates the Service Enablement Infrastructure under policies and procedures that are designed to provide physical and logical/IT security to IBM Services for Managed Applications infrastructure, facilities and systems. The IBM Data Security and Privacy Principles document defines the technical and organizational measures applied to IBM Cloud Services inclusive of IBM Services for Managed Applications.

SD-3.1. General

IBM maintains a wide-ranging security program with the objective of broadly incorporating security measures into all IBM computing and networking environments. IBM identifies the security controls for the IBM Services for Managed Applications Client environment as Information Security Controls (ISC). IBM provides this document to set forth the ISC within the scope of the applicable Schedule. IBM reviews and updates this document on a regular basis. IBM security standards specify the means and levels of protection for information in transit or in storage regarding the type of environment and media and within each information classification. The standards also specify the requirements for information destruction and media sanitization.

The Client will:

- Determine appropriate Security Policy requirements based on business objectives, assessment of risk, and interpretation of legal, regulatory and contractual obligations
- Validate that the security controls specified in the ISC meet the Client requirements
- Request exceptions to the ISC, as needed
- Notify IBM through the change request process if Client security requirements change
- Confirm (when Client discloses Client content which includes personal or other sensitive third party data to IBM for the purpose of having IBM process such data) that it has the required legal authority and provided the necessary notice and consents to do so to the extent permitted by applicable law.

SD-3.2. Certifications, Audit Reports and PCI DSS

IBM has undertaken to obtain applicable security-related certifications for certain of the Services or Service Components (or features) described in this Service Guide, including under ISO 27001. IBM will provide validation of its auditing results under these standards, where applicable, upon Client request.

IBM will provide, at Client's request, on an annual basis, a copy of the latest multi-Client Service Organization Controls (SOC) 1 Type II auditing report to Client with respect to IBM's facilities from which the Client's Services are hosted.

The Services described in this Service Guide do not store, process or transmit cardholder data but rather provide one or more infrastructure components that may be used by Clients to store, process or transmit cardholder data. Components of the hosting and IT infrastructure services described in this Service Guide may come within the scope of one or more Payment Card Industry Data Security Standard (PCI DSS) assessment activities conducted by IBM as part of one or more service-specific PCI DSS assessment(s). The Services or Service Components described in this Service Guide are subject to a PCI DSS assessment.

SD-3.3. Security Services - Included and Optional

Pricing for Included Services are included in Client's charges. Standardized of custom or optional services can be provided for additional charges. Please refer to Appendix A for additional security roles and responsibilities.

Service Feature	Included	Optional - Custom	
Primary Firewall	X		All Client solutions include an IBM-managed primary firewall. Primary firewall rules support inbound/outbound network traffic.
Software based virtual firewall	X		Virtualized Client solutions include software based virtual firewall rules that support internal network (LAN) segmentation.
Network Intrusion Prevention (NIPS)	X		All Client solutions with a software based virtual firewall include standard NIPS.
Two-Factor Authentication	X		Included for Clients who retain server administrative access to Client systems.
Anti-Virus Protection	X		Installed, monitored and managed on Windows and Red Hat systems receiving Operating System and Advanced Managed support.
Security Information and Event Management (SIEM)	X		SIEM is included for all components in IBM's Service Enablement Infrastructure (SD-2.1) used to deliver and manage Client solutions.
Vulnerability Scanning	X		Non-authenticated network-based vulnerability scanning of Client systems in internal networks is included.
Web Application Firewall (WAF)		X	Available as a standard option with an Initial service level of up to five WAFpolicies.

Service Feature	Included	Optional - Custom	
Disk Encryption		X	Encryption of Client Data is available as a standardized option on IBM Services for Managed Applications Managed Storage.
Compliance Management		X	Client specific configurations can be supported as an option.
File Integrity Monitoring (FIM) Operating System components	X		Included for IBM-managed operating systems. IBM implements file integrity monitoring by validating the integrity of the operating system using an automated verification method comparing the current file state and an IBM baseline.
File Integrity Monitoring (FIM) Application Software		X	As a standard option, IBM can implement file integrity monitoring by validating the integrity of IBM or Client Managed application software using an automated verification method between the current file state and an IBM baseline.
Host Intrusion Prevention (HIPS) – Software		X	As a standard option, IBM can implement Host Intrusion Prevention Software.
Penetration Testing	X		Included for the SEI infrastructure components.
Penetration Testing		X	As a custom option, Penetration Testing is available for Client server infrastructure components.

SD-3.4. Security Services

SD-3.4.1 Firewall

IBM installs and manages dedicated virtual infrastructure and software licensing to support Client firewall policies. As a custom option, and for additional charges, IBM can install and manage dedicated physical firewall infrastructure and software licensing to support Client firewall policies. During implementation, IBM creates initial firewall policies to restrict all unnecessary and unauthorized access to environments, and tests firewalls and networking components. Client requests for updates to physical, virtual and software-based firewall policies are made through the Move, Add, Change process.

SD-3.4.2. Network-Based Intrusion Prevention

IBM implements network-based intrusion prevention (NIPS), monitors the systems, responds to intrusion prevention system alerts and performs event correlation. A standard NIPS policy will be applied to all Client solutions.

SD-3.4.3. Two-Factor Authentication

IBM provides licensing, installation and proactive monitoring and management for two-factor authentication alerts for IBM managed servers. It is required when accessing IBM managed operating systems.

SD-3.4.4 Anti-Virus Software

Anti-virus software is installed and managed on IBM managed virtual and dedicated servers using Microsoft Windows Server, Suse and Red Hat Enterprise Linux operating system software. Anti-virus software is required for all Operating System (SD-6.4.1) and Advanced Managed (SD-6.4.2) servers.

SD-3.4.5. Security Information and Event Management

IBM will perform Security Information and Event Management services to collect and store security and audit logs for its SEI management infrastructure only. SIEM implements monitoring, correlation of events, notifications, analysis and reporting of log data.

SD-3.4.6. Vulnerability Scans

IBM will perform routine vulnerability scans on its SEI management infrastructure including the Client server infrastructure and will notify Client if an identified risk vulnerability requires Client's immediate attention. Notice of such risk vulnerabilities may include a cure period allowing Client time to resolve the vulnerability. IBM can suspend Service if Client is unable to or does not cure the risk vulnerability in the allocated timeframe or if such risk vulnerability might cause imminent threat or harm to the IBM network or use of IBM Services or network by unauthorized people.

SD-3.4.7. Web Application Firewall

As a standard option for additional charges, IBM can install and manage virtual infrastructure and software licensing to support Client web application firewall policies. Implementation and support involves the deployment and tuning of the baseline policies and adjusting the policies for client usage during the implementation phase and ongoing support of the baseline policies.

SD-3.4.8. Disk Encryption

As a standard option, and for additional charges, IBM can provide software licensing and agent installation to Client devices to encrypt Client data on the IBM managed storage disk volume.

SD-3.4.9. Compliance Management

IBM uses compliance management tools to enable compliance with IBM security policy and standards. As a standard option, and for additional charges, Client-specific configurations can be supported.

SD-3.4.10. File Integrity Monitoring

IBM implements file integrity monitoring for all IBM-managed operating systems. IBM validates the integrity of operating system files using an automated verification method comparing the current file state and an IBM baseline. As a standard option for additional charges, IBM can implement file integrity monitoring by validating the integrity of IBM or Client Managed application software using an automated verification method between the current file state and an IBM baseline.

SD-3.4.11. Host Based Intrusion Prevention

As a standard option for additional charges, IBM can implement host based intrusion prevention, monitor the systems and respond to the intrusion prevention system alerts where such option is purchased by Client.

SD-3.4.12. Client Audit Privileges

Client or Client-sponsored third-party audits of the Service, functions related to the Service or IBM facilities are not permitted unless expressly authorized in writing by IBM. Client may request an audit in writing to IBM through a service request ticket. All desired audit points should be defined in the request for review. Client is required to execute a separate agreement with IBM establishing the rates, terms and conditions

under which Client or its third-party auditor are entitled to audit a Service, functions related to the Service or IBM facilities.

SD-3.4.13. Penetration Testing

IBM will perform penetration testing on SEI annually as defined in IBM Data Security and Privacy Principles. As a custom option, and for additional charges, IBM can implement penetration testing for Client servers.

SD-3.4.14. Server Patch Management

Updates and software patches for operating systems on Operating System and Advanced Managed Servers are applied automatically via scripts during standard Scheduled Maintenance windows. IBM will provide notice of a planned update or available patch in advance of the Scheduled Maintenance window.

SD-4. Connectivity

SD-4.1. Managed Internet Access Services

Managed Internet Access Services provide Client with an IP connection. Managed Internet access connectivity includes configuration of:

- Internet bandwidth at a specified outbound Internet data transfer rate per GB as defined in the applicable Schedule
- Internet bandwidth at a specified committed information rate as defined in the applicable Schedule
- VLANs and IP devices

SD-4.2. Client Terminated Circuit

Connectivity supporting a Client terminated circuit into an IBM Extended CDC connects the Client environment to secure space or other point of connection to allow connectivity to a Client network. The circuit to support back-end connectivity into the IBM Service Enablement Infrastructure is not included and must be ordered separately by the Client in accordance with IBM circuit fiber requirements. Standard circuit configurations include:

- Up to a T1
- Greater than a T1
- Interconnectivity between Primary Extended CDC locations

Clients must provide the Client managed devices in support of private circuits that terminate in the Client's hosted network. Client is responsible for the configuration of the Client managed devices.

IBM will be responsible for extending the circuit(s) from the demarcation point to the Client provided equipment and/or IBM managed router. For each circuit, IBM will provide the Client with a single IP from a Client-Terminated Circuit (CTC) VLAN for a Client device to connect to the IBM network/switch. Client will provide IPs and manage all internetworking between the Client provided devices.

Client will procure at least one POTS (Plain Old Telephone Line) per CDC for out-of-band management of Client managed devices.

SD-4.3. Direct Link Connection Support

Direct Link Connection Support provides Client with redundant, private connectivity options for Managed Applications environments hosted in IBM Cloud Primary data center locations. The service is not available in Extended locations as defined in SD-2.1.

This Service provides support for Direct Link Dedicated and Direct Link Exchange connectivity options.

Both Direct Link Dedicated and Direct Link Exchange connectivity options require IBM Cloud Vyatta Gateways to deliver the termination point for the Client's circuit into the Client's Managed Application environment. Client has the choice of a 1Gbps or 10 Gbps Vyatta Gateway port speed. Local routing is

included as part of Direct Link Dedicated and Direct Link Exchange options and includes access to all IBM Data Centers connected directly to the PoP and provides unlimited ingress/egress traffic. If clients need to route their traffic outside the POP in the area within which they are ordering Direct Link, they must add the Global Routing option; otherwise, Client traffic will be restricted to the services provided by the local POP. As a standardized option, Global routing expands access to include all IBM Cloud data centers globally. Bandwidth is metered and charged monthly based on the market rates. If you select Global Routing, you are not charged for any local egress traffic, only for traffic that originates or terminates outside of the local POP.

There is no minimum term for this service.

There shall be a one-time setup effort and charge for each physical and/or logical port connected to SEI.

IBM will:

- Provide location and contact information for the PoP for Direct Link connections;
- Provision the Vyatta Gateways as documented in the Schedule;
- For Direct Link Dedicated, provide 1 Gbps or 10 Gbps Ethernet port(s), as documented in the Schedule, to the backbone that Client can connect to via a virtual or physical cross connect option as available within the PoP (T1s, DS3s, ISDN, POTs lines are not supported);
- Provide private connectivity from the PoP to the Client's Managed Application environment via a client dedicated IBM Cloud Vyatta Gateway
- Provide VPN connectivity from the IBM Cloud Vyatta Gateway to the Client's Managed Application firewall
- Provide support for overlapping address space as described in the Knowledgebase: http://knowledgelayer.softlayer.com/learning/direct-link-connectivity-options;
- Coordinate with the Client to connect Client network to the IBM Direct Link service upon receipt of the completed set-up form
- Manage the connections between Direct Link and the Client Vyatta Gateway.

Client will:

- Be responsible for the solution and any fees associated with reaching the PoP from Client premise and any virtual or physical cross connects needed within the PoP facility;
- Be responsible for the solution and any fees associated with collocating their equipment if Client's network carrier requires that a router or other device physically sit in the PoP;
- Be responsible to work with Client's network carrier, charges, and ordering the cross connect to the backbone connection port;
- Manage Client devices and if required Client end of the network tunnels to the Vyatta Gateway
- Designate a technically qualified network representative to serve as the focal point to provide IBM with required configuration and set-up information;
- Provide configuration information by completing and returning to IBM the set-up information form for each PoP where a connection is to be established;
- Perform testing of connectivity for Client workloads between Client environment and Cloud Service Environment;
- Perform troubleshooting and correction of any issues with the configuration of Client connection, any routing issues within Client network or any routing issues between Client network or the backbone; and
- Initiate and maintain proper Client network security controls

SD-4.4. Data Center Interconnectivity

Interconnectivity is provided between CDCs as defined in the applicable Schedule. Interconnectivity is enabled using a private wide area network (WAN) to enable geographically diverse server-to-server connectivity, load-balancing, high availability, and disaster recovery offerings. Data Center Interconnectivity includes configuration of:

- Private WAN bandwidth at a specified data usage transfer rate per GB as defined in the applicable Schedule
-

Bandwidth utilization of the private WAN at the following CDCs is metered at a per GB and Clients requiring datacenter interconnectivity will be billed monthly at a specified usage transfer rate. Interconnectivity options are described below:

Server-to-Server Connectivity: Primary IBM Cloud to Extended Location Interconnectivity

- Poughkeepsie, NY and Ashburn, VA: Primary to Extended Location Interconnectivity
- Dallas, TX (1) and Dallas, TX (2): Primary to Extended Location Interconnectivity

Disaster Recovery Connectivity:

- Poughkeepsie, NY and Dallas, TX (1): Extended Location Interconnectivity
- Ashburn, VA and Dallas, TX (2): Primary IBM Cloud Location Interconnectivity
- London, UK and Frankfurt, DE Primary IBM Cloud Location Interconnectivity

SD-4.5. Site-to-Site VPN Tunneling

The site to site VPN option includes provisioning and installation of an IPsec-compliant device on the Client's hosted network. IBM will provide configuration based on Client specifications.

IBM configuration and testing of the VPN tunnel at the IBM location is based on Client-provided IP identification of Client Internet Protocol Security (IPsec)-compliant device on the Client's network. Client is responsible for maintaining configuration on the device and for maintaining connectivity between the Client location and the Internet.

SD-4.6. Translation of IP Addresses

In the event of a conflict of private IP addresses, Client shall provide network address translation to map IBM private IP addresses to public IP addresses at Client site(s). Client has no ownership or transfer rights to any IP address assigned to Service and may not use IP addresses or VLANS not assigned to Client.

SD-4.7. Outbound Mail Relay (OMR)

IBM can provide shared outbound mail delivery as part of the Service. Clients may configure the application to utilize these shared resources for non-business critical emails, notifications, system level status emails and/or email alerts. The Cloud Service can be used for transactional emails; however, IBM does not warrant the delivery, provide support for mass email campaigns or troubleshooting of email issues such as spam surfaced from third party email systems.

SD-4.8. Domain Name System Hosting

IBM will support domain names for Client as specified on the technical service document. Client registers domain names and makes IBM the technical contact with the domain name registrar.

SD-4.9. Support for Microsoft Active Directory®

IBM-managed Active Directory includes deployment, configuration and management of operating system and operating system monitoring agents onto the Active Directory server, including installation and configuration of domain controller, patching, monitoring and troubleshooting authentication and replication issues. IBM retains sole domain administrator access (Advanced Server Management). Client is not provided root or equivalent access to operating systems. At least two Active Directory servers are required for redundancy. IBM will perform an initial load of base roles, organization unit, users and distribution groups not to exceed one hour.

SD-5. Client Networking

The Client Networking functions listed below are implemented using an integrated, highly available, virtualized dedicated network infrastructure. Client networking can be used with Client Terminated Circuits and/or Managed Internet Access and can also be used with the all IBM Server Management options. As a custom option and for additional charges, IBM can implement physically dedicated Client Networking infrastructure.

SD-5.1. Managed LAN Switching

Managed LAN switching provides Client with one or more LAN Layer 2 or Layer 3 switches that enable aggregation of multiple devices. As a custom option and for additional charges, IBM can implement physically dedicated Managed LAN switching. If Client requires five or more cross connects to support connectivity, Client is required to order physically dedicated LAN switching or another device to support the cross connects.

SD-5.2. Managed Load Balancing - Application Acceleration

Managed Load Balancing balances traffic across Client's servers located within an IBM CDC using Gigabit Ethernet connection to the Internet.

The standard service is available in a high availability dedicated virtual configuration. As a custom option and for additional charges IBM can deliver physically dedicated hardware configurations. Physically dedicated configurations require that Client also purchase IBM-managed LAN switching services.

Standard configurations include:

Feature	Base	Good	Better	Best
Basic LTM (round robin, least connection)	Yes	Yes	Yes	Yes
Complex LTM	No	Yes	Yes	Yes
Basic Health Checks	Yes	Yes	Yes	Yes
Complex Health Checking	No	Yes	Yes	Yes
Basic Load Distribution	Yes	Yes	Yes	Yes

Feature	Base	Good	Better	Best
Bandwidth Throughput	Up to 25 Mbps	200M, 1G, 3G 2x4 VM	200M, 1G, 3G 8x16 VM	200M, 1G, 3G 8x32 VM
iRules	No	Yes	Yes	Yes
Application Acceleration - Software compression	No	Yes	Yes	Yes

Application accelerators are load balancing service options supporting Secure Sockets Layer (SSL) acceleration, caching and compression to improve application performance and network efficiency. Optionally, application acceleration may include hardware/software compression, caching, enhanced web acceleration and SSL acceleration.

When SSL acceleration is ordered, IBM is not responsible for providing and managing any required encryption certificate keys and passwords.

SD-6. Managed Servers

The Server functions listed below are implemented using an integrated, highly available, virtualized computing infrastructure. Compute services can be used with Client Networking and with IBM Managed Storage options. The service supports virtual and bare metal configurations. As a custom option, and for additional charges, IBM can deliver a physically dedicated server configuration.

IBM maintains a library of certified server hardware, hypervisor, operating system, middleware and application software configurations, including configurations supporting Oracle and SAP™ certified workloads for SAP NetWeaver™ and SAP HANA™ usage. These certified configurations are used to build and deliver IBM Services for Managed Applications.

SD-6.1. Server Hardware

IBM will provide management of server hardware. IBM maintains a library of certified server hardware configurations, which are used to build and deliver server, hypervisor, operating system, and application monitoring and management services. Managed Server Hardware Services include:

- Monitoring and resolution of detected hardware failures
- Coordination of preventative maintenance
- Installation and maintain firmware upgrades
- Power cycling or reboot
- Physical inspection of all hardware components.

In cases where IBM repairs managed Server Hardware, IBM will reimage the server using the applicable current IBM-certified server hardware. IBM may modify (including the right to discontinue) a certified server hardware.

Managed Server Hardware may be used to deliver bare metal or virtual servers. Bare Metal servers are IBM-certified devices dedicated to a single Client.

SD-6.2. Virtual Machines

Virtual machines are IBM-certified and managed virtual devices configured with virtual core processor units (vCPUs) and virtual memory. As a standardized option, IBM Managed virtual machines are delivered on multi-tenant compute infrastructure. As a custom option, IBM can deliver IBM Managed virtual machines on physically dedicated compute infrastructure. Virtual Machine configurations are defined in the Schedule.

SD-6.3. Bare Metal

Bare Metal servers are implemented with Operating System or Advanced Server Management as part of a total Client solution. Bare Metal includes deployment and configuration of the IBM-managed operating system. IBM is responsible for configuration management, internal monitoring, patching and troubleshooting of all issues based on Server.

IBM will provide proactive monitoring and alerting of Server Hardware, network accessibility (ping) and web service (TCP Port 80) for Bare Metal servers. IBM will also perform verification that non-web TCP services respond to connection requests on a specific port, such as 21-FTP, 23Telnet and 25-SMTP, on request by Client. Standard Bare Metal configurations:

Bare Metal Configuration	Primary IBM Cloud Locations	Extended Locations
Small	2 vCPU x 64GB with four 1G ports	2 vCPU x 96GB
Medium	2 vCPU x 64GB with four 10G ports	2 vCPU x 192GB
Large	2 vCPU x 128GB with four 10G ports	2 vCPU x 384GB
Extra Large	2 vCPU x 384GB with four 10G ports	2 vCPU x 768GB – 32 core
Extra – Extra Large	2 vCPU x 768GB with four 10G ports	2 vCPU x 768GB – 48 core

SD-6.4. Server Management Options

IBM Services for Managed Applications provides two standard options for server management.

SD-6.4.1. Operating System Management

IBM will provide operating system support and access. Client access to the operating system will be provided using a strict least access required approach. Client is required to specify the number, type of operating system and configuration of the virtual machine and bare metal server instances. Use of operating system software is subject to acceptance by Client of software license terms. A Move, Add, Change (MAC) order is required to instantiate a new virtual machine or change an existing virtual machine.

Client is responsible for managing Client applications.

If operating system failure occurs and Client has not ordered Managed Data Backup Service (SD-9.), IBM will return server to the latest certified IBM operating system image (rebuilds) when necessary. Service includes a maximum of two rebuilds per server per year. Additional rebuilds will be charged at time and material rates. Rebuilds restore IBM certified operating system only and do not restore Client data, applications or application configuration.

IBM provides proactive monitoring of IBM-managed operating systems. IBM will provide Clients with notification of Priority 1 events related to operating systems. IBM will monitor and manage the IBM-supported operating systems and will provide Client with electronic notifications.

Alarms and/or events are generated per predefined usage thresholds assigned to each component being monitored; thresholds are set by default and can later be modified. Client is provided access to near-real time and historical reports for each monitored parameter, alarms and/or events. Alarms or notifications are available through the Portal.

SD-6.4.2. Advanced Server Management

For servers used in managed database, middleware and application services environments IBM manages and proactively monitors the availability, performance and recovery of its IBM managed reference operating systems and IBM-certified application software for Advanced Managed servers. IBM provides service reports, change request, trouble reporting and communications tools to Clients through the Portal. IBM retains exclusive administrative access to the Service platform. Service does not include Client access to operating systems.

SD-6.4.3. EU Labor

As a standard option at additional cost, IBM can provide EU based labor services "above the hypervisor" support to the client. This option provides European Union based personnel for the areas of operating system support.

SD-7. Managed Storage

Managed storage is delivered on a multi-tenant array using predefined primary storage tiers. Clients utilizing the standard tier configurations leverage standardized snapshot and replication features. IBM provides premium, performance, base and value storage tiers. Clients can select a storage tier based on the specific requirements of their workloads. Storage tier options are differentiated by cost and performance.

Standard Storage Tiers

- **Premium** (Tier 0): The storage is designed to support the most demanding and performance sensitive workloads that require very high IOPS with sustained throughput.
- **Performance** (Tier 1): The storage is designed to support high transaction database workloads requiring a high percentage of active data.
- **Base** (Tier 2): The storage is designed to support enterprise workloads that provide consistent IOPS for reliable application performance.
- **Value (**Tier 3): The storage is designed to provide lower IOPS relative to the amount of capacity provisioned at a lower price point, however performance might vary significantly.

As a custom option and for additional charges, IBM can deliver a physically dedicated storage hardware configuration. Physically dedicated managed storage technical specifications and licensing can be tailored specifically to meet Client requirements. Standard tier configurations, snapshot, and replication features may not be available.

Other storage related functions may require additional fees or need to be managed by the Client at the operating system, database, or application level depending on which management services have been contracted for those other offerings.

SD-7.1. Storage Capacity

Capacity limitations may apply, or extended delivery timelines could be necessary to accommodate large capacity requests. Dedicated storage, switch hardware or replication bandwidth could be required depending on the total amount of storage capacity and/or number of switch ports and/or replication bandwidth needed for the storage environment

Additional fees apply for backup or storage services if Client environment exceeds designated backup or storage limits.

SD-7.2. Maintenance

Maintenance of the managed storage infrastructure may require migration of Client data. IBM will notify Client in writing when data migration is necessary to allow a mutually agreeable maintenance window to support maintenance activities.

SD-7.3. Connectivity to Managed Storage services

Connectivity to the dedicated and multi-tenant storage infrastructure is provided over redundant 1Gbps or 10Gbps IP Ethernet (NFS/CIFS/iSCSI) or redundant 16Gbps Fibre Channel (SAN).

All Client managed servers or other hardware appliances requiring connectivity to dedicated managed storage must be configured with IBM certified NICs or HBAs.

Servers connected to SAN must use a minimum of two separate connections to two IBM-certified host bus adapters (HBAs) per server.

Servers connected to NAS must run UNIX-based operating systems to use Network File System (NFS) protocol or Microsoft Windows-based operating systems to use Common Internet File System (CIFS) protocol.

Associated monthly service charges per IP Ethernet, and/or Fibre Channel, switch ports will apply as necessary.

SD-7.4. Storage Service Level Support

IBM will provide the following levels of support for managed storage:

- **Operating system management** - Availability of data within the operating system of the bare metal server and/or VMs.
- **Advanced management** - Availability of data within the operating system, as well as any managed middleware, databases, or applications on bare metal servers and/or VMs.

SD-8. Data Protection for Managed Storage

IBM Services for Managed Applications provides a number of backup and restore policy options for physical and virtual servers using the storage snapshot capability as described below. These data protection options are mainly available for file systems provided through the multitenant Managed Storage offerings. Dedicated managed storage offerings can use these services if appropriate technical specifications and licensing requirements are met. File systems using internal disks on bare metal servers cannot leverage these data protection services. Additional fees apply for backup or storage services if Client environment exceeds designated backup or storage limits.

SD-8.1. Storage Snapshot Backups

Storage Snapshot Backups are available for file systems provided through the multitenant or dedicated managed storage offerings. Storage capacity is allocated per GB as necessary to meet the Client contracted data protection requirements and services are billed monthly based on total allocation.

Storage snapshot backups include supporting data availability, configuring snapshot and replication schedules, and facilitating restore of data from snapshots.

Snapshot Option	Definition
BU-5	Daily backup with ability to restore retained data to any day within the previous 5 days.
BU-14	Daily backup with ability to restore retained data to any day within the previous 14 days. A copy of backup data is retained offsite.
BU-30	Daily backup with ability to restore retained data to any day within the previous 30 days. A copy of backup data is retained offsite.

SD-8.2. Storage Snapshot Backup Replication

Daily snapshots are retained as defined in SD-8.1. with asynchronous replication to secondary offsite storage in another data center. Depending on the data center, the remote replication network bandwidth from the primary location to the secondary location is available for an additional charge per gigabyte. Remote replication requires custom scripting; additional charges will apply for the generation of the local replication scripts.

Optional local replication of storage is available for an additional charge per gigabyte. Local replication requires custom scripting; additional charges will apply for the generation of the local replication scripts.

SD-8.3. Storage Snapshot Service Level Support

Snapshot Option	Operating System Management	Advanced Management
BU-5	Available (Crash-Consistency Only) *Recommended for Non-Production Environments*	Available (Crash-Consistency Only) *Recommended for Non-Production Environments*
BU-14	Available (Crash-Consistency Only) *Recommended for Production Environments*	Application consistency is provided only for IBM-managed databases and IBM-managed applications that can be supported by standard tools and scripts. Database roll-forward is provided for IBM managed databases supporting that feature. This includes retaining database archive logs from the previous 24 hours in order to minimize data loss when restoring database data from the most recent storage snapshot.
BU-30		

Snapshot Option	Operating System Management	Advanced Management
		Recommended for Production Environments
Crash-Consistency Only does not guarantee recoverability of open files associated with running VM's, applications or databases.		

SD-8.4. Storage Snapshot Backup Condition/Limitation

Storage snapshots do not guarantee recoverability of the operating system or Client applications. Storage snapshots require that application and database files be in a consistent state – that is, either not in use or with usage temporarily suspended – during the storage snapshot execution.

Storage snapshots do not include integration with Client managed operating systems, databases, or applications. Database or application integration with storage snapshots is only provided for IBM managed databases and applications that can be supported by standard tools and scripts.

If necessary, Clients shall provide pre- and post-backup scripts for Client managed or nonstandard databases and applications. Clients will be responsible for maintaining alignment between scripts and database configurations and therefore IBM cannot guarantee application consistency of snapshots for Client managed or non-standard databases and applications.

SD-9. Managed Data Backup

The managed data backup and restore service provides a 24x7 data backup process for Client information such as individual files, file systems and online or offline databases. Data backup and restore is not a disaster recovery service.

SD-9.1. Fixed Rate Managed Backup

Fixed Rate Managed Backup Options				
BU-3	Daily incremental backups with bi-weekly full and cumulative backups	Client may restore to: • Any day within the past 30 days; up to 30 daily incremental backups each retained for 30 days. • Any week in the past 90 days; up to 12 bi-weekly full and cumulative backups each retained for 90 days. • Any quarter in the past 180 days; up to 2 quarterly full backups each retained for 180 days. (The last full backup in the last month of the quarter, usually in March, June, Sept., Dec., or as specified by Client).	Daily Offsite Replication and/or Daily Vaulting (Optional weekly vaulting)	AES 128-bit Encryption
BU-2	Daily incremental backups with bi-weekly full and cumulative backups	Client may restore to: • Any day within the past 30 days; up to 30 daily incremental backups each retained for 30 days. • Any week in the past 1 year; up to 52 bi-weekly full and cumulative backups each retained for 365 days.	Daily Offsite Replication and/or Daily Vaulting (Optional weekly vaulting)	AES 128-bit Encryption

Fixed Rate Managed Backup Options				
BU-1	Daily incremental backups with bi-weekly full and cumulative backups	Client may restore to: • Any day within the past 90 days; 90 daily incremental backups each retained for 90 days. • Any week in the past 1 year; up to 52 bi-weekly full and cumulative backups each retained for 365 days. • Any quarter in the past 5 years; up to 20 quarterly full backups each retained for 1825 days. (The last full back up in the last month of the quarter, usually in March, June, Sept., Dec., or as specified by Client).	Daily Offsite Replication and/or Daily Vaulting (Optional weekly vaulting)	AES 128-bit Encryption

SD-9.2. Managed Backup Service Restores

Client may restore data that has been previously backed up. Restoring data available onsite will begin within 60 minutes of IBM's receiving Client's request. Restoring data stored offsite will begin within 60 minutes of IBM's receiving the backup data onsite.

SD-9.3. Purchase of Managed Backup Data

As a custom option, and for an additional charge, copies of available backup data are available upon Client request. Prior to termination of subscription to managed backup and restore service, Client may purchase copies of the managed backup data. Upon Service termination, stored data is no longer available.

SD-9.4. Managed Backup and Restore Connectivity

Connectivity to the dedicated and multi-tenant storage infrastructure is provided over redundant 1Gbps or 10Gbps IP Ethernet.

Associated monthly service charges per IP Ethernet switch port will apply as necessary.

Dedicated switch hardware could be required depending on the total number of switch ports needed for the Client hosted environment.

SD-9.5. Suspended Servers - Maximum Term 90 Days

Servers subscribed to the Managed Backup service may suspend backup for a maximum of 90 days. If suspended for more than 90 days, reactivation of service is required and is subject to additional nonrecurring charges.

SD-10. Disaster Recovery Options

As an option and for additional charges, IBM can provide disaster recovery options for the managed services described in this Service Guide. Disaster Recovery (DR) enables the failover of managed services defined in the Schedule from the primary location to the secondary geographically disparate location within a required Recovery Point Objective (RPO) and Recovery Time Objective (RTO). The RPO is defined as the amount of time in which data is lost prior to the declared disaster, and the RTO is defined as the amount of time to recover managed services after a declared disaster.

The DR service is available in two service subscription levels:

- Base DR Service: Recovery Time Objective (RTO) is 24 hours and Recovery Point Objective (RPO) is 24 hours.

- Enhanced DR Service: Recovery Time Objective (RTO) is 4 hours and Recovery Point Objective (RPO) is 1 hour.

Disaster Recovery provides for coordinated implementation of all applicable IBM managed network, OS, storage, database, and application services. The service provides controlled procedures to support failover from primary to secondary IBM locations, as well as scheduled updates and patches to facilitate symmetry between the primary and secondary SEI compute instances as necessary to support disaster recovery.

Connectivity between primary and secondary IBM locations can leverage:

- Data Center Interconnectivity to provide the bandwidth for data replication between SEI managed compute instances and storage volumes and applies associated Mb/s bandwidth utilization fees as necessary to meet the Client's contracted disaster recovery requirements.
- Client Terminated Circuits (CTC) to provide Client dedicated connectivity between SEI locations and may be required to accommodate replication for large quantities of data with high data change rates.

Disaster declaration is the responsibility of IBM. In a disaster situation, Client will not be charged for the services at the primary site that have been affected by the disaster, for the duration of the disaster period.

Disaster Recovery options can include a disaster recovery plan which is tested annually. The annual DR test allows the Client to non-disruptively conduct a controlled test validating the availability of their environment and data at an alternate location. Supplemental DR tests are available per Client request for an additional cost as described in the Schedule. If IBM declares a site disaster at an SEI location, IBM Services for Managed Applications will notify the Client and execute applicable DR plans. The IBM Services for Managed Applications managed disaster recovery service does not provide for Client executed failover. IBM will execute a Client failover request by agreement of IBM and Client.

SD-10.1. Disaster Recovery for IBM Managed Databases with Roll Forward Option

This service provides the retention of database archive logs from the previous 24 hours in order to minimize data loss when restoring database data from the most recent storage snapshot. This service is available for Clients with IBM managed databases and applications utilizing IBM managed storage offerings delivered to an available standby DR environment at an alternate datacenter within the defined RTO/RPO.

SD-11. Managed Core Services

IBM Managed Core Services provides Operating System management and/or Advanced Server Management for middleware and database services deployed onto SEI infrastructure.

Service includes installation, administration and support for the operating system, database and middleware environment. IBM will monitor, alert, resolve and restore application events and provide Client with electronic notifications.

IBM will apply relevant patches, fixes and updates (excluding major new releases) and perform data protection, managed backup and/or disaster recovery services as defined in the applicable Schedule. Client and IBM specific roles and responsibilities for certified database and middleware applications are defined in the applicable Schedule.

Alarms and/or events are generated per thresholds assigned to each application being monitored. Client is provided access to reports for monitored parameters, alarms and/or events. Alarms or notifications are available through the Portal.

SD-11.1. Web Server and Middleware Management

As a standardized option, web server and middleware management includes installation, configuration, monitoring and proactive IBM Advanced Server Management of IBM certified web server and middleware software.

As a standardized option, IBM will configure external monitoring and alerting. These monitors originate from outside an IBM datacenter over the internet to monitor the Client's application through an automated method of simulating click-paths of a given user experience based on the Client's requirements. The number of simulated click-paths are measured in monthly units and specified in the Client's Schedule.

SD-11.2. Database (DB) Management

As a standardized option, Database management includes installation, configuration, monitoring and proactive management of IBM certified database software. An IBM operation DB administrator (ODBA) will provide day-to-day operation of Client database management system (DBMS) software package. The ODBA will execute all changes to the DBMS or DB instances that require system-level administrative access; upgrade or change the DBMS configuration files as required; provide fault analysis and fault management for errors related to the DBMS; make recommendations for directory/file structure and placement for optimal performance; and manage backup, restore and recovery of DBs as specified by Client. IBM's ability to restore DBs to a specific point in time is dependent on Client-provided backup and recovery services. IBM is not responsible for management of DB content.

SD-11.2.1. Database (DB) Clustering Service

DB clustering service manages a clustered configuration of server hardware and Advanced Managed servers that are bundled with supported DBs (managed storage service), with an active/passive DB cluster configuration that runs two identically configured systems with access to an IBM managed storage service. Each DB server within the cluster is designated as either active or passive. Using cluster software and high-availability private network connections, the servers within the cluster remain aware of the active DB server's status. When the active DB server fails or does not respond to queries, the passive DB server is activated, and all DB transactions are directed to it for processing. DB clustering service is implemented in three phases:

1. Initial build and delivery of functional DB cluster – Upon completion of environmental readiness test after installation, DB integration begins.
2. Database integration – Upon request by Client, IBM builds Client DB cluster based on Client specifications. Upon completion of operations readiness testing, monthly recurring charges for service begin. Additional DB integration activities shall be billed as as new cluster deployments.
3. Post-production tuning – For the first 14 calendar days after DB integration, IBM will monitor and manage the DB cluster and provide optimization and tuning to the DB cluster configuration.

SD-12. Application Services

Subject to acceptance by Client of applicable software license terms, IBM will provide IBM certified (or will manage Client-provided) applications hosted on and supported by IBM Service Enablement Infrastructure. Managed Application Services are delivered with Advanced Managed servers using SEI.

SD-12.1. Commerce

IBM provides managed services for commerce applications, included in which are managed services for IBM WebSphere Commerce as well as the Commerce suites from Oracle, SAP and Adobe.

The applications are deployed onto virtual and/or bare metal servers. The infrastructure, environments and software architecture are based on information provided by the Client and are specified in the Schedule.

The performance of the infrastructure supporting the applications may vary based on how the applications are customized by the Client. Should there be a requirement to increase or decrease the infrastructure capacity, IBM will work with the Client to make necessary adjustments to run the applications for optimal performance.

Services can include application installation, administration, standard tuning, and support for the commerce applications as well as varying levels of integration and support of third party services. IBM will monitor, alert, resolve and restore application events. IBM will apply relevant patches, fixes and updates (excluding major new releases) and perform data protection and managed backup services as defined in the Schedule.

Client and IBM specific application, implementation and support responsibilities are defined in the Schedule.

Alarms and/or events are generated per thresholds assigned to each application being monitored. Client is provided access to reports for monitored parameters, alarms and/or events. Alarms or notifications are available through the Portal.

The following additional commerce services are available for purchase by Client at the rates detailed in the Schedule:

Additional Commerce Service	Description
Basic Load Testing Support	IBM will participate in Client's load test. Tasks include reviewing Client's performance test plan, observing the load test and providing performance data of the managed service. For more advanced support, a separate statement of work can be provided.
Data Migration Support	IBM will assist in Client's migration to the managed service. Tasks include executing up to 3 data loads and installing files at the direction of the Client's instructions. For migration of encrypted databases, a separate statement of work can be required.
Additional Application Integration Setup	IBM will integrate up to 10 external systems with the managed service with Client's requirements. These integrations must be URI based using encrypted protocols. The service can integrate with an existing message queue but does not include a message queue (sold separately).
Additional User Account Setup	IBM will create up to 3 additional user accounts for one environment based on the Client's requirements. The user accounts provide server level access with least privileged access, with dual factor authentication supported with provided RSA tokens. Client connectivity to the environment is required (sold separately).
Additional Client Alerting Setup	IBM will create up to 10 custom alerts based on the Client's requirements. Existing log files will be monitored and alert thresholds configured. Alarms and notifications are available through the Client's Portal.
Additional Custom Job Setup	IBM will create up to 10 additional custom jobs based on the Client's requirements. Custom jobs include script development, system configuration, monitoring, and run-time execution.
Disaster Recovery Plan and Testing	This service is required for any Client solution that has disaster recovery. IBM will participate in one of

Additional Commerce Service	Description
	the Client's disaster recovery testing exercises. Activities include reviewing the Client's test plan, providing updates for IBM owned activities and conducting test procedures. The service does not include data or environment refresh activities.

SD-12.2. SAP

IBM provides managed services for SAP solutions deployed onto virtual and/or bare metal SAP certified servers. The Client solution is based upon the information provided by the Client or Client's system integrator. The solution/architecture and contracted applications are specified in the Schedule.

Service includes application installation, administration and support for the SAP environment. IBM will monitor, alert, resolve and restore application events. IBM will apply relevant patches, fixes and updates (on same release level) and perform data protection and managed backup services as defined in the applicable Schedule.

Alarms and/or events are generated per thresholds assigned to each application being monitored. Client is provided access to reports for monitored parameters, alarms and/or events. Alarms or notifications are available through the Portal.

The performance of the infrastructure supporting the applications may vary based on how the applications are customized by the Client. Should there be a requirement to increase or decrease the architecture, IBM will work with the Client to make necessary adjustments to run the applications for optimal performance. Changes in architecture may result in pricing changes (may reduce or increase the price) and will be handled through change control procedures.

SAP implementation and Support processes will be provided along the specified distribution of Responsibility, Accountability, Consulting, and Inform (RACI) table specified in the applicable Schedule.

SD-12.3. Oracle

IBM provides managed services for Oracle solutions deployed onto virtual and/or bare metal servers. The Client solution is based upon the information provided by the Client or Client's system integrator. The solution/architecture and contracted applications are specified in the Schedule.

Service includes application installation, administration and support for the Oracle environment. IBM will monitor, alert, resolve and restore application events. IBM will apply relevant patches, fixes and updates (on the same release level) and perform data protection and managed backup services as defined in the applicable Schedule.

Alarms and/or events are generated per thresholds assigned to each production application being monitored. Client is provided access to reports for monitored parameters, alarms and/or events. Alarms or notifications are available through the Portal.

The performance of the infrastructure supporting the applications may vary based on how the applications are customized by the Client. Should there be a requirement to increase or decrease the architecture. IBM will work with the Client to make necessary adjustments to run the applications for optimal performance. Changes in architecture may result in pricing changes (may reduce or increase the price) and will be handled through change control procedures.

Oracle implementation and Support processes will be provided along the specified distribution of Responsibility, Accountability, Consulting, and Inform (RACI) table specified in the applicable Schedule.

Client and IBM specific application, implementation and support responsibilities are defined in the applicable Schedule.

Additional Oracle Services	Description
Database and application monitoring for non-production environments	As part of this service, IBM can enable monitoring for non-production environments. When monitoring is enabled, the specific environment becomes a "controlled environment" and change management policies are applicable to them; sufficient lead time is required to schedule changes. Monitoring for production environment and non-production infrastructure are included in the default Oracle Managed Services.
Disaster Recovery (DR) Test	If DR is included in the solution, one (1) annual DR test is already included in the services. If Client prefers to perform additional DR tests, IBM can provide this service for an additional fee.

SD-12.4. Messaging & Collaboration

IBM provides a managed Microsoft Exchange, SharePoint and Skype for Business solution deployed in a single-tenant configuration of virtual and/or bare metal Advanced Managed servers, including Active Directory integration.

Additional Messaging & Collaboration Services	Description
Perimeter email antivirus, antispam, and content filtering	IBM will integrate Client solution with an email perimeter antivirus, antispam, and content control service. IBM will configure domain level policies, directory synchronization (where applicable) and provide Client administrators access to service platform where the Client can manage email policies.
Perimeter email encryption	IBM will integrate Client solution with an email encryption service. IBM will configure domain level policies, directory synchronization (where applicable) and provide Client administrators access to service platform where the Client can manage email policies.
Email Continuity	IBM will integrate Client solution with an email continuity service, a web-based portal used for sending email in the event of a disaster recovery scenario not natively built into the solution. IBM will configure directory synchronization, account activation/deactivation based on Client directory configuration and requirements. IBM will configure domain level policies and provide Client administrators access to service platform.
Email Archiving	IBM will integrate Client solution with an email archiving service designed to accommodate Client retention and eDiscovery requirements. IBM will configure directory synchronization, account activation/deactivation based on Client directory configuration and requirements, and enable Client

Additional Messaging & Collaboration Services	Description
	access to discovery archive. IBM will configure domain level policies and provide Client administrators access to service platform. The Client will manage legal holds and administrator access to the archiving platform.

Service includes application installation, administration and support for the hosted Microsoft Exchange, SharePoint and/or Skype for Business environment as identified in the applicable Schedule. IBM will monitor, alert, resolve and restore application events; apply relevant patches, fixes and updates (excluding major new releases); and perform data protection and managed backup services and optional archiving as defined in the Schedule. Client and IBM specific application, implementation and support responsibilities are defined in the applicable Schedule. Optional email services include perimeter anti-virus, anti-spam, content filtering, encryption, continuity, and archiving.

SD-13. IBM Client Support Services

SD 13.1. Client Onboarding and Implementation

IBM will provide onboarding and implementation services for the infrastructure and applications as defined in the applicable Schedule. Onboarding and Implementation services include project management, project planning and assistance with the preparation of the environment at the Service Location in support of the Services. Following execution of the Schedule, IBM will coordinate a conference call with Client's program sponsor to prepare for the project. During the conference call, IBM will:

- Review and confirm project objectives, scope and approach;
- Establish project timeline, schedule and milestones;
- Review project assumptions; and
- Review Client-provided documentation and diagrams supporting the Services.

Onboarding and Implementation Services can also provide:

- Support during the preproduction implementation stage;
- Inventory and provisioning;
- Development and implementation of operations readiness test and cutover procedures prior to the management being transitioned to lifecycle support teams; and
- Technical support to assist with Client's application deployment.

A project plan will be developed which will define the activities required to install the infrastructure and applications. Client is required to:

- Assign a single point of contact to ensure ongoing Client focus and support.
- Provide a single point of contact that will work with IBM to coordinate scheduling and logistical support.
- Provide technical resources to assist with the implementation of the Services.
- Provide an access list of persons authorized for: access, opening trouble tickets, scheduling maintenance, and requesting changes.
- Identify those employees authorized to request modifications to the access list.
- Provide timely access to and participation of Client personnel during implementation activities, in accordance with the schedule mutually agreed upon.

SD-13.1.1. Inventory and Provisioning

This service provides management of ordering, tracking and delivery of IBM-owned/managed hardware and software, including software licensing provided by IBM and delivered on IBM-owned/managed hardware. Client is responsible for ordering, tracking and delivery of Client-owned/managed software applications. IBM will communicate processes to support change activity to the IBM-managed environment.

SD-13.1.2. Test and Turn-Up of the Managed Services

IBM will perform system validation testing of IBM-managed Service Components in conjunction with IBM test schedules prior to transition to lifecycle support by:

- Assigning the IP address space pursuant to forecasted design.
- Validating that IBM managed infrastructure and applications are operational and subject to IBM monitoring.
- Validating that noncertified or uniquely configured software is operating according Client specifications as defined in the applicable Schedule.
- Document and audit environment controls, devices and configuration to verify operational readiness.
- Apply quality assurance methodology to environment including redundancy testing and automated startup/shutdown procedures including supported applications as contracted.
- User acceptance testing prior to environment go live.

To allow IBM to complete system validation testing, Client shall:

- Coordinate testing in conjunction with IBM test schedules.
- Provide additional information or documentation relating to Client managed elements within overall service design as required to allow IBM to complete testing.
- Provide user acceptance testing prior to environment go live.

SD-13.1.3. Cut-Over of Production Traffic

Upon notification from IBM of production and lifecycle support readiness, Client is responsible for redirecting Domain Name System (DNS) entries from the existing sites/services (if applicable) to the IBM-supported IP addresses. When necessary, IBM will validate the DNS redirection.

SD-13.2. Client Service Management

Client Service Management is led by two primary IBM leaders:

- Client Partner Executive (CPE) owns the overall contract and associated relationship with Client. The Client Partner Executive has the primary role of executive advocate for all matters pertaining to the contract as well as the Strategic Governance model.
- Delivery Partner Executive (DPE) is responsible for oversight and facilitation of all operational aspects of service delivery. The DPE is a primary point of contract for any issues or needs associated with IBM's service delivery performance.

Client Service Management provides for multiple Client experiences by aligning Clients to one of three Service Tiers: Basic, Advanced or Premium. These tiers are designed to reflect the scale of management required by Client and expected volumes of Client-initiated monthly Service Requests and Change Requests (Service Plans). Each Service Plan is 10 Change Requests or Service Requests per calendar month as requested by Client.

Additionally, each tier entitles Client to service features that will further enhance Client experience.

		Service Tier		
		Basic	**Advanced**	**Premium**
Monthly Entitlement	Incidents and Ticketing	Uncapped	Uncapped	Uncapped
	Baseline Service Plans	1 Service Plan	2 Service Plans	3 Service Plans
	Offering(s)	Managed Core Services	Managed Core Services Managed Application Services	Managed Core Services Managed Application Services
Onboarding & Readiness	Onboarding	Onboarding Project Manager	Project Integration Manager	Project Integration Manager
	Service Readiness	Checklist for Managed Core Services	Checklist for Managed Core Services Managed Application Services	Checklist for Managed Core Services Managed Application Services
Case Management	Severity 1 Incidents	Escalations via Portal	24x7 by On Call Managed Escalation Support for Production Environments	24x7 by On Call Managed Escalation Support for Production Environments
	Severity 2 Incidents	Normal Business Hours via Portal	24x5 (Monday through Friday) by On Call Managed Escalation Support for Production Environments	24x5 (Monday through Friday) by On Call Managed Escalation Support for Production Environments
	Severity 3 Incidents	Normal Business Hours via Portal	Managed during Normal Business Hrs.	Managed during Normal Business Hrs.
	Support for Change Management	As needed on a twice a month basis	Managed weekly in collaboration with Client change controls Process	Managed weekly in collaboration with Client change controls Process
	Language Support	English	English	Local language(s) options
Governance	Operations Review	None	Weekly	Weekly

	Monthly Measurements Review	None	Review of Key Service Metrics and ongoing projects	Review of Key Service Metrics and ongoing projects
	Quarterly Business Reviews	None	Joint Executive Business Strategy and Innovation Topics	Joint Executive Business Strategy and Innovation Topics
Value Added	Business Continuity Testing	Additional Charges	Additional Charges	1 DR Test Annually 1 DR Test included following initial implementation phase

If Client exceeds Service Plan entitlement as reflected in the Schedule in any calendar month, IBM shall reserve the right to charge Client for additional Service Plans consumed.

IBM may recommend Client contracts for additional Service Plans for fulfillment of IBM-identified Client trends. For avoidance of doubt, Change Requests and Service Requests accounted for in each Service Plan shall not include Client tickets raised outside the Change Management Process and Service Request management process.

Clients subscribing to Premium Service Tier:

- may request local languages DPE support provided IBM has in-region personnel that speak the languages requested by Client; and
- may order Ad-hoc services such as additional disaster recovery planning for additional charges.

SD-13.3.3. Portal

Where necessary to allow IBM to provide monitoring and management of Services to Client, Client authorizes IBM to access Client information using the Portal.

SD-14. General Terms

SD-14.1. Client Orders for Service or Service Components

To order IBM Services for Managed Applications, IBM and Client will develop a technical service definition form that contains the technical details necessary to provision service on infrastructure at a CDC. “Infrastructure” includes IBM and Client provided equipment and software applications that constitutes the physical and virtual computing, storage and network devices used to run software operating systems and applications, and may also include, but is not limited to, routers, switches, servers, and peripheral devices (including security service devices and fiber optic), used to provide the Service.

Client is required to provide all technical details necessary to identify Service components required before Services may be provisioned.

An Order and Pricing Schedule will be the vehicle for documenting a change to an existing Service. The Order and Pricing Schedule will describe the change and the effect the change will have on the Services and charges. The Order and Pricing Schedule must be accepted by authorized representatives to implement any changes.

Following Client's original Order and Pricing Schedule, a Service Request for additional Service features may be made via an additional Order and Pricing Schedule or (if available via a portal). All orders are subject to the terms of the Agreement, and Client agrees to pay for any such Services.

SD-14.2. Services Changes

IBM may from time to time add new Services or options, or in its reasonable discretion, withdraw existing Services or options, in whole or in part as set forth below:

1. IBM may change the computing environment and architecture used to provide the Service at any time without notice, provided the change 1) does not degrade the Services as described in the Service Guide, and 2) applies to all similarly situated Services Clients; and 3) does not degrade the Service security features.
2. IBM may change the computing platform on which the underlying computing environment and architecture used to provide the Service reside. IBM will manage the end to end migration plan and coordinate with the Project Executive to migrate Client from the current platform to the new destination platform. Both IBM and Client are responsible to perform their applicable migration responsibilities for this offering as set forth in the Agreement using the defined migration rules.
3. For changes to existing Services or options described in this Service Guide, IBM will notify Client of any new or changed Services and the effective date of such by providing notice directly to a Project Executive using current information in Client's Account.
4. For any withdrawal of Services, or for any change that affects existing Services, the change will be effective the later of i) 90 days after the date of the notice; ii) the specified effective date; or iii) as may otherwise be specified.
5. For withdrawal of the Service in its entirety, IBM will provide Client with one hundred eighty (180) days' notice.

SD-14.3. Acceptance of Changes

Client acknowledges its agreement to any of the above changes by i) continuing to use or ordering Services after the effective date of the change, ii) allowing Services to renew after receipt of the change notice; or iii) by signing (in writing or electronically, where permitted) an applicable revised Order and Pricing Schedule or other change authorization mechanism IBM may provide (such as on-line acceptance).

SD-14.4. Services Rates, Billing and Service Activation

Billing for Service shall be on a nonrecurring (one-time) and monthly recurring basis. Billing for Service or Service Component begins on the date(s) specified in the Schedule.

Commitments and options selected by Client and actual usage will affect the total charges IBM will invoice.

Client will be invoiced monthly beginning on the first day of the month following the Service Activation Date. Client agrees that the charges stated in a signed Schedule will apply to all Services ordered, are payable in the specified currency, and are exclusive of any duty, tax, levy or fee. Client understands that IBM may from time to time add additional Services or options and make them available to Client to order at then current prices.

IBM will invoice applicable charges as follows:

- usage charges will be billed at the end of each month based upon actual use of Services multiplied by the specified unit charge;
- recurring charges will be billed at the end of each charge period (e.g., monthly, quarterly or annually) and will be prorated based on when such Services begin or end; and
- one-time charges will apply when such Services are delivered.

In addition, for early termination by Client, Termination Charges as per the Schedule may apply and will be billed upon the closing of Client's Account.

Client will reimburse the travel and out-of-pocket expenses that IBM incurs in performing the Services and which have been pre-approved by Client in writing. IBM may charge late payment fees at the lower of 2% per month (24% per annum) or the maximum rate allowed by law for overdue payments.

Any requests for additional services may be submitted to IBM in accordance with the Changes section of the Schedule. SD-14.4.1. Service Activation Date

For all IBM managed Services or Service Components, the Service Activation Date for the Services or for the individual Service Component(s) is the implementation date.

The implementation date for operating system server management Services is the date when the infrastructure and applications for Client service is installed by IBM and supplied with network connectivity, regardless of whether Client managed content or software applications have been deployed by Client.

For Application Services Clients with advanced managed servers or other Services or Service Components, the implementation date is when IBM provides notice that the Service is available for use or the date on which a Client or user begins using the Service or Service Component, whichever date is earlier.

SD-14.4.2. Client Delay of Service Activation

If Client's actions or omissions, including Client's failure to supply information necessary to fulfill Client's order, cause IBM to be unable to complete Service activation of a Service or Service Component by the scheduled Service Activation Date, at IBM's election, IBM may cancel the Service or Service Component subject to the Client-caused delay and charge Client the charges set forth in the applicable Schedule.

SD-14.5. Termination or Cancellation of Services or Service Components

SD-14.5.1. Termination of Services or Service Components

Client may terminate Services or Service Components after the Service Activation Date as specified in the Schedule by (1) providing not less than sixty (60) days prior written notice; (2) paying for all Services and Service Components provided up through the effective date of termination; and (3) paying all disconnection, deinstallation and applicable termination charges, as described in the applicable Schedule.

SD-14.5.2. Withdrawal of Services or Service Components

Unless expressly otherwise provided in the Agreement, and unless applicable law or regulation mandates otherwise, IBM may discontinue providing the Services upon 180 days' notice or a Service Component upon 120 days' notice to Client, but only where IBM generally discontinues providing the Services or Service Component to similarly situated Clients.

SD-14.5.3. Removal of Property

Client shall remove all Client-owned devices from CDC by the effective termination or cancellation date. If Client fails to remove all equipment and other property from Client space or the CDC within 45 days of such disconnection, termination, cancellation or expiration, Client:

- Agrees that IBM may dispose of such property as it deems appropriate, which may include, at IBM's election, the sale, destruction or erasure of such property; and
- Fully and completely releases IBM from any and all liability arising out of such disposal, of whatever nature, and shall fully indemnify, defend and hold IBM harmless against any and all claims of third parties directly or indirectly arising out of or related to such disposal.

To the extent provided by applicable law, Client's failure to remove any property from a CDC does not create any terms of bailment between Client and IBM, and IBM disclaims any status as a bailee.

SD-14.5.4. Return of Content

Not later than 30 days after expiration or termination of the applicable Schedule, IBM will, at Client's expense, return the Client Content and personal property of Client in IBM's possession or control.

SD-14.6. Data Center Location

IBM utilizes multiple Cloud Data Center locations to deliver the Services, and not all Services and options are available in all Data Centers.

Client acknowledges that i) the central infrastructure supporting the Portal and Client Account contact information and User ID information provided by Client (Client Account Information) is stored and delivered from the central business support system data center location in IBM's European Cloud Data Center or other locations IBM deems necessary for the delivery of the Services, and ii) Client VMs are stored and delivered from the operational support system CDCs that IBM makes available.

Client may use the Services to create and make available to Solution Recipients Client Solutions based on the Services. However, Client may not resell direct access to any of the Services to any third party without entering into a separate agreement with IBM. Client is responsible to have appropriate agreements in place with Client's Solution Recipients, including rights to process content requested or provided by Client or Client's Solution Recipients, and is responsible for their use of a Client Solution.

IBM, at its expense, may change the location of the data center at any time upon sixty (60) days prior written notice to the Client. Upon Client's request, IBM will provide information to reasonably demonstrate that the new data center facilities are at least equivalent to the current data center facilities in all material respects. IBM will develop a migration plan prior to any move, and Client and IBM will agree on any Client activities included in the plan, such as Client testing requirements or assistance. Client will perform its activities at its own expense.

SD-14.7. Third Party Software License Rights and Restrictions

Client will retain all its rights, title, and interest in and to Client content. Client content and the Services may contain confidential information and other valuable proprietary information. Neither party, directly or through a third party, will alter, copy, reverse engineer, decompile, disassemble, attempt to derive source code from, license, sell, transfer, lease, disclose, or modify or remove any copyright or proprietary notice, from Client content (in the case of IBM) or from the Services (in the case of Client). Client also will comply with all third-party license terms for Client software.

Services may contain software licensed by IBM or licensed by third party software providers. Specific terms below may apply depending on the software licensor, and in addition third party software and its use will be licensed in accordance with the applicable third-party license agreement ("Third-Party Agreement"). The Third-Party Agreement is an agreement between Client and the third-party software owner or rights holder only. IBM is not a party to any such Third-Party Agreement. Client receives no warranties, indemnities or express or implied patent or other license from IBM with respect to any third-party software. IBM's provision of Services hereunder does not constitute a distribution of the third-party software by IBM.

SD-14.7.1 Client Provided Software

Client is permitted to bring and upload its own properly licensed non-operating system software (BYOSL) for use within the Services by installing it directly on a VM. Client is responsible to ensure Client has the necessary licenses, entitlements, and approvals for adding, installing, uploading, transferring, and using such software with the Services.

For any Client provided Microsoft software, Client shall ensure that any BYOSL Microsoft software uploaded by Client to a VM in the IBM cloud environment is covered with licenses / software maintenance (if required)

which are adequate in type and sufficient in quantities to comply with Microsoft's license requirements and that they are eligible to be used in a multi-tenant cloud environment. Client agrees to reimburse IBM for any reasonable costs and other amounts that IBM may incur from Client's failure to obtain these licenses or approvals.

Services are provided from a shared, multi-tenant environment operated by IBM as a service provider. The following provisions apply to any BYOSL non-operating system software licensed to Client by Microsoft Corporation or a Microsoft authorized reseller.

For the purposes of this provision, "License Mobility through Software Assurance" means the rights described in the section titled "License Mobility through Software Assurance" in the Microsoft Product Use Rights. The Microsoft Product Use Rights are located at: http://www.micrsoft.com/licensing/software-assurance/default.aspx or a successor site.

In order to exercise License Mobility through Software Assurance rights, Client must, prior to uploading any Microsoft software as BYOSL to a VM in the IBM cloud environment, execute the "Mobility Verification Form" located at: http://www.microsoft.com/licensing/softwareassurance/license-mobility.aspx or at a successor site and submit the completed Mobility Verification Form to Microsoft for verification.

Microsoft will provide IBM and Client with confirmation of Client verification status to exercise the License Mobility through Software Assurance Product Use Rights, and the specific products and license counts Client will be authorized to deploy in the IBM cloud environment. This information may be used to support compliance reviews and discussions.

If IBM or Microsoft believe in good faith that Client is not complying with the terms of License Mobility through Software Assurance, as described in the Product Use Rights, Client must cooperate in good faith with Microsoft or IBM to investigate and remedy any potential noncompliance. If requested by IBM and/or Microsoft, Client agrees to provide any additional and reasonable information to support the investigation and remediation, if any, of the noncompliance.

If Microsoft determines that Client is non-compliant with the License Mobility through Software Assurance program requirements, Microsoft will provide Client with written notice of the noncompliance which will include an itemization of the non-compliant issues. Client will work with Microsoft to resolve the Client's status and determine if termination can be avoided. If the parties are unable to achieve a mutually agreeable resolution, Microsoft will provide Client and IBM with written notice to terminate the benefits of License Mobility through Software Assurance for Client. Upon receipt of such notice, Client will promptly remove the instances provided in the notice and utilized by Client and provide written notice to Microsoft with a copy to IBM.

Client must ensure that any License Mobility through Software Assurance Product deployed in the IBM cloud environment uses the Client's own Product media and keys.

Client's licenses under the License Mobility through Software Assurance program must remain on a VM within the same CDC for no less than ninety (90) days. Client may move instances under a particular license from one IBM CDC to another IBM CDC; however, Client may not (a) move the instances run under that license back to the Client computing environment, (b) outside of IBM's CDC, or (c) to another third-party cloud data center within ninety (90) days of the last assignment.

For software Client has licensed separately from IBM Corporation ("IBM Software"), only those that are in accordance with the "IBM Eligible Public Cloud BYOSL Policy", which can be found at this url: https://www-01.ibm.com/software/passportadvantage/eligible_public_cloud_BYOSL_policy.html#eligiblesoftware may be uploaded as BYOSL software for use in the Services.

SD-14.7.2. Additional Service Component Software Terms

If Client uses software for which Client does not have proper licensing, IBM may assess additional charges based upon actual use and require Client to obtain proper licensing.

Client understands IBM may be required by agreement with the applicable third-party supplier of software to provide usage data and Entitlement information specific to usage of a third-party Services Component. Client will be responsible to such third-party supplier for any improper use, including additional charges and requirements to obtain additional Entitlements.

Client's use of Services Component Software, governed by the applicable license agreement, which may include license information or other documentation associated with such software, ("License Agreement"). For Service Component Software from the IBM Corporation, applicable license agreements are also available at http://www.ibm.com/software/sla (by selecting the option to "search for a specific program license agreement" and then entering the name of the IBM software).

Notwithstanding any terms of a License Agreement to the contrary, the following terms apply to all Service Component Operating System Software, and each SC Software product for which Client brings Client's own existing license, except if otherwise specified by Client's license with the software provider:

- The Services Component is provided for a term set forth in the Agreement and is not perpetual;
- No installation or download by Client of a Services Component, in whole or in part, is permitted except as set forth in the applicable Schedule;
- No copies (including back-up copies) of a Services Component, in whole or in part, are permitted except as specifically set forth in the applicable Schedule;
- No transfer of a Services Component, in whole or in part, is permitted during the term of the Services; and
- Any money back guarantee and warranty that may be provided in a License Agreement may not apply to Services Components.

Services Components may not contain all features or functions of the generally available software available directly from the software licensor.

SD-14.7.3. IBM Provided Operating Systems

Each VM will be provisioned with an Operating System Image (Operating System Software) of Client's selection. IBM will provide all Operating System Software for virtual and baremetal machines used by Client. Client legacy Operating System images may not be used in the Service.

For the purposes of this section, Operating System currency means that IBM will support two (2) versions of an Operating System software, whether the two most recent levels are considered minor or major releases. For purposes of illustration, IBM will support versions 1.4.1 and version 1.4.2, or version 1.4.2 and version 2.0.

IBM will maintain currency of supported Operating System software as follows:

- Minor versions IBM provides (for example, v1.4.1 to v1.4.2) will generally be deployed and supported throughout the VMs in the IBM Cloud Data Centers within three (3) months of general availability as announced by the software vendor;
- Major versions IBM provides (for example, v1 to v2.0) will be generally deployed and supported throughout the VMs in the IBM Cloud Data Centers within six (6) months of general availability as announced by the software vendor; and
- For any version (minor or major) of the Operating System software that is no longer to be supported by the software vendor, for any reason:

- IBM will withdraw any such Operating System software from sales no later than six (6) months before the date the vendor has announced that support will no longer be available, if the software vendor provides at least six (6) months' notice; otherwise, the Operating System software will be withdrawn from sales immediately;
- IBM will provide support to such Operating System software installed on VMs in the IBM Cloud Data Centers until the day before the date the vendor discontinues its support; and
- Client accepts full responsibility for risks which may be incurred related to use of Operating System software that is no longer to be supported by the software vendor for any reason including, but not limited to, risks to the security integrity, availability, and confidentiality of the system, databases, applications, and its data.

IBM may provide update/migration custom services for an additional charge to Client.

SD-14.7.4. Service Component Operating System Software License Terms

Client's use of Services Component Operating System Software is governed by the applicable license agreement (“License Agreement”) below:

a. All software from the IBM Corporation provided with IBM Services for Managed Applications is licensed under the applicable license agreements available at http://www.ibm.com/software/sla (by selecting the option to "search for a specific program license agreement" and then entering the name of the IBM software).

b. Red Hat Linux server software is licensed from Red Hat under additional license terms to be found at www.redhat.com/licenses/cloud_cssa/.

c. Microsoft Server operating system software product (referred to as "Product" in this section) is licensed from Microsoft and IBM is required include the following terms and Client agrees to the following:

- Client shall not remove, modify, or obscure any copyright, trademark or other proprietary rights notices that are contained in or on the Products;
- Client shall not reverse engineer, decompile or disassemble the Products, except to the extent that such activity is expressly permitted by applicable law;
- Microsoft disclaims, to the extent permitted by applicable law, all warranties by Microsoft and any liability by Microsoft or its suppliers for any damages or remedies, whether direct, indirect, or consequential, arising from the Software Services. For the purposes of this section Software Services means the services IBM provides to Client that make available, display, run, access or otherwise interact, directly or indirectly, with the Products;
- IBM may disclose Client information such as the total number of licenses and country of usage, Client name and address;
- technical support for the software Services will be provided by IBM or a third party on IBM's behalf (and not Microsoft or its suppliers);
- there is a "No High Risk Use" requirement that the user may not use the Product in any application or situation where the Product(s) failure could lead to death or serious bodily injury of any person, or to severe physical or environmental damage ("High Risk Use"). Examples of High Risk Use include but are not limited to: aircraft or other modes of human mass transportation, nuclear or chemical facilities, life support systems, implantable medical equipment, motor vehicles, or weaponry systems. High Risk Use does not include utilization of Products for administrative purposes, to store configuration data, engineering and/or configuration tools, or other non-control applications, the failure of which would not result in death, personal injury, or severe

physical or environmental damage. These non-controlling applications may communicate with the applications that perform the control, but must not be directly or indirectly responsible for the control function; and

d. Client accepts full responsibility for risks which may be incurred related to use of Operating System software that is no longer to be supported by the software vendor for any reason including, but not limited to, risks to the security integrity, availability, and confidentiality of the system, databases, applications, and its data.

SD-14.7.5. Microsoft Application Software with License Administration Services

For Advanced Managed VMs only, Client may order licenses for available Microsoft SC application Software by submitting a change order. IBM will provide the software product libraries and license keys as necessary. IBM will perform license administration for the selected software products, invoice for the quantities consumed, and will perform compliance reporting required by Microsoft's Service Provider License Agreement program. The Client is responsible for actual software product installation, maintenance, and ongoing lifecycle management ad defined in the applicable Schedule. Client will readily assist IBM with monthly reconciliation of consumption of the Microsoft SC application Software.

IBM will work with Client to reconcile the number of licenses for payment purposes. IBM will then invoice Client monthly based on Client's actual consumption. This mechanism also provides tracking and invoicing for Clients who install, but do not formally request, the Microsoft SC Application Software.

SLA-1. Service Level Agreements

SLA-1.1. General Terms Applicable to Service Level Agreements (SLAs)

- Except where an individual SLA states differently, SLAs and the collection of data measurements against a performance objective shall begin on the 91st day after Service Activation Date.
- SLA reporting will be made available to Client in the next complete monthly reporting period.
- Except as otherwise stated in an Order and Pricing Schedule, SLAs apply only to production environments.

SLA-1.2. Service Level Agreement (SLA) Exclusions and Limitations

IBM is not responsible for failure to meet an SLA resulting from any of the following events:

- Negligent conduct or misuse of the Service by Client
- Conduct of a third-party service provider providing Service to Client
- Failure or deficient performance of power, equipment, services or systems not provided by IBM
- Unplanned network volumes more than the capacity being provided on the Service Activation Date or changes in Client business requirements not reported to IBM by Client through the change order process, such as adding a new location or new services
- Service interruptions, deficiencies, degradations or delays:
    - Due to Client equipment managed by IBM that has not been upgraded by Client as required by IBM
    - Due to Client equipment managed by IBM or for which maintenance is not available
    - Due to failure of code or software managed and/or written by Client or a third-party vendor for Client
    - During any period when IBM or its agent is not afforded access to Client equipment or when IBM or its agent is prevented from implementing software patches or upgrades necessary for IBM to provide Service

- During any application failures caused by Client disrupting or adversely impacting its service or failing to respond to alerts as agreed or creating false alerts
- During any period when a Service Component is removed from service for maintenance, replacement or rearrangement purpose or for the implementation of a Client order
- Due to an act by Client through the use of root or administrative access to a virtual or physical server
- Due to interruptions caused by a Client-managed Active Directory domain controller, including, without limiting the foregoing, interruptions arising from faulty domain communications, domain policies on the environment, or the security configuration of the domain controller.

- Client's refusal to allow IBM to perform maintenance deemed necessary to maintain the Service, whether scheduled or unscheduled
- Force majeure conditions

SLA-1.3. Service Level Agreement (SLA) Claims

SLA-1.3.1. SLA Process

Each month IBM will measure SLAs and, where Client is due a remedy, IBM will issue a credit against the ensuing month's service fees in accordance with this Service Guide.

To be eligible for a Services Credit, Client shall notify IBM in writing of a claim within 10 days of the day IBM failed to meet the SLA performance objective or that Client otherwise became eligible for the Services Credit. Client shall send its claim to an email address specified by IBM. All claims submitted by Client shall include the date and time of the outage or other event that Client believes makes it eligible for a Services Credit. IBM shall, in its sole and reasonable determination, verify and determine Client's eligibility for a Services Credit.

SLA-1.3.2. SLA Claims Limitations

Excluding the IBM Services for Managed Applications Response Time SLA detailed in SLA-3 below, Client may claim one (1) SLA Services Credit per calendar month, consisting of all claims for that month. Client will not receive a Services Credit for IBM Services for Managed Applications installation charges, other monthly recurring charges or charges related to additional services. Any Services Credit paid to Client shall constitute the Client's sole and exclusive remedy for IBM's failure to meet an SLA.

SLA-2. Availability Service Level Agreement (SLA) Matrix

<table>
<tr><th>Offer Service Level</th><th>Service Level Tier</th><th>Availability Metric</th></tr>
<tr><td rowspan="4">Managed Core Services
(SD-11) – Operating System
(SD-11) – Database
Managed Application Services Commerce (SD-12)
Managed Application Services SAP (SD-12)
Managed Application Services Oracle (SD-12)
Managed Application Services Messaging & Collaboration (SD-12)</td><td>Standard</td><td>99.90%</td></tr>
<tr><td rowspan="2">Standard (with non-redundant service components)</td><td rowspan="2">99.50%</td></tr>
<tr><td>High Availability</td><td>99.95%</td></tr>
</table>

SLA-3. IBM Services for Managed Applications Response Time SLA

IBM offers an SLA for response time. Response Time is measured from the time that IBM receives notice of an incident until the time that IBM responds to Client. “Notice” as used in this section refers only to notification that occurs in electronic form through email or on the Portal.

IBM will respond to 100% of Priority incidents during the hours of support for the Client per the following:

LABEL	DEFINITION	RESPONSE TIME
Priority 1	Incident that prevents all Client use of the Service	within 15 minutes
Priority 2	Incident with significant and materially adverse effect on use of the Service or on Client’s key business processes	within 30 minutes
Priority 3	Incident with nominal adverse impact on use of the Service or on Client’s key business processes	within 60 minutes

Client’s sole and exclusive remedy for IBM’s failure to meet the response time will be a $750 credit for each failed Priority 1 response, $500 for each failed Priority 2 response and $250 for each failed Priority 3 response.

P-1. Pricing

Rates and charges for IBM Services for Managed Applications are found in the applicable section of this Service Guide or in the applicable Schedule.

Rates and charges set forth in this Service Guide are subject to change. Modification of the Service Guide shall be deemed notice of the change to Client.

A-1. Security Roles & Responsibilities

The following table lists security responsibilities and states which party is responsible for each one by inserting an “R” in the appropriate column for IBM or Client.

Category	Task	IBM	Client
Information Security Policies	Perform periodic systematic identification and evaluation of risks pertaining to the scope of the Agreement.	R	R
Information Security Policies	Perform risk and regulatory reviews and determine appropriate IBM Services for Managed Applications base security controls.	R	
Information Security Policies	Maintain Security Document and exception process.	R	
Information Security Policies	Evaluate exception requests posing risk to the larger IBM Services for Managed Applications environment and other Clients.	R	
Information Security Policies	Evaluate base controls in the IBM-managed portion of their environment to address requirements created by: business strategy, regulations, legislation and contracts, the current and projected information security threat environment.		R
Information Security Policies	Communicate to IBM their need for more stringent controls or risk acceptance of less stringent controls.		R
Information Security Policies	Notify IBM of all applicable regulatory requirements and inventory of affected devices.		R
Information Security Policies	Notify IBM of changes to security or regulatory requirements.		R
Information Security Policies	Remain in compliance with the Security Document including regulatory requirements and approved exceptions.		R
Information Security Policies	Provide Maintenance windows and support resources to maintain compliance.		R
Organization of Information Security	Provide a focal point for protection of its information assets and coordination of security related activities.		R
Organization of Information Security	Provide contact method for a primary and secondary security focal.	R	R
Organization of Information Security	Provide a schedule of maintenance windows.	R	

Category	Task	IBM	Client
Human Resource Security	Address security requirements in the hiring, termination and personnel management processes for personnel they manage.	R	R
Human Resource Security	Provide security awareness training to personnel they manage.	R	R
Human Resource Security	Take appropriate management action if there is a misuse of authority by personnel they manage.	R	R
Asset Management	Identify and communicate Client data or information requiring special handling.		R
Asset Management	During device decommissioning, destroy residual Client data within IBM's control.	R	R
Asset Management	Manage information identified by the Client as confidential information per Security Document.	R	
Cryptography	Define and provide to IBM Client’s data protection and handling requirements, if different from Security Document.		R
Cryptography	Provide and support encryption contained in the respective components they manage.	R	R
Cryptography	Generate, distribute and manage data encryption keys for the respective components they manage.	R	R
Physical and Environmental Security	Provide physical security infrastructure and controls at IBM-Managed Data Centers.	R	
System Acquisition, Development and Maintenance	Implement Security Document controls in systems acquisition and activation for IBM-managed components.	R	
Supplier Relationships	Establish contracts/agreements with external suppliers they manage.	R	R
Supplier Relationships	Coordinate all security activities with third parties managed by their organization.	R	R
Supplier Relationships	Establish policies and procedures for external suppliers they manage with access to information within their scope.	R	R
Supplier Relationships	Monitor performance against contracts/agreements/policies with external suppliers they manage.	R	R
Security Incident Management	Promptly report any security issues in the IBM managed environment.	R	R

Category	Task	IBM	Client
Security Incident Management	Provide for security incident coordination.	R	R
Security Incident Management	Cooperate in initial security incident evaluation.	R	R
Security Incident Management	Take actions to resolve security incidents involving networks, systems, data and personnel they manage.	R	R
Security Incident Management	Interface, as needed, with external entities such as law enforcement, legal or regulatory agencies.	R	R
Security Incident Management	Responsible for the business continuity including assessment, planning, testing and maintenance. Business continuity planning should include information security.		R
Operations Security	Provide a security audit focal point to coordinate IT audit support activities.	R	R
Operations Security	Provide support for IT audit activities such as data collection, audit tool installation and report generation.	R	R
Access Controls	Authorize user ids and privileges for components they manage.	R	R
Access Controls	Administer passwords on components they manage.	R	R
Access Controls	Reset and disclose passwords for components they manage.	R	R
Access Controls	Perform Employment Verification for their personnel on components they manage.	R	R
Access Controls	Perform Business Need Revalidation for their personnel on components they manage.	R	R
Access Controls	Configure a Business Use Notice for components they manage.	R	R
Access Controls	Identify and implement the protection and access logging requirements for user resources in components they manage.	R	R
Access Controls	Implement the functions and features of the software to set initial access controls for new folders, directories or files, for software components they manage.	R	R
Access Controls	Identify the protection requirements for critical system and software product files for software they manage.	R	R
Access Controls	Manage changes to components they manage according to the Change Control Process.	R	R

Category	Task	IBM	Client
Access Controls	Maintain compliance in the installation, maintenance and upgrades of software components they manage.	R	R
Access Controls	Capture and manage access records for components they manage, per the Security Document.	R	R
Operations Security - Network	Capture and manage logging functions for network components they manage.	R	R
Communications Security	Manage the internal and Internet-facing network infrastructure security for segments they manage.	R	R
Communications Security	Manage network security infrastructure components they manage, used for the inter-connection of Client network and IBM network.	R	R
Communications Security	Establish procedures for logging, alarming and reporting of network security violations on network devices they manage.	R	R
Communications Security	Perform periodic configuration reviews on IBM managed network infrastructure components.	R	
Communications Security	Manage access to IBM-managed software that monitors, manages, manipulates or modifies network configurations and traffic on infrastructure network segments managed by IBM.	R	
Communications Security	Implement and manage in-scope intrusion-detection and/or intrusion-prevention components on infrastructure network segments managed by IBM.	R	
Compliance	Perform external, non-authenticated TCP/IP vulnerability scans inside the internet firewalls.	R	
Compliance	Provide summary results of vulnerability scans upon request.	R	
Compliance	Take timely corrective action to address vulnerabilities, in accordance with risk level.	R	R
Compliance	Notify Client if vulnerabilities requiring Client's immediate attention.	R	
Compliance	For Client managed components, take timely corrective action to address vulnerabilities requiring immediate attention.		R
Operations Security - Compute	Provide and operate malware detection software for systems under IBM management.	R	
Operations Security - Compute	Respond to malware incidents on systems and devices they manage.	R	R

Category	Task	IBM	Client
Operations Security - Compute	Implement real-time scanning for malicious code on managed end points.	R	
Operations Security - Compute	Perform automated system security health assessment and enforcement for software managed by IBM.	R	
Operations Security - Software Maintenance (systems, network, storage)	Communicate planned security patch and update maintenance windows for IBM-managed software components.	R	
Operations Security - Software Maintenance (systems, network, storage)	Provide automation to support unattended installation of security patches and upgrades (e.g., automated application shutdown/restart).		R
Operations Security - Software Maintenance (systems, network, storage)	Assemble, and test patch bundles for IBM-managed software components and notify Client of contents.	R	
Operations Security - Software Maintenance (systems, network, storage)	Install patch bundles in scheduled maintenance windows for all IBM-managed software components and notify Client of results.	R	
Operations Security - Software Maintenance (systems, network, storage)	Provide for testing if required for approval prior to deploying patches and updates.		R
Operations Security - Software Maintenance (systems, network, storage)	Responsible for the management and installation of security patches and updates for all software components not managed by IBM.		R
Operations Security - Software Maintenance (systems, network, storage)	Maintain awareness of available security patches and upgrades for their environment, assess their applicability and determine their urgency.		R
Operations Security - Software Maintenance (systems, network, storage)	Notify IBM promptly when installation of security updates is required prior to the next scheduled maintenance window.		R
Operations Security - Software Maintenance (systems, network, storage)	Communicate impacts of anticipated and currently unsupported software components managed by IBM.	R	
Operations Security - Storage	Perform back-up and restore of storage assigned to the Client.	R	
Operations Security - Storage	Remove residual data at allocation of storage for use.	R	
Operations Security - Storage	Responsible for data removal meeting NIST-800-88 or other regulatory requirements.		R
Operations Security - Storage	Develop the security update and maintenance window schedule for Storage components.	R	

Category	Task	IBM	Client
Operations Security - Storage	Install applicable Storage security updates for components managed by IBM.	R	
Operations Security - Storage	Notify IBM promptly when installation of Storage security updates is required prior to the next scheduled window.		R
Operations Security - Storage	Client must provide for testing if required for approval to deploy updates.		R
Operations Security - Storage	Communicate impacts of anticipated and currently unsupported Storage components.	R	

A-2. Definitions

The definitions below apply to all IBM Services for Managed Applications. Additional definitions may be provided in the applicable Schedule.

Affiliates – entities that control, are controlled by, or are under common control with a party to this Agreement.

APIs – application programming interfaces IBM provides as Service Component which provide programming code to interface with and utilize the Services, including requesting and ordering Services options and Service Components, which bypass Cloud Web Portal user interfaces.

Availability - means a Client end-user's ability to access the production environment over the Infrastructure. Availability is calculated in accordance with the following formula: $x = [(n - y) * 100]/n$, where x = Availability percentage, n = total hours per month, and y = hours the Service was not available solely because of an act or omission by IBM for Services within IBM's direct control as detailed in applicable Parts of the Schedule (excluding Maintenance).

Change Request - modifications requested by Client and undertaken by IBM to the Client environment submitted via IBM's Change Request management process for risk and planning consideration.

Client – the Enterprise company identified in the signature block of the Order Document that incorporates services from this Service Guide and its Users.

Cloud Data Center – a data center facility where IBM provides the Services from and where Services Components are hosted and made available for Client use.

IBM – International Business Machines Corporation or its Enterprise (or offshore company operating in Client's country) that makes the Services available for the country specified in the Client's business address provided upon acceptance of this Service Guide.

Image – a software image file containing the functionality of the software program(s) that IBM makes available as part of the Services. An Image contains an Operating System Image by itself or in conjunction with an IBM Image or Third-Party Image.

Incident – means an unplanned IT service disruption affecting normal operations to any of Client's Services provided under a Schedule.

Internet – the public worldwide network of TCP/IP-based networks.

Infrastructure – includes equipment and software applications provided and managed by IBM and the Client that constitutes the physical and virtual computing, storage and network devices used to run software operating systems and applications, and may also include, but is not limited to, routers, switches, servers, and peripheral devices (including security service devices and fiber optic), used to provide the Service.

OS – Operating System software.

Order and Pricing Schedule (or Schedule) – means an ordering document signed by IBM and Client that is required for Client's initial order and any additional orders.

Portal – IBM Web site(s) designed to enable Client to use the Services and view additional Services options and Account information.

Service Catalog – a view of Service Components and Service options IBM makes available for Client selection and use within the Service.

Service Component Software – software functionality that IBM makes available as a Service Component.

Service Activation Date – a date when IBM notifies Client that IBM Services are available for Client use. Services may be initiated in stages (for example per each environment) and charges will begin for any portion of Services being received by Client as of each Service Activation Date.

Service Components – the hardware, software, Service Component Software, APIs, tools, and any documentation (electronic or otherwise) IBM utilizes to provide the infrastructure, Cloud Web Portal, and functionality of the Services or that IBM makes available as part of the Services.

Service Plan – 10 Change Requests or Service Requests per calendar month as requested by Client.

Service Request – means any request for Services or information made by Client to IBM in accordance with IBM's Service Request management process.

Service Tier – predetermined Client experience specified by IBM for servicing and managing IBM and Client relationship.

Services Credit – an amount equal to ten percent (10%) of Client's current monthly recurring charges (excluding any applicable taxes and fees) for each SLA, as applicable.

Services Focal Point – the IBM contact point(s) as specified by IBM to which Client directs communications relative to the Services.

Solution – Client-created software application service solution Client makes available to Solution Recipients in a VM.

Solution Recipients – means any entities or individuals to whom Client provides access to a VM or product or services that Client offers in a VM.

Subcontractor – a contractor, vendor, agent, or consultant selected and retained by IBM or Client, respectively

Usage Entitlements or **Entitlements** – mean the Authorizations and business parameters relating to Client's use of the Services that are set forth in the Charges Schedule and are used in part to determine the fees paid by Client for the Services (e.g. users, transactions, storage).

VM – a virtual machine instance that IBM makes available to Client as part of the Services consisting of virtual computer processing unit(s) ("CPUs"), virtual memory and virtual local storage.

End of Service Guide

IBM Corporation 2017

IBM, the IBM logo and ibm.com are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), these symbols indicate US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

ITIL is a registered trademark of AXELOS Ltd.

Microsoft, Windows, Windows NT, and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product and service names may be trademarks or service marks of others

This document is current as of the initial date of publication and may be changed by IBM at any time.

Not all offerings are available in every country in which IBM operates.

THE INFORMATION IN THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT ANY WARRANTY, EXPRESS OR IMPLIED, INCLUDING WITHOUT ANY WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND ANY WARRANTY OR CONDITION OF NONINFRINGEMENT.

IBM products are warranted according to the terms and conditions of the agreements under which they are provided.

This page is blank