IBM Managed Security Services - Vulnerability Scanning

This Service Description describes the Service IBM provides to Client.

1.1 Service

IBM Managed Security Services - Vulnerability Scanning (called "VS") is a vulnerability scanning service designed to provide Client with the support necessary to meet a range of needs (such as support for Client's internal audit and risk assessment, regulatory compliance, and industry compliance requirements). VS includes a robust suite of functionality although Client must specifically request that an environment be configured for Client if Client desires certified Payment Card Industry ("PCI") Approved Scanning Vendor reports.

Under VS, Client may request IBM to perform un-validated scans of Client's environment using internal or external scanning methods, which can be employed together or separately. External scanning involves vulnerability scans originating from outside Client's physical environment. Scans of Client's public-facing IP addresses and Web applications are designed to provide vulnerability detection of security risk exposures open to the Internet (i.e., an intruder reaching Client's environment from the public Internet). Internal scanning allows Client to assess the state of security vulnerabilities from within Client's enterprise network. Internal scans may provide a more thorough analysis of target machines by avoiding scan interference from firewalls and other security devices.

Decisions as to which vulnerabilities will be detectable by VS are at IBM's sole discretion and will be based in part on severity, prevalence, and priority of the vulnerability relative to other threats being covered.

The Services features described herein are dependent upon the availability and supportability of products and product features being utilized. Even in the case of supported products, not all product features may be supported. Information on supported features are available from IBM upon request. This includes both IBM-provided and non-IBM-provided hardware, software, and firmware. VS support analysts are only available Monday through Friday between the hours of 1AM GMT and 7AM GMT.

1.1.1 Service Activities – VS Deployment and Activation

During VS deployment and activation, IBM will work with Client to configure the Services and, if ordered by Client, provide remote assistance to deploy the required Agents for internal scanning that will be located on Client's premises, as specified in the Order Document.

IBM Responsibilities

IBM will:

a. provide Client with a document called "Customer Premise Equipment (CPE) Vulnerability Scanner Setup Instructions" which details:
   (1) specifications for the hardware/software that Client must provide;
   (2) options for hardware/software requirements;
   (3) the steps Client must take to configure and install internal Agents for use with the Services; and
   (4) network access requirements to allow IBM to connect to internal Agent(s) at Client's location;

b. if applicable, provide Client with access to the software image including operating system and virtual scanning software to apply to the hardware that Client provides, when virtual scanning is requested.

Client Responsibilities

Client agrees:

a. to provide server hardware and/or software compliant with the system requirements contained in the CPE Vulnerability Scanner Setup Instructions for any locations for which Client requests internal scanning;

b. and acknowledges that any hardware and/or software Client provides, that is not compliant with the IBM-provided system requirements, may result in a software package installation or operation failure;

c. to follow the provided setup instructions for loading and configuring the internal virtual scanning software image;

d. to ensure that any hardware and/or software provided is covered under an active service contract for the duration of the Services;

e. and acknowledges, for complete and accurate scanning results, Client must configure and maintain Client's network topology and security devices to allow unfiltered scan traffic from Client's scan engines to Client's selected scan targets; and

f. to perform scans only on IP addresses and/or web domains that Client owns or has legal authority to scan. Pursuant to the "Systems Owned by a Third Party" clause in the Order Document and prior to Client initiating associated scans, Client must obtain and provide to IBM evidence of consent from the owner of each system authorizing Client to perform scans.

1.1.2 Service Activities - Managed Agent Health and Availability Monitoring

IBM will monitor the health status and availability of the internal scanners. Such monitoring is designed to assist in increasing availability and uptime of the Agents.

Depending on the number of IP addresses under Client's active VS contract, IBM will monitor a specific number of Agents specified in the Order Document.

IBM Responsibilities

IBM will:

a. verify health and alert monitoring is reporting correctly to the Vulnerability Portal environment;

b. perform quality assurance testing of the Agent;

c. support Client in executing Services acceptance testing;

d. verify availability and functionality of the Agent in the Vulnerability Portal; and

e. remotely demonstrate the primary features of the Vulnerability Portal for up to ten (10) of Client's personnel, for up to one hour.

Client Responsibilities

Client agrees:

a. to be responsible for development of all of Client's specific acceptance testing plans;

b. to be responsible for performing acceptance testing of Client's applications and network connectivity; and

c. and acknowledges:

(1) IBM does not participate in troubleshooting and or problem resolution activities that do not directly pertain to the deployment and/or health of the managed Agent subscribing to the Services;

(2) that additional acceptance testing performed by Client, or lack thereof, does not preclude IBM from setting the Agent to "active" in the SOCs for ongoing support and management; and

(3) Client is responsible for scheduling night and weekend work in advanced as determined during the project kick-off call. Night and weekend work is provided at an additional cost and subject to IBM resource availability and blackout dates.

1.1.3 Service Activities - Agent Management

Agent application and security updates are critical components of an enterprise.

IBM Responsibilities

IBM will:

a. maintain system status awareness; and

b. to maintain current licensing, and support and maintenance contracts.

Client Responsibilities

Client agrees:

a. to perform IBM-specified platform upgrades to support the current software;

b. to ensure appropriate consents are in place with Client's vendors to allow IBM to leverage existing support and maintenance contracts on Client's behalf. If such agreements are not in place, IBM will not be able to contact the vendor directly to resolve support issues; and

c. and acknowledges:

   (1) all updates are transmitted and applied via the Internet; and

   (2) if vendor consents are not obtained or are revoked at any point during the contract period, Services and/or SLAs may be suspended by IBM.

1.1.4 Service Activities - Services Vulnerability Scanning and Reporting

Utilizing the Vulnerability Portal, Client will have access to Services information and reporting.

IBM Responsibilities

IBM will:

a. provide Client with access to reporting capabilities for the Service in the MSS Portal and Vulnerability Portal which include:

   (1) number, types, and summary of Services requests/tickets;

   (2) details of scans performed in a variety of predefined and customizable formats;

   (3) tuning; and

   (4) scan scheduling and configuration;

b. provide Client with access to scan results raw scan data, available for thirteen (13) months from date of creation in the Vulnerability Portal; and

c. implement scans based on client provided scan schedule and configuration.

Client Responsibilities

Client agrees:

a. to access the Vulnerability Portal to view scan reports;

b. and acknowledges that reports are available for no longer that seven (7) days from the date of creation;

c. to provide valid IP inventory for scanning; and

d. to provide details regarding scan configuration and policy.

1.1.5 Service Activities - PCI Approved Scanning Vendor Services

Client may request that IBM act as an Approved Scanning Vendor ("ASV"), which is a vulnerability scanning solution provider, approved by the Payment Card Industry Security Standards Council ("PCI SSC"). PCI SSC is the organization responsible for defining data security standards for organizations that handle credit card data. Such ASVs provide services to organizations and are subject to the Payment Card Industry ("PCI") data security standards. Upon request, IBM will act as an ASV to enable Client to submit ASV-certified scan reports to Client's acquiring banks or payment brands.

IBM Responsibilities

At Client's request and for no additional charge, IBM will:

a. respond to vulnerability exception requests by:

(1) accepting an unlimited number of vulnerability exception requests submitted by Client via tickets from the MSS Portal;

(2) reviewing vulnerability exception requests to verify Client has provided adequate documentation to justify the requested exception;

(3) approving or denying vulnerability exception requests, at IBM's sole discretion, within the timeframes established in the section of this Services Description entitled "Service Level Agreements", "PCI vulnerability exception request response";

b. produce the ASV Scan Report Attestation of Scan Compliance cover sheet and the scan reports as required for submission by Client to acquiring banks or payment brands; and

c. retain scan reports and related work products for two years, as required by the Validation Requirements for Approved Scanning Vendors.

Note: Client's access and use of the reports provided via the MSS Portal is also subject to the Terms of Use provided therein. Where such Terms of Use conflict with the terms of this Services Description or any associated contract documents, the MSS Portal Terms of Use shall prevail over this Services Description. In addition to the Terms of Use provided in the MSS Portal, Client's use of any information on any links or non-IBM Web sites and resources are subject to the terms of use posted on such links, non-IBM Web sites, and resources.

Client Responsibilities

Client agrees:

a. to identify (and configure if appropriate) MSS Portal users who are authorized to use the PCI feature of the vulnerability management tool within the MSS Portal;

b. configure accurate merchant account settings within the PCI feature of the vulnerability management tool;

c. to define the scope of external vulnerability scanning, which includes:

(1) purchase a license sufficient to include all systems that are in scope for the PCI ASV scan per Payment Card Industry Data Security Standards ("PCI DSS") which states that external vulnerability scanning be performed quarterly by an ASV qualified by PCI SSC;

(2) configuring the scope within the PCI feature of the vulnerability management tool per PCI DSS requirements; and

(3) implementing proper network segmentation for any excluded external facing IP addresses;

d. and acknowledges that Client is solely responsible for the accuracy and completeness of the scope for PCI scans (i.e., the IP addresses and/or Web domains);

e. to ensure that devices do not interfere with the ASV scan, including:

(1) configuring intrusion detection systems (IDSs), intrusion prevention systems (IPSs) and other devices so they do not interfere with the scan (e.g., allow temporary unfiltered network access to target systems from the relevant external scanners);

(2) coordinating with IBM if Client has load balancers in use;

f. if load balancers are in use, to provide:

(1) documented assurance that the infrastructure behind the load balancer(s) is synchronized in terms of configuration, or

(2) documented assurance that the configured PCI scope uniquely identifies all load balanced devices such that a complete scan can be performed;

g. to be responsible for coordinating with Client's Internet service provider ("ISP") and/or hosting providers to allow completely unfiltered network traffic between the relevant external scanners and Client's target network(s);

h. if Client disputes scan results for a particular vulnerability, Client will:

(1) use the MSS Portal to request an exception and provide sufficient documentation to IBM to aid IBM's investigation and resolution of the disputed findings (for example, suspected false positives), and provide related attestation within the MSS Portal via SOC ticket;

(2) submit system-generated evidence such as screen dumps, configuration files, system versions, file versions, and a list of installed patches. Such system-generated evidence must be accompanied by a description of when, where and how it was obtained; and

(3) acknowledge that IBM may require Client to engage (at Client's expense) a PCI Qualified Security Assessor ("QSA") before approving certain disputes (such as proposed compensating controls);

i. to use the Vulnerability Portal to initiate scanning;

j. to review the scan results and correct any noted vulnerabilities that result in a non-compliant scan;

k. to use the Vulnerability Portal to initiate re-scanning of any non-compliant IP addresses to obtain a passing quarterly scan;

l. generate all required reports within the tool;

m. submit reports via the tool to the ASV for review and approval as appropriate;

n. to submit a SOC ticket via the MSS Portal to request that IBM review Client's submitted reports to product the final quarterly PCI ASV Attestation of Scan Compliance;

o. to download completed ASV scan reports and submit them to Client's acquirer or payment brands, as directed by the payment brands; and

p. that by downloading and submitting ASV reports to acquirers or payment brands, Client attests and acknowledges that:

(1) Client has not and will not change or alter the system-generated ASV reports in any way before submitting them to Client's acquirers or payment brands;

(2) Client is responsible for proper scoping of the scans and have included all components in the scan that should be included in the PCI DSS scope;

(3) Client has implemented network segmentation, if any components are excluded from PCI DSS scope;

(4) Client has provided accurate and complete evidence to support any disputes over scan results; and

(5) scan results only indicate whether scanned systems are compliant with the external vulnerability scan requirement for PCI DSS and are not an indication of overall compliance with any other PCI DSS requirements.

1.2 Service Levels

IBM provides the following service level agreements ("SLAs") for the Services. The SLAs become effective when the deployment process has been completed, the Agent(s) (if any) has been set to "active", and support and management of the Agent have been successfully transitioned to "active" in the SOCs. The SLA remedies are available provided Client meets Client's obligations as defined in this Services Description and all associated contract documents.

1.2.1 Service Level Availability

The SLA defaults described below comprise the measured metrics for delivery of the Services. Unless explicitly stated below, no warranties of any kind shall apply to Services delivered under this Services Description. The sole remedies for failure to meet the SLA defaults are specified in the section of this Services Description entitled "SLA Remedies".

a. Pre-Scheduled Scanning implementation – IBM will begin implementation of a pre-scheduled Vulnerability Scan no later than one (1) hour after the pre-scheduled time by Client (or by IBM on Client's behalf).

b. Scanning Implementation Support – Response times for VS Clients can take up to two (2) business days for any non-scheduled scans (general service support and report analysis.) This SLA applies only to correctly configured scan requests, customer-premises Agents that are on-line and accessible by the SOC infrastructure, and scan targets that are fully accessible from the designated scan engine.

c. PCI scope change request acknowledgement – IBM will acknowledge PCI scope change requests within two (2) hours after such requests are submitted via the MSS Portal. Client may submit an unlimited number of PCI scope change requests.

d. PCI scope change implementation – IBM will implement PCI scope changes within three (3) business days of receiving sufficient and acceptable documentation from Client to justify the PCI scope change.

e. PCI vulnerability exception request response – IBM will respond with either an approval or denial for the first fifteen (15) of the exception requests submitted by the Client in a given day within three (3) business days of receiving sufficient and acceptable documentation from Client to justify the PCI vulnerability exception request.

Note: Client may submit an unlimited number of PCI vulnerability exception requests. All requests beyond the first fifteen (15) received in a given day will be accepted but not treated as a priority, and will not be bound by this SLA.

The SLA defaults described comprise the measured metrics for delivery of services. Unless explicitly stated, no warranties of any kind shall apply to Services delivered under this Service Description. The sole remedies for failure to meet the SLA defaults are specified in the section of this Service Description entitled, "SLA Remedies."

1.2.2 Service Level Remedies

Services availability, MSS Portal availability, Proactive system monitoring, scanning implementation, PCI scope change request acknowledgement, PCI scope change request implementation, PCI vulnerability exception request response – If IBM fails to meet any of these SLAs, a credit will be issued for the applicable charges for one (1) day of the monthly VS service charges.

SLAs and Remedies Summary

Service Level Agreements	Availability Remedies
Proactive system monitoring	Credit for one (1) day of the monthly Services charge
Scanning implementation	
PCI scope change request acknowledgement	
PCI scope change request implementation	
PCI vulnerability exception request response	

1.3 Payment Card Industry Covenants

Client acknowledges that IBM is an ASV and is operating under a current agreement with the PCI SSC. In accordance with the terms of such agreement, the following flow-through provisions are incorporated into this Services Description.

a. Client acknowledges and agrees that Client may be ordering Services from IBM in connection with Client's obligation to comply with the Payment Card Industry Data Security Standard ("PCI-DSS"). Client understands that administration of the PCI-DSS in connection with security assessments is conducted by major payment card brands ("Brands"), and such administration is placed with the PCI SSC. Client acknowledges and agrees that Client chose IBM to provide Services from a list of approved vendors published by the PCI SSC (the "ASV List"). Further, Client acknowledges that in order for IBM to be included in the ASV List, IBM is required to sign an agreement with the PCI SSC (the "ASV Agreement") a form of which is located at www.pcisecuritystandards.org, "Validation Requirements for Approved Scanning Vendors, Appendix A PCI ASV Compliance Test Agreement". Client also acknowledges that parts of that agreement require IBM to include certain provisions in its agreements with its customers.

(1) Client understands and agrees that the inclusion of IBM on the ASV List is neither an implied or express PCI SSC endorsement or recommendation, nor warranty by the PCI SSC or any of its Members regarding IBM, IBM services or products, or the functionality, quality or

performance of any aspect of any of the foregoing. Additionally, Client understands and agrees that the PCI SSC does not require Client to use IBM products or services. Client also agrees that for the purposes of this "Payment Card Industry Covenants" section, capitalized terms in items a. (2), (3), (4), and (5) below shall have the meanings ascribed to them in the ASV Agreement.

(2) Client understands and agrees that (i) IBM may disclose testing and assessment results (including scan reports) and related information as requested by the PCI SSC and/or its Members, as requested by Client, (ii) to the extent any Member obtains such information in accordance with the preceding clause, such Member may disclose such information on an as needed basis to such Members' respective Financial Institutions and Issuers and to relevant governmental, regulatory, and law enforcement inspectors, regulators and agencies, and (iii) IBM may disclose such information as necessary to comply with its obligations and requirements pursuant to the ASV Agreement, as further specified in clause (4) below. Client agrees that the PCI SSC or their Acquirer may disclose Confidential Information obtained by the PCI SSC in connection with the ASV Agreement to Members in accordance with this item a. (2), who may in turn disclose such information to their respective Member Financial Institutions and other Members. Client consents to (i) such disclosure by the PCI SSC and its Members and (ii) any disclosure of Confidential Information, including without limitation testing and assessment results (including scan reports), and related information, permitted by this item a. (2). To the extent, Client has any confidentiality agreement with IBM; the terms of this item a. (2) are incorporated into such agreement by this reference.

(3) Client understands that IBM has, in the ASV Agreement, agreed to maintain certain data protection handling practices regarding Personal Information, if any, received by IBM from the PCI SSC or any Member or Customer, and IBM has also agreed to make available to the PCI SSC and its Members and/or Acquirers/Issuers such appropriate reviews and reports to monitor IBM compliance with those data protection handling practice requirements. Client consents to IBM furnishing such reviews and reports to the PCI SSC and its Members and/or Acquirers/Issuers and also agrees that Client shall provide the PCI SSC or any Member and/or Acquirers/Issuers with such appropriate reports and reviews to monitor IBM compliance with those data protection handling practice requirements as the PCI SSC or its Members and/or Acquirers/Issuers may reasonably request from time to time.

(4) Client also understands that IBM has, in the ASV Agreement, upon written request by PCI SSC or any Member (each a "Requesting Organization") agreed to provide to such Requesting Organization such testing and assessment results (including scan reports) as such Requesting Organization may reasonably request with respect to (i) if the Requesting Organization is a Member, any Vendor Client for which IBM has performed an assessment and that is a Financial Institution of such Member, an Issuer of such Member, a merchant authorized to accept such Member's payment cards, an Acquirer of accounts of merchants authorized to accept such Member's payment cards or a Processor performing services for such Member's Financial Institutions, Issuers, Merchants or Acquirers or (ii) if the Requesting Organization is PCI SSC, any Vendor Client for which ASV has performed testing or assessment. Client consents to any such disclosure of any testing and assessment results (including scan reports) regarding it and grant IBM all necessary rights, licenses and other permissions necessary for IBM to comply with its obligations and requirements under the ASV Agreement.

Client's Indemnity regarding Payment Card Industry Services

b. To the extent that IBM provides Services as an ASV, Client shall defend, indemnify and hold harmless IBM from and against all claims, losses, liabilities, damages, claims, suits, actions, government proceedings, taxes, penalties or interest, associated auditing and legal expenses and other costs (including without limitation, reasonable attorney's fees and related costs) arising out of claims by PCI Security Standards Council LLC, its Members and their respective subsidiaries, and all affiliates, subsidiaries, directors, officers, employees, agents, representatives, independent contractors, attorneys, successors, and assigns of any of the foregoing against IBM or IBM Affiliates relating to the Services hereunder.