IBM United Kingdom Limited
Registered in England: 741598
Registered Office: PO Box 41,
North Harbour, Portsmouth,
PO6 3AU (hereinafter "IBM")

Services Description

IBM Managed Security Services (Cloud Computing) - Hosted Vulnerability Management

IN ADDITION TO THE TERMS AND CONDITIONS SPECIFIED BELOW, THIS SERVICES DESCRIPTION INCLUDES THE "IBM MANAGED SECURITY SERVICES GENERAL PROVISIONS" ("GENERAL PROVISIONS") LOCATED AT http://www-935.ibm.com/services/uk/gts/html/contracts_landing.html AND INCORPORATED HEREIN BY REFERENCE.

1. Scope of Services

IBM Managed Security Services (Cloud Computing) - Hosted Vulnerability Management (called "VMS" or "Services") is a vulnerability scanning service designed to provide you with the tools necessary to meet a range of needs (such as support for your internal audit and risk assessment, regulatory compliance, and industry compliance requirements). VMS includes a comprehensive suite of functionality although you must specifically request that an environment be configured for you if you desire certified Payment Card Industry ("PCI") Approved Scanning Vendor reports.

IBM provides VMS as a solution to be operated by you. IBM provides the scanning application and technical support for the application; however, you are responsible for operating the Services and for the results achieved from the Services.

Decisions as to which vulnerabilities will be detectable by VMS are at IBM's sole discretion. Such decisions will be based on severity, prevalence, ability of VMS to safely detect the vulnerability, and priority of the vulnerability relative to other threats being covered.

VMS is provided in two distinct types of scanning which can be employed together or separately;

- External – IBM hosts and manages vulnerability scanners on the Internet. Such scanners can be used to scan your public-facing IP addresses and Web applications and are designed to provide vulnerability detection of security risk exposures open to the Internet.
- Internal – allows you to assess the state of security vulnerabilities within your enterprise network, utilizing an IBM-managed on-premise scanning device (called "Agent"). Such Agents must not be used for any other purpose while under management by IBM.

The Services features described herein are dependent upon the availability and supportability of products and product features being utilised. Even in the case of supported products, not all product features may be supported. Information on supported features is available from IBM upon request. This includes both IBM-provided and non-IBM-provided hardware, software, and firmware.

2. Definitions

Alert Condition ("AlertCon") – a global risk metric, developed by IBM, using proprietary methods. The AlertCon is based on a variety of factors, including quantity and severity of known vulnerabilities, exploits for such vulnerabilities, the availability of such exploits to the public, mass-propagating worm activity, and global threat activity. The four levels of AlertCon are described in the IBM Managed Security Services ("IBM MSS") portal (called "Portal").

Approved Scanning Vendor ("ASV") – a vulnerability scanning solution provider, approved by the PCI SSC. Such ASVs provide services to organisations which are subject to the Payment Card Industry ("PCI") data security standards.

Education Materials – include, but are not limited to, lab manuals, instructor notes, literature, methodologies, electronic course and case study images, policies and procedures, and all other training-related property created by or on behalf of IBM. Where applicable, Education Materials may include participant manuals, exercise documents, lab documents and presentation slides provided by IBM.

External Vulnerability Scanning – vulnerability scans originating from an IBM scanner located outside your physical environment. External scans simulate the point of view of an outsider threat (for example, a hacker reaching your environment from the public Internet).

Internal Vulnerability Scanning – vulnerability scans originating from a scanning device located on your premises. Internal scans may provide a more thorough analysis of target machines by avoiding scan interference from firewalls and other security devices.

Payment Card Industry Security Standards Council ("PCI SSC") – the organisation responsible for defining data security standards for organisations that handle credit card data.

3. Services

The following table highlights the measurable Services features. The subsequent sections provide narrative descriptions of each Services feature.

Services Feature Summary

Services Feature	Metric or Qty	Service Level Agreements
Services availability	100%	Services availability SLA
IBM MSS Portal availability	99.9%	IBM MSS Portal availability SLA
Authorised Security Contacts	3 users	N/A
Agent health alerting	15 minutes	Proactive system monitoring SLA
External/internal scan quantity/frequency	Unlimited	N/A
Vulnerability scanning implementation	+/- 1 hour	Scanning implementation SLA
PCI ASV Services Features	**Metric or Qty**	**Service Level Agreements**
PCI scope change request	Unlimited	N/A
PCI scope change request acknowledgement	2 hours	PCI scope change request acknowledgement SLA
PCI scope change request implementation	72 hours	PCI scope change request implementation SLA
PCI vulnerability exception review request	Unlimited	N/A
PCI vulnerability exception review request response	72 hours	PCI exception review request SLA
PCI ASV Attestation	One per quarter	N/A

3.1 Security Operations Centers

IBM Managed Security Services are delivered from a network of IBM Security Operations Centers ("SOCs"). IBM will provide access to the SOCs 24 hours/day, 7 days/week.

3.2 Portal

The Portal provides you with access to an environment (and associated tools) designed to monitor and manage your security posture by merging technology and service data from multiple vendors and geographies into a common, Web-based interface.

The Portal may also be used to deliver Education Materials. All such Education Materials are licensed not sold and remain the exclusive property of IBM. IBM grants you a license in accordance with the terms provided in the Portal. EDUCATION MATERIALS ARE PROVIDED "AS IS" AND WITHOUT WARRANTY OR INDEMNITY OF ANY KIND BY IBM, EXPRESS OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THE WARRANTIES OF SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF PROPRIETARY AND INTELLECTUAL PROPERTY RIGHTS.

3.2.1 IBM Portal Responsibilities

IBM will:

a. provide access to the Portal 24 hours/day, 7 days/week. The Portal will provide:
   (1) default scanning templates and reporting templates:
   (2) security intelligence awareness and alerting;
   (3) service ticket information;
   (4) ticketing and workflow initiation and updates;
   (5) live chat and collaboration with SOC analysts;
   (6) a template-driven reporting dashboard;
   (7) access to scan results;
   (8) authorisation to download data; and
   (9) access to Education Materials in accordance with the terms provided in the Portal; and

b. maintain availability of the Portal in accordance with the metrics provided in the section of this Services Description entitled "Service Level Agreements", "Portal Availability".

3.2.2 Your Portal Responsibilities

You agree to:

a. utilise the Portal to perform daily operational Services activities;

b. ensure your employees accessing the Portal on your behalf comply with the Terms of Use provided therein including, but not limited to, the terms associated with Educational Materials and other deliverable items, such as scan and summary reports;

c. appropriately safeguard your login credentials to the Portal (including not disclosing such credentials to any unauthorised individuals);

d. promptly notify IBM if a compromise of your login credentials is suspected; and

e. indemnify and hold IBM harmless for any losses incurred by you or other parties resulting from your failure to safeguard your login credentials.

3.3 Services Contacts

You may choose from multiple levels of access to the SOC and the Portal to accommodate varying roles within your organisation.

Authorised Security Contacts

An Authorised Security Contact is defined as a decision-maker on all operational issues pertaining to IBM Managed Security Services.

Designated Services Contacts

A Designated Services Contact is defined as a decision-maker on a subset of operational issues pertaining to IBM Managed Security Services, an Agent, or a group of Agents. IBM will only interface with a Designated Services Contact regarding operational activities that fall within the subset for which such contact is responsible (for example, designated Agent outage contact).

Portal Users

IBM provides multiple levels of access for Portal users. These levels of access can be applied to an IBM Managed Security Service, an Agent, or a group of Agents. Portal users will be authenticated via static password or a public-key encryption technology you provide (for example, RSA SecureID token) based on your requirements.

3.3.1 IBM Services Contacts Responsibilities

Authorised Security Contacts

IBM will:

a. allow you to create up to three Authorised Security Contacts;

b. provide each Authorised Security Contact with:
   (1) administrative Portal permissions to your Agents;

(2) the authorisation to create unlimited Designated Services Contacts and Portal users;

(3) the authorisation to delegate responsibility to Designated Services Contacts;

c. interface with Authorised Security Contacts regarding support and notification issues pertaining to the Services; and

d. verify the identity of Authorised Security Contacts using an authentication method that utilises a pre-shared challenge pass phrase.

Designated Services Contacts

IBM will:

a. verify the identity of Designated Services Contacts using an authentication method that utilises a pre-shared challenge pass phrase; and

b. interface only with Designated Services Contacts regarding the subset of operational issues for which such contact is responsible.

Portal Users

IBM will:

a. provide access to the Portal with capabilities that may include (as appropriate):

(1) submitting Services requests to the SOCs;

(2) "live chat" communicating with SOC analysts regarding specific incidents or tickets, generated as part of the Services;

(3) creating internal Services-related tickets and assigning such tickets to Portal users;

(4) querying, viewing, and updating Services-related tickets;

(5) creating and modifying custom scan templates (except PCI templates);

(6) creating and modifying custom report templates (except PCI reports);

(7) submitting vulnerability exception requests;

(8) reviewing, and approving vulnerability exceptions (except PCI exceptions);

(9) defining scan sites (the IP addresses and web domains to be included in the scan scope) and the users and policies associated with the site (except PCI scope);

(10) scheduling and running scans;

(11) scheduling and running reports;

b. authenticate Portal users using static password; and

c. authenticate Portal users using a public-key encryption technology you provide (for example, RSA SecureID token) based on your requirements.

3.3.2 Your Services Contacts Responsibilities

Authorised Security Contacts

You agree:

a. to provide IBM with contact information for each Authorised Security Contact. Such Authorised Security Contacts will be responsible for:

(1) creating Designated Services Contacts and delegating responsibilities and permissions to such contacts, as appropriate;

(2) creating Portal users;

(3) authenticating with the SOCs using a pre-shared challenge pass phrase; and

(4) maintaining notification paths and your contact information, and providing such information to IBM;

b. to ensure at least one Authorised Security Contact is available 24 hours/day, 7 days/week;

c. to update IBM within three calendar days when your contact information changes; and

d. and acknowledge that you are permitted to have no more than three Authorised Security Contacts regardless of the number of IBM services or Agent subscriptions for which you have contracted.

Designated Services Contacts

You agree:

a. to provide IBM with contact information and role responsibility for each Designated Services Contact. Such Designated Services Contacts will be responsible for authenticating with the SOCs using a pass phrase; and

b. and acknowledge that a Designated Services Contact may be required to be available 24 hours/day, 7 days/week based on the subset of responsibilities for which it is responsible (i.e., Agent outage).

Portal Users

You agree:

a. that Portal users will use the Portal to perform daily operational Services activities;

b. to be responsible for providing IBM-supported RSA SecureID tokens (as applicable); and

c. and acknowledge the SOCs will only interface with Authorised Security Contacts and Designated Services Contacts.

3.4 Security Intelligence

Security intelligence is provided by the IBM X-Force® Threat Analysis Center. The X-Force Threat Analysis Center publishes an Internet AlertCon threat level. The AlertCon describes progressive alert postures of current Internet security threat conditions. In the event Internet security threat conditions are elevated to AlertCon 3, indicating focused attacks that require immediate defensive action, IBM will provide you with real-time access into IBM's global situation briefing. As a user of the Portal, you have access to the X-Force Hosted Threat Analysis Service. The X-Force Hosted Threat Analysis Service includes access to the IBM X-Force Threat Insight Quarterly ("Threat IQ").

Utilizing the Portal, you can create a vulnerability watch list with customised threat information. In addition, each Portal user can request to receive an Internet assessment e-mail each business day. This assessment provides an analysis of the current known Internet threat conditions, real-time Internet port metrics data, and individualised alerts, advisories and security news.

Note: Your access and use of the Security intelligence provided via the Portal (including the Threat IQ and the daily Internet assessment e-mail) is 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 Portal Terms of Use shall prevail. In addition to the Terms of Use provided in the Portal, your 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.

3.4.1 IBM Security Intelligence Responsibilities

IBM will:

a. provide you with access to the X-Force Hosted Threat Analysis Service;

b. provide you with a username, password, URL and appropriate permissions to access the Portal;

c. display security information on the Portal as it becomes available;

d. if configured by you, provide security intelligence specific to your defined vulnerability watch list, via the Portal;

e. if configured by you, provide an Internet security assessment e-mail each business day;

f. publish an Internet AlertCon via the Portal;

g. declare an Internet emergency if the daily AlertCon level reaches AlertCon 3. In such event, IBM will provide you with real time access into IBM's global situation briefing;

h. provide Portal feature functionality for you to create and maintain a vulnerability watch list;

i. provide additional information about an alert, advisory, or other significant security issue as IBM deems necessary; and

j. provide access to the Threat IQ via the Portal.

3.4.2 Your Security Intelligence Responsibilities

You agree to use the Portal to:

a. subscribe to the daily Internet security assessment e-mail, if desired;

b. create a vulnerability watch list, if desired; and

c. access the Threat IQ; and

d. provide your agreement to adhere to the licensing agreement and not forward Services information to individuals who do not have a proper license.

3.5 Deployment and Activation

During deployment and activation, IBM will work with you to configure the Services and, if applicable, deploy internal scanning Agents.

Note: Deployment and activation activities are performed one time during the performance of the services. If you choose to replace, upgrade, or move your Agent(s) during the Services contract, IBM may require that such Agent(s) be redeployed and reactivated (called "Redeployment"). Such Redeployments will be provided at an additional charge as specified in the Schedule. Redeployment charges apply only to hardware replacements, upgrades, or moves that you initiate. Such charges do not apply to Agent failures resulting in Agent Return Material Authorisation ("RMA") activities.

3.5.1 IBM Deployment and Activation Responsibilities

Activity 1 - Project Kickoff

The purpose of this activity is to conduct a project kickoff call, if applicable. IBM will send you a welcome e-mail and (if applicable) conduct a kickoff call, for up to one hour for up to three of your personnel, to:

a. introduce your Point of Contact to the assigned IBM deployment specialist;

b. review each party's respective responsibilities;

c. set schedule expectations; and

d. begin to assess your requirements and environment.

Completion Criteria:

This activity will be complete when IBM has conducted the project kickoff call.

Deliverable Materials:

- None

Activity 2 - Internal Scanning Agent Hardware Requirements

The purpose of this activity is to establish hardware requirements for internal scanning engine(s) that will be located on your premises.

IBM will:

a. provide you with a document called "Customer Premise ("CPE") Vulnerability Scanner Setup Instructions" which details:

   (1) specifications for hardware you must provide; and

   (2) the steps you must take to configure and install internal scan engines for use with the Services;

b. provide you with access to the software image including operating system and scanning software to apply to the hardware that you provide.

Completion Criteria:

This activity will be complete when IBM has provided your Point of Contact with the Customer Premise ("CPE") Vulnerability Scanner Setup Instructions.

Deliverable Materials:

- Customer Premise ("CPE") Vulnerability Scanner Setup Instructions

Activity 3 - Network Access Requirements for Internal Scanning

The purpose of this activity is to establish network access requirements.

IBM will:

a. provide you with a document called "Network Access Requirements", detailing:

(1) how IBM will connect remotely to your network;

(2) specific technical requirements to enable such remote connectivity;

Note: IBM may make changes to the "Network Access Requirements" document, as it deems appropriate, throughout the performance of the Services.

b. connect to your network through the Internet, using IBM standard access methods; and

c. if appropriate, utilise a site-to-site virtual private network ("VPN") to connect to your network. Such VPN may be provided by IBM for an additional charge as specified in the Schedule.

Completion Criteria:

This activity will be complete when IBM has provided your Point of Contact with the Network Access Requirements document.

Deliverable Materials:

- Network Access Requirements document

Activity 4 - Assessment

The purpose of this activity is to perform an assessment of your current environment, and business and technology goals, and (if applicable) to help develop the required security strategy for deployment and usage of internal scanning Agent(s).

Task 1 - Gather Data

IBM will:

a. provide your Point of Contact with a data gathering form on which you will be asked to document items such as:

(1) team member names, contact information, roles and responsibilities;

(2) unique country and site requirements;

(3) number and type of end users;

(4) key business drivers and/or dependencies that could influence Services delivery or timelines; and

(5) PCI IP addresses and domains subject to PCI (as applicable).

Task 2 - Assess Environment for Internal Scanning

IBM will:

a. use the information provided in the data gathering form to assess your existing environment;

b. determine optimal Agent placement; and

c. if applicable, provide recommendations to adjust the layout of the network and security policies to allow scanning of desired targets.

Completion Criteria:

This activity will be complete when IBM has completed its assessment of your environment.

Deliverable Materials:

- None

Activity 5 - Implementation for Internal Scanning

The purpose of this activity is to implement the Agent(s).

Task 1 - Configure the Agent

IBM will:

a. remotely assess the Agent(s) to verify it meets IBM specifications;

b. identify Agent hardware that does not meet current IBM-supported levels; and

c. provide live phone support to assist you with loading the software image and configuring the Agent with a public IP address and associated settings. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist.

Task 2 - Install the Agent

IBM will:

a. provide live support, via phone and/or e-mail, to assist you in locating applicable vendor documents that detail physical installation procedures and cabling. Such support must be scheduled in advance to ensure availability of an IBM deployment specialist;

b. provide recommendations to adjust the layout of the network to help enhance security (as applicable); and

c. remotely configure the Agent, including registering the Agent with the IBM MSS infrastructure.

Note: You may contract separately for IBM to provide physical installation services.

Completion Criteria:

This activity will be complete when the Agent has been registered with the IBM MSS infrastructure.

Deliverable Materials:

- None

Activity 6 - Testing and Verification

The purpose of this activity is to perform testing and verification of the Services.

IBM will:

a. for each Agent
   (1) verify connectivity of the Agent to the IBM MSS infrastructure;
   (2) verify delivery of scan data from the Agent to the IBM MSS infrastructure;
   (3) verify availability and functionality of the Agent in the Portal;
   (4) perform quality assurance testing of the Agent;

b. perform Services acceptance testing;

c. remotely demonstrate the primary features of the Portal for up to ten of your personnel, for up to one hour.

Completion Criteria:

This activity will be complete when IBM has verified availability and functionality of the Agent in the Portal.

Deliverable Materials:

- None

Activity 7 - Services Activation

The purpose of this activity is to activate the Services.

IBM will:

a. assume management and support of the Agents;

b. set Agents to “active”;

c. transition Agents to the SOCs for ongoing management and support.

Completion Criteria:

This activity will be complete when the Services are activated and Agents are set to “active”.

Deliverable Materials:

- None

3.5.2 Your Deployment and Activation Responsibilities

Activity 1 - Project Kickoff

You agree to:

a. attend the project kickoff call; and

b. review each party’s respective responsibilities.

Activity 2 - Internal Scanner Agent Hardware Requirements

You agree:

a. to provide server hardware compliant with the system requirements contained in the Customer Premise ("CPE") Vulnerability Scanner Setup Instructions for any locations for which you request internal scanning;

b. and acknowledge that any hardware you provide, 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 scan engine software image; and

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

Activity 3 - Network Access Requirements for Internal Scanning

You agree to:

a. review and comply with the IBM "Network Access Requirements" document during deployment and throughout the term of the contract; and

b. be solely responsible for any charges incurred as a result of IBM utilizing a site-to-site VPN to connect to your network.

Activity 4 - Assessment

Task 1 - Gather Data

You agree to:

a. complete and return any questionnaires and/or data gathering forms to IBM within five days of your receipt;

b. obtain and provide applicable information, data, consents, decisions and approvals as required by IBM to perform the Services deployment, within two business days of IBM's request;

c. work in good faith with IBM to accurately assess your network environment;

d. provide contacts within your organisation, and specify a notification path through your organisation, in the event IBM must contact you; and

e. update IBM within three calendar days when your contact information changes.

Task 2 - Assess Environment for Internal Scanning

You agree:

a. to implement required changes to your network layout and security policies to allow scanning of desired scan targets; and

b. to situate scanning Agents in your network such that they can reach the target devices and such that firewalls and other security devices will not interfere with the scans.

Activity 5 - Implementation for Internal Scanning

Task 1 - Configure the Agent

You agree to:

a. update your hardware to meet IBM specifications;

b. download and install the IBM-provided Agent software image (i.e., physically load media as applicable);

c. configure the Agent with a public IP address and associated settings; and

d. assist IBM in exercising the existing Agent configuration and policy (if applicable).

Task 2 - Install the Agent

You agree to:

a. work with IBM in locating vendor documents that detail physical installation procedures and cabling. You will schedule such support in advance to ensure availability of an IBM deployment specialist;

b. be responsible for the physical cabling and installation of the Agent(s);

c. perform any IBM-specified adjustments to the layout of your network and security policies to allow scanning of desired scan targets; and

d. place scanning Agents in your network such that they can reach the target devices and will not allow firewalls and other security devices to interfere with the scans.

Activity 6 - Testing and Verification

You agree:

a. to be responsible for development of all of your specific acceptance testing plans;

b. to be responsible for performing acceptance testing of your applications and network connectivity; and

c. and acknowledge that additional acceptance testing performed by you, or lack thereof, does not preclude IBM from setting the Agent to "active" in the SOCs for ongoing support and management.

Activity 7 - Services Activation

You acknowledge:

a. you will use the Services to scan only IP addresses and/or Web domains that you own or have legal authority to scan; and

b. for complete and accurate scanning results, you must configure and maintain your network topology and security devices to allow unfiltered scan traffic from your scan engines to your selected scan targets.

3.6 Collection and Archival

IBM utilises the X-Force Protection System for collecting, organizing, archiving and retrieving Services scan data and reports. The Portal provides you with a 24 hours/day, 7 days/week view into the Services, including online access to scan history and reports stored within the X-Force Protection System infrastructure.

3.6.1 IBM Collection and Archival Responsibilities

IBM will:

a. collect scan data generated by Agent(s) as such data reaches the IBM MSS infrastructure;

b. collect scan data generated by IBM's external scanning infrastructure;

c. purge temporary scan logs generated by Agents and external scanners after importing scan results to the X-Force Protection System database;

d. if applicable, make results of individual PCI scans available for viewing in the Portal for two years;

e. make results of individual non-PCI scans available for viewing in the Portal for six months;

f. for individual non-PCI scans, once the initial six month period has expired, make summarised scan results available for 18 months; and

g. purge data based on the retention periods described above.

3.6.2 Your Collection and Archival Responsibilities

You agree:

a. and acknowledge that:

(1) IBM will purge temporary scan logs and individual scan results in accordance with the timeframes stated in the "IBM Collection and Archival Responsibilities" section above;

(2) notwithstanding any retention periods specified in the "IBM Collection and Archival Responsibilities" section above, if the Services are terminated or cancelled for any reason whatsoever, IBM will be relieved of its obligation to store your Services data;.

(3) all scan data will be transmitted to the SOCs via the Internet;

(4) IBM can only collect and scan data that successfully reaches the IBM MSS infrastructure; and

(5) IBM does not guarantee the legal submission of any Services data into any domestic or international legal system. Admissibility of evidence is based on the technologies involved and your ability to prove proper data handling and chain of custody for each set of data presented; and

b. to use the Portal to review scan results.

3.7 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 active VMS Services contract, IBM will monitor a specific number of Agents according to the following table.

IP Addresses		Number of Allowed Agents
From	To	
1	199	2
200	999	6
1,000	2,999	12
3,000	29,999	16
30,000+ IPs		one per 2,000 IPs

You acknowledge that if you require additional Agents, additional Agent monitoring charges will apply.

3.7.1 IBM Managed Agent Health and Availability Monitoring Responsibilities

Activity 1 - Monitoring

The purpose of this activity is to monitor the health and performance of the Agents.

Agent-Based Monitoring

IBM will install software on Agents to monitor system health and performance, and report metrics back to the SOCs.

IBM will:

a. for eligible platforms, install monitoring software on the Agents;

b. analyze and respond to key metrics, which may include:

(1) hard disk capacity;

(2) CPU utilisation;

(3) memory utilisation; and

(4) process availability; and

c. respond to alerts generated by the monitoring software.

Activity 2 - Troubleshooting

The purpose of this activity is to perform research and investigation if the Agents do not perform as expected or a potential Agent health issue is identified.

IBM will:

a. create a trouble ticket in the event of an Agent performance problem or potential Agent health issue;

b. begin research and investigation of the documented issue;

c. if the Agent is identified as the potential source of a network-related problem, examine the Agent configuration and functionality for potential issues; and

d. display the Agent health and outage ticket in the Portal.

Activity 3 - Notification

The purpose of this activity is to notify you if the Agent becomes unreachable through standard in-band means.

IBM will:

a. notify you if the Agent becomes unreachable through standard in-band means. Such notification will be via telephone using a predetermined notification procedure within the timeframe established in the section of this Services Description entitled "Service Level Agreements", "Proactive system monitoring";

b. begin investigation of problems related to the configuration or functionality of the Agent, following initiation of telephone notification; and

c. display Agent health and outage tickets in the Portal.

3.7.2 Your Managed Agent Health and Availability Monitoring Responsibilities

Activity 1 - Monitoring

No additional responsibilities are required by you for this activity.

Activity 2 - Troubleshooting

You agree:

a. to participate in troubleshooting sessions with IBM (as required);

b. to be responsible for providing all remote configuration and troubleshooting, if it has elected not to implement an out-of-band ("OOB") solution, or if the OOB solution is unavailable for any reason; and

c. and acknowledge that if the managed Agent is eliminated as the source of a given problem, no further troubleshooting will be performed by IBM.

Activity 3 - Notification

You agree to:

a. provide your notification paths and contact information;

b. update IBM within three calendar days when your contact information changes; and

c. ensure an Authorised Security Contact or Agent outage Designated Services Contact is available 24 hours/day, 7 days/week.

3.8 Agent Management

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

3.8.1 IBM Agent Management Responsibilities

IBM will:

a. be the sole provider of software-level management for the Agents;

b. maintain system status awareness;

c. install patches and software updates in order to improve performance, enable additional functionality, or resolve an application problem. IBM assumes no responsibility for, and makes no warranties concerning, vendor-provided patches, updates or security content;

d. declare a maintenance window in advance of Agent updates that may require platform downtime or your assistance to complete; and

e. clearly state, within the maintenance window notification, the expected impacts of a scheduled maintenance and your specific requirements.

3.8.2 Your Agent Management Responsibilities

You agree:

a. to perform IBM-specified hardware upgrades to support the current software and firmware;

b. to work with IBM to perform Agent updates (as required);

c. to be responsible for all charges associated with hardware upgrades;

d. to maintain current licensing, and support and maintenance contracts;

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

f. and acknowledge:

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

   (2) data traveling across the Internet is encrypted using industry-standard strong encryption algorithms whenever possible;

(3) 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;

(4) noncompliance with IBM-required software upgrades may result in suspension of Services delivery and/or SLAs; and

(5) noncompliance with IBM-required hardware upgrades may result in suspension of Services delivery and/or SLAs.

3.9 Services Reporting

Utilizing the Portal, you will have access to Services information and reporting with customisable views of assets and scan results.

3.9.1 IBM Services Reporting Responsibilities

IBM will provide you with access to reporting capabilities in the Portal which include:

a. number of SLAs invoked and met;

b. number, types, and summary of Services requests/tickets;

c. details of scans performed in a variety of predefined and customisable formats; and

d. make generated reports (PDF, CSV, XML, etc.) available for download by you from the Portal for one year from date of creation (two years for PCI reports).

3.9.2 Your Services Reporting Responsibilities

You agree to:

a. generate Services-related reports using the Portal; and

b. be responsible for scheduling reports (as applicable).

4. Optional Services

Optional services selected by you, and any additional charges for such services, will be specified in the Schedule.

4.1 Out-of-Band Access

OOB access is a highly recommended feature that assists the SOCs if connectivity to an Agent is lost. If such connectivity problems occur, the SOC analysts can dial into the modem to verify the Agent is functioning properly and assist in determining the source of the outage before escalating to you.

4.1.1 IBM Out-of-Band Access Responsibilities

At your request, for no additional charge, IBM will:

a. provide live support, via phone and e-mail, to assist you in locating applicable vendor documents which detail physical installation procedures and cabling;

b. configure the OOB device to access the managed Agents; or

c. work in good faith with you to utilise an IBM-approved existing OOB solution.

4.1.2 Your Out-of-Band Access Responsibilities

You agree:

a. for new OOB solutions:

(1) to purchase an IBM-supported OOB device;

(2) to physically install and connect the OOB device to the Agent;

(3) to provide a dedicated analog telephone line for access;

(4) to physically connect the OOB device to the dedicated telephone line and maintain the connection;

(5) to be responsible for all charges associated with the OOB device and telephone line; and

(6) to be responsible for all charges associated with the ongoing management of the OOB solution;

b. for existing OOB solutions:

(1) to ensure the solution does not allow IBM to access non-managed devices;

(2) to ensure the solution does not require installation of specialised software;

(3) to provide IBM with detailed instructions for accessing managed Agents; and

(4) to be responsible for all aspects of managing the OOB solution;

c. and acknowledge that existing OOB solutions must be approved by IBM;

d. to maintain current support and maintenance contracts for the OOB (as required); and

e. to be responsible for providing all remote configuration and troubleshooting, if you elect not to implement an OOB solution or if the OOB solution is unavailable for any reason.

4.2 PCI Approved Scanning Vendor Services

You may request that IBM act as an ASV to enable you to submit ASV-certified scan reports to your acquiring banks or payment brands.

4.2.1 IBM PCI Approved Scanning Vendor Responsibilities

At your request, for no additional charge, IBM will:

a. establish a separate environment within VMS for performing PCI scans;

b. with your input, establish sites within VMS defining the scan components (IP addresses and/or domains) that will be subject to PCI scanning;

c. as scheduled by you, perform vulnerability scans in accordance with PCI Data Security Standard ("DSS") requirement 11.2;

d. respond to PCI scope change requests (additions or deletions to previously supplied PCI scope) by:

(1) accepting an unlimited number of PCI scope change requests, via the Portal;

(2) acknowledging PCI scope change requests via the Portal within the timeframes established in the section of this Services Description entitled "Service Level Agreements", "PCI scope change request acknowledgement";

(3) reviewing PCI scope change requests to verify you have provided adequate documentation to justify the scope change;

(4) implementing PCI scope changes within the timeframes established in the section of this Services Description entitled "Service Level Agreements", "PCI Scope Change Request Implementation;

e. respond to vulnerability exception requests (for example, suspected false positives) by:

(1) accepting an unlimited number of vulnerability exception requests submitted by you via the Portal;

(2) reviewing vulnerability exception requests to verify you have 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";

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

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

Note: Your access and use of the reports provided via the 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 Portal Terms of Use shall prevail over this Services Description. In addition to the Terms of Use provided in the Portal, your 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.

4.2.2 Your PCI Approved Scanning Vendor Responsibilities

You agree:

a. to identify Portal users who are authorised to use the PCI environment within VMS;

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

(1) providing IBM with the IP addresses and/or domain names of all Internet-facing systems;;

(2) requesting any PCI scope changes via the Portal and providing complete and accurate justification for such scope changes;

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

c. to be responsible for ensuring you have the legal authority to scan IP addresses and/or Web domains in the requested PCI scope;;

d. and acknowledge that you are 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 IBM's external scanning engines);

(2) coordinating with IBM if you have 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 synchronised in terms of configuration, or

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

g. to be responsible for coordinating with your Internet service provider ("ISP") and/or hosting providers to allow completely unfiltered network traffic between IBM's external scan engines and your target network(s);

h. if you dispute scan results for a particular vulnerability, you will:,

(1) use the 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 VMS;.

(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 you to engage (at your expense) a PCI Qualified Security Assessor ("QSA") before approving certain disputes (such as proposed compensating controls);

i. to use the Portal to initiate scanning;

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

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

l. to use the Portal to request that IBM produce your quarterly PCI ASV Attestation of Scan Compliance;

m. to download completed ASV scan reports and submit them to your acquirer or payment brands, as directed by the payment brands;

n. that by downloading and submitting ASV reports to acquirers or payment brands, you attest and acknowledge that:

(1) you have not and will not change or alter the system-generated ASV reports in any way before submitting them to your acquirers or payment brands;

(2) you are 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) you have implemented network segmentation, if any components are excluded from PCI DSS scope;

(4) you have 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 (PCI DSS 11.2) and are not an indication of overall compliance with any other PCI DSS requirements.

5. Service Level Agreements

IBM SLAs establish response time objectives and countermeasures for specific events resulting from 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 you meet your obligations as defined in this Services Description and all associated contract documents.

5.1 SLA 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. Services availability – IBM will provide 100% service availability for the SOCs.

b. Portal availability – IBM will provide 99.9% accessibility for the Portal: 1) outside of the times specified in the section of the General Provisions entitled "Scheduled and Emergency Portal Maintenance"; and 2) outside of an additional standard, scheduled maintenance window on the third Saturday of every month from 8:00 a.m. – 12:00 p.m. (noon) United States Eastern Time.

c. Proactive system monitoring – IBM will notify you within 15 minutes after IBM determines your Agent is unreachable via standard in-band connectivity.

d. Scanning implementation – IBM will begin implementation of a scheduled vulnerability assessment within one hour (plus or minus one hour) of the time scheduled by you (or by IBM on your behalf) and all scans will be completed. 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.

e. PCI scope change request acknowledgement – IBM will acknowledge PCI scope change requests within two hours after such requests are submitted via the Portal.

f. PCI scope change implementation – IBM will implement PCI scope changes within 72 hours of receiving sufficient and acceptable documentation from you to justify the PCI scope change.

g. PCI vulnerability exception request response – IBM will respond with either an approval or denial of the exception request within 72 hours of receiving sufficient and acceptable documentation from you to justify the PCI vulnerability exception request.

   Note: You may submit an unlimited number of PCI vulnerability exception requests; however, only the first 15 requests submitted in a given day will be subject to this SLA. Subsequent requests (beyond the first 15 received in a given day) will be accepted but not treated as a priority, and will not be bound by this SLA.

5.2 SLA Remedies

Services availability, 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 day of the monthly VMS service charges.

SLAs and Remedies Summary

Service Level Agreements	Availability Remedies
Services availability	Credit for 1 day of the monthly Services charge
Portal availability	
Proactive system monitoring	
Scanning implementation	

PCI scope change request acknowledgement	
PCI scope change request implementation	
PCI vulnerability exception request response	

6. Other Terms and Conditions

6.1 General

You acknowledge and agree:

a. that all software provided by IBM as part of these Services is licensed, not sold. Except for the licenses specifically granted herein, all right, title, and interest in and to the software shall remain vested in IBM or its licensors;

b. that you will inform IBM in writing, at least 30 days prior to the cancellation or termination of the Services, or promptly if the license for the scanning software is terminated by IBM for any reason, whether you choose to:

   (1) have IBM remove the scanning software either remotely or by assisting you to remove the scanning software; or

   (2) retain the scanning software.

   If you choose to have the scanning software removed, you agree to cooperate with IBM by providing the remote access necessary for IBM to remove the scanning software, or by assisting IBM in removing the scanning software

c. in addition to the terms and conditions listed above, specific licensing terms will be presented for your review and acceptance both when you download and when you install the software.

6.2 Permission to Perform Testing

Certain laws prohibit any unauthorised attempt to penetrate or access computer systems. You authorise IBM to perform the Services as described herein and acknowledge that the Services constitute authorised access to your computer systems. IBM may disclose this grant of authority to a third party if deemed necessary to perform the Services.

The Services that IBM performs entail certain risks and you agree to accept all risks associated with such Services; provided, however, that this does not limit IBM's obligation to perform the Services in accordance with the terms of this SOW. You acknowledge and agree to the following:

a. excessive amounts of log messages may be generated, resulting in excessive log file disk space consumption;

b. the performance and throughput of your systems, as well as the performance and throughput of associated routers and firewalls, may be temporarily degraded;

c. some data may be changed temporarily as a result of probing vulnerabilities;

d. your computer systems may hang or crash, resulting in system failure or temporary system unavailability;

e. any service level agreement rights or remedies will be waived during any testing activity;

f. a scan may trigger alarms by intrusion detection systems;

g. some aspects of the Services may involve intercepting the traffic of the monitored network for the purpose of looking for events; and

h. new security threats are constantly evolving and no service designed to provide protection from security threats will be able to make network resources invulnerable from such security threats or ensure that such service has identified all risks, exposures and vulnerabilities. .

6.3 Systems Owned by a Third Party

For systems (which for purposes of this provision includes but is not limited to applications and IP addresses) owned by a third party that will be the subject of testing hereunder, you agree:

a. that prior to IBM initiating testing on a third party system, you will obtain a signed letter from the owner of each system authorizing IBM to provide the Services on that system, and indicating the

owner's acceptance of the conditions set forth in the section entitled “Permission to Perform Testing” and to provide IBM with a copy of such authorisation;

b. to be solely responsible for communicating any risks, exposures, and vulnerabilities identified on these systems by IBM’s remote testing to the system owner, and

c. to arrange for and facilitate the exchange of information between the system owner and IBM as deemed necessary by IBM.

You agree:

d. to inform IBM immediately whenever there is a change in ownership of any system that is the subject of the testing hereunder;

e. not to disclose the deliverable Materials, or the fact that IBM performed the Services, outside your Enterprise without IBM’s prior written consent; and

f. to indemnify IBM in full for any losses or liability IBM incurs due to third party claims arising out of your failure to comply with the requirements of this section entitled, "Systems Owned by a Third Party" and for any third party subpoenas or claims brought against IBM or IBM’s subcontractors or agents arising out of (a) testing the security risks, exposures or vulnerabilities of the systems that are the subject of testing hereunder, (b) providing the results of such testing to you, or (c) your use or disclosure of such results.

6.4 Disclaimer

You understand and agree that:

a. it is solely within your discretion to use or not use any of the information provided pursuant to the Services hereunder. Accordingly, IBM will not be liable for any actions that you take or choose not to take based on the services performed and/or deliverables provided hereunder;

b. IBM does not provide legal services or represent or warrant that the services or products IBM provides or obtains on your behalf will ensure your compliance with any particular law, including but not limited to any law relating to safety, security or privacy; and

c. it is your responsibility to engage competent legal counsel to advise you as to the identification and interpretation of any relevant laws that may affect your business and any actions needed for compliance with such laws.

6.5 Payment Card Industry Covenants

You acknowledge 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 Statement of Work.

a. You acknowledge and agree that you may be ordering Services from IBM in connection with your obligation to comply with the Payment Card Industry Data Security Standard (“PCI-DSS”). You understand 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. You acknowledge and agree that you chose IBM to provide Services from a list of approved vendors published by the PCI SSC (the “ASV List”). Further, you acknowledge 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 (“ASVs”) Version1.2”, Appendix A “PCI ASV Compliance Test Agreement” . You also acknowledge that parts of that agreement require IBM to include certain provisions in its agreements with its customers.

   (1) You understand and agree 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, you understand and agree that the PCI SSC does not require you to use IBM products or services. You also agree that for the purposes of this “Payment Card Industry Covenants” section, capitalised terms in items a. 2, 3, 4, and 5 below shall have the meanings ascribed to them in the ASV Agreement.

   (2) You understand and agree 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 you, (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. You agree 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. You consent 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 you have any confidentiality agreement with IBM; the terms of this item a.2 are incorporated into such agreement by this reference.

(3) You understand 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. You consent to IBM furnishing such reviews and reports to the PCI SSC and its Members and/or Acquirers/Issuers and also agree that you 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) You also understand that IBM has, in the ASV Agreement, upon written request by PCI SSC or any Member (each a "Requesting Organisation") agreed to provide to such Requesting Organisation such testing and assessment results (including scan reports) as such Requesting Organisation may reasonably request with respect to (i) if the Requesting Organisation 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 authorised to accept such Member's payment cards, an Acquirer of accounts of Merchants authorised 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 Organisation is PCI SSC, any Vendor Client for which ASV has performed testing or assessment. You consent 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.

b. Your Indemnity regarding Payment Card Industry Services

To the extent that IBM provides Services as an ASV, you 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.