Software Asset Management (SAM) Statement of Work (SOW) – HEALTHCARE CYBERSECURITY REVIEW

(For use with the Microsoft SAM Services Program)

1. Description

The SAM Healthcare Cybersecurity Assessment provides the customer with a foundational analysis of their cybersecurity infrastructure taking into consideration current software deployment, usage, and licensing data. The analysis will be the basis for the evaluation of the customer's basic cybersecurity state, providing insights into what software is deployed and areas of potential risk. The analysis will also provide guidance on cybersecurity programs and policies to help enable strong software asset management and improved cybersecurity.

The SAM partner collects the data and performs a full discovery and inventory outlining all Microsoft product deployments, usage, and entitlements. The partner will use third-party tools, interviews with key customer stakeholders, as well as other sources to capture all relevant data.

Use of Intelligent Asset Manager (IAM) is required in this SAM Healthcare Cybersecurity Assessment to receive Channel Incentives. All work contemplated under this Statement of Work (SOW) will be provided in accordance with the IAM Terms of Use ("TOUs"), available at http://aka.ms/IAMDATAUSAGE.

In this SAM Assessment, the ELP is optional. Components for the ELP are broken out separately in each section. The choice of including the ELP in this engagement belongs to the SAM Engagement Manager in discussions with the customer and the partner. Principally, the SAM Assessment isn't an exercise to determine a licensing gap, but rather a way to identify specific opportunities to improve the customer's asset management value, and business objectives. The ELP, as a customer-facing document, has great value to clearly articulate to the customer their current standing on entitlements compared to deployment and is often requested by the customer at the outcome of the engagement.

2. Inputs

The partner will collect the following inputs from the customer's premises:

1. The customer's IT vision and/or roadmap, including current cybersecurity concerns and plans.
2. A complete background of the customer's existing IT infrastructure and environment, including on-premises, Cloud and outsourced installations for all locations and/or divisions, an understanding of remote employee and external contractor protocols for accessing the network, and corporate network connectivity to external networks.
3. Current IT infrastructure and organization diagrams including locations, IT group names, SAM tool(s) or supporting processes in use, and stakeholder names.
4. The customer's IT policy manual related to managing cybersecurity, if one exists.
5. Deployment inventory data coverage of no less than 90% from at least one (1) automated discovery tool for each customer location where Microsoft products are installed (see Data collection requirements).

If an Effective License Position (ELP) is required:

The partner will collect the following inputs from the customer's premises:

1. Entitlement data outside Microsoft Volume License Agreements from procurement and any applicable sources or suppliers which may include:
    i. Original Equipment Manufacturer (OEM)
    ii. Full Packaged Product (FPP) / Retail
    iii. Outsourcer
    iv. Service provider (Hosters, etc.)
    v. Additional reseller(s)
    vi. Changes to entitlements resulting from mergers, acquisitions or divestitures
    vii. Independent Software Vendors (ISV)
    viii. Any servers/environments managed by a Service Provider Licensing Agreement (SPLA)
2. A full and confirmed list of affiliates, if they exist, and any relevant amendments to their Microsoft Volume License Agreements, including any license transfer documents, either granting or receiving licensing rights.
3. Location of software entitlement, deployment and retirement records as well as level of access allowed.

The partner will collect the following inputs from Microsoft:

Microsoft License Statement (MLS) including Microsoft Product and Services Agreement (MPSA) data where relevant.

3. Data collection

This section lists steps partners must take to build the foundation for the required analysis and customer deliverables. Partners will ensure that all data collected will be stored securely and in accordance with the requirements set out in the IAM TOUs. The main category of data collection is data related to the Cybersecurity assessment, optimization, and recommendations. Partners must ensure that the data collected is complete and accurate. Any deviation or change to this scope needs to be approved by Microsoft, the partner, and the customer.

Discovery and inventory of hardware and software assets: data collection requirements

Data coverage must reach at least 90% of all devices pertaining to this engagement. Data coverage is defined as the percentage of total devices for which all required installation data has been obtained. Where devices are not joined to the directory or network, manual collection of data is acceptable while maintaining the 90% data coverage requirement. Some specific guidance includes, but is not limited to:

1. Complete extraction of user accounts from the customer's Active Directory (AD) domain(s) and Lightweight Directory Access Protocol (LDAP) and/or workgroups.
2. Data extract must be cross-referenced against a minimum of one (1) additional data source, including but not limited to:

    i. Records from existing network performance/security monitoring and management tools
    ii. Network management frameworks
    iii. Virtual machine performance monitoring
    iv. Security sources (anti-virus)
3. All trust accounts must be extracted to ensure no domains are missed.
4. Extraction of user accounts by group (if applicable, e.g., for Citrix). Output includes a listing of user objects and the AD Groups they belong to.
5. Identification of active users in the past 90 days based upon the technique(s) employed by the customer (based on output from Step 1).
6. Complete extraction of data from the customer's current management and inventory tools and the calculation of current coverage levels of existing tool(s).
7. Inventory of any missing device, including but not limited to devices that:
    i. Do not report inventory
    ii. Are non-networked
    iii. Are unmanaged devices

Cybersecurity Assessment: data collection requirements

Through data discovery, make sure to identify:

i. Versions and editions of all Microsoft products discovered
ii. Windows Update availability on all machines (if using SCCM or other tool that captures this information as part of discovery process)
iii. Presence of System Center Endpoint Protection or other anti-virus software on machines (if using SCCM or other tool that captures this information as part of discovery process)
iv. Firewall software on machines (if using SCCM or other tool that captures this information as part of discovery process)
v. SQL Server Service Pack Deviation information
vi. Windows Server Service Pack Deviation information
vii. User password setting information from AD
viii. Operation system activations
ix. Browser version
x. Enterprise Mobility and Security (EMS)

If an ELP is required:

This section lists steps partners must take to complete the ELP. Some specific guidance includes, but is not limited to:

1. Virtual environment mapping output includes:
    i. Clusters
    ii. Physical hosts
    iii. Virtual guests and virtual guest movement across physical hosts within the past 90 days to accurately calculate licensing needs for products such as Windows Server, SQL Server, etc.
2. Identification of workstations and servers used by Microsoft Developer Network (MSDN®) subscribers. Products installed on these devices will be identified and excluded if appropriate. Facilitation of the identification of devices covered by MSDN® subscriptions by employing

various methods such as determining preferred user for devices, linking last logged-on user to devices, or soliciting feedback from customer personnel that have a MSDN® subscription (email template can be provided.) **This step should be completed as early as possible in the data collection phase.**

3. For server products that can be licensed in multiple ways (e.g., server/CAL or per processor), the licensing metric applicable to each implementation must be identified.
4. SQL Server output includes:
    1. Version and edition
    2. License type required for each SQL Server instance for customers with mixed licensing metric (server/CAL or per processor or per core)
    3. Confirm passive SQL Servers assigned Failover Rights
5. Windows Server output includes:
    i. Server name
    ii. Physical or virtual operating system environment
    iii. Operating system version and edition
    iv. Processor and core information
6. System Center Server output includes:
    i. Server names
    ii. Physical or virtual data
    iii. Component e.g. SCCM, SCVM version and edition
    iv. Processor and core information

4. Analysis

The SAM Healthcare Cybersecurity Assessment data must be analyzed, reviewed, and agreed upon with the customer as an accurate point-in-time reflection of the customer's current deployment and license position. This data, along with the additional customer inputs, will also provide a basis for the development of a solid Cybersecurity Assessment unique to the customer. Based on the inputs and data collection, the partner will complete the following required analysis:

1. Reconciliation analysis between license entitlements and deployment data, including the application of license benefit and optimization rules (e.g. upgrades, downgrades, promotions, etc.).
2. Aggregation and review of data from stakeholder interviews, noting any information that was either unavailable or challenging for the customer to gather.
3. Assess the customer cybersecurity maturity, specifically related to asset management policies and procedures.
4. Review customer's current IT environment mapped to an optimized environment based on customer's cybersecurity goals, including assessment of outdated product versions and editions, patch management policies and practices, and more.

5. Deliverables

The following deliverable is **due to the customer** at the **beginning** of the engagement:

Letter of Engagement. This letter must include at a minimum:

i. A Statement of Work (SOW) for the engagement being performed, including a list of all customer deliverables
ii. Scope of the engagement, including any scope limitations
iii. Dates and timelines
iv. Partner project team members and their relevant Microsoft Certified Professional (MCP) credentials
v. List of key contacts that must include names, titles, phone number, and email addresses
vi. Planned disclosure of engagement deliverables to Microsoft
vii. Statement explaining that data collected by partners from customer's information system environment is transferred to Microsoft, and how Microsoft will use that data collected to generate reports necessary for partners to effectuate the SAM services.
viii. Consent from the customer to transfer data to Microsoft, any of its affiliates, and to the subprocessors Microsoft may employ to generate the reports necessary for the SAM services, including consent to transfer Personal Information to the United States and other countries where Microsoft's subprocessors are located. "Personal Information" means any information provided by Microsoft or collected by partner in connection with this Agreement (a) that identifies or can be used to identify, contact, or locate the person to whom such information pertains, or (b) from which identification or contact information of an individual person can be derived. Personal Information includes, but is not limited to: name, address, phone number, fax number, and email address.

    Additionally, to the extent any other information (such as, but not necessarily limited to, a personal profile, unique identifier, and/or IP address) is associated or combined with Personal Information, then such information also will be considered Personal Information.

    For more information reference the IAM TOUs.

The Letter of Engagement must be in writing and signed by authorized representatives of the partner and customer.

The following deliverables are **due to the customer** at the **end** of the engagement:

1. Healthcare Cybersecurity Assessment Report. This report must contain at a minimum:
    i. An Executive Summary. A high-level summary of project background and scope, engagement result, recommendations and next steps.
    ii. An assessment of the customer's overall cybersecurity state, in relation to their current IT infrastructure.
        b. SQL Server Service Pack deviations
        c. Windows Server Service Pack deviations
        d. Mainstream/Extended support analysis – Operating system and Microsoft software
        e. Anti-virus software /Anti- malware running in environment
        f. User account status
        g. Password controls and last login dates

        h. Stale domains and data sources
    iii. A cybersecurity roadmap based on a maturity model using the Cybersecurity Framework (CSF) v1.0 published by the National Institute of Standards and Technology (NIST) to assist the customer in better protecting their IT assets, including all business, licensing, and technology guidance.
    iv. An assessment of customer's cybersecurity-related SAM policies and procedures strengths, weaknesses, and areas of opportunity, including recommendations for improvement.
    v. Advice on how to engage with a local cybersecurity professional, if needed, and a list of additional resources on cybersecurity.
    vi. Additional Uses of Data. In this section of the report, the partner provides specific cybersecurity related findings. Examples of information that can be included in this report are:
        a. A summary of current or upcoming end-of-life products, with upgrade path recommendations
2. Established Deployment Position (EDP). A document with details related to all hardware and software currently deployed within the customer's IT infrastructure.

If an ELP is required:

1. The Effective License Position. A spreadsheet that provides details related to license entitlements and deployments. The spreadsheet must be produced using IAM (Note: Defined in Deliverables to Microsoft).
2. License Optimization Report. This report must contain the risks, liabilities, and issues associated with customer's current licensing practices and prioritized recommendations on how to better manage their licenses to minimize risks in the future. The report could also contain, but is not limited to:
    i. Identification of all of the customer's Volume License Agreements (VLAs) with Microsoft and a recommendation on any beneficial consolidation.
    ii. Consumption information, detailing installed products that are unused or underutilized (e.g., no use in last six months).
    iii. Recommendations for a repeatable, simplified inventory collection process for future True-ups (for Enterprise Agreement customers only).
    iv. Additional customer-specific recommendations based on captured data and insights.

The following deliverables are due to Microsoft as necessary Proof of Execution (POE) in order for the partner to collect Channel Incentives payment.

The SAM partner must notify the Microsoft SAM Engagement Manager when the POE is uploaded into the required system as designated by Microsoft (currently, CHIP). POE includes the following deliverables due to Microsoft upon the completion of the SAM Engagement and must be provided as necessary POE for the partner to collect Channel Incentives payment:

1. Letter of Engagement. This must be the same Letter of Engagement provided to the customer and signed by the customer and the partner **at the beginning of the engagement.**
2. Established Deployment Position (EDP). The EDP, an IAM generated Excel report, provides details related to the customers' Microsoft software deployments and usage data. The software

deployments are identified using discovery tools and manual inputs as outlined in the Data collection section. The partner must first input all relevant data into the customer Inventory Data Contract (CIDC) template, which will be uploaded into IAM. The EDP will then be created by the partner using IAM which is to be given to the customer and Microsoft. EDPs produced outside of IAM will not be accepted as proof of execution. The EDP data must meet or exceed the minimum quality standards published in the current SAM Minimum EDP Quality Standards.

3. Cybersecurity Assessment Report. This must be the same Cybersecurity Assessment Report provided to the customer, as outlined above.
4. Letter of Confirmation (China only)
   The Letter of Confirmation should be drafted after completion of the SAM engagement and requires customer's chop (stamp) or email from customer corporate domain confirming provision of SAM engagement.

   The Letter of Confirmation must include the following statement:

   "This is to confirm Microsoft SAM partner <insert partner Name> has implemented SAM service <insert SAM Engagement Type> to customer <insert customer name>."

If an ELP is required:

1. Effective License Position. The ELP provides details related to license entitlements and deployments and is generated using I-AM. The ELP must be finalized in I-AM. ELPs produced outside of I-AM will not be accepted. An encrypted ELP must be uploaded into the designated tool (currently CHIP) as proof of execution.

6. SAM resources

SAM partner eligibility, program overview, and partner incentive guides are located at http://aka.ms/SAMIncentiveGuide