SAM

SOFTWARE ASSET MANAGEMENT

SAM Cybersecurity

Engagement Kit

Microsoft

Table of Contents

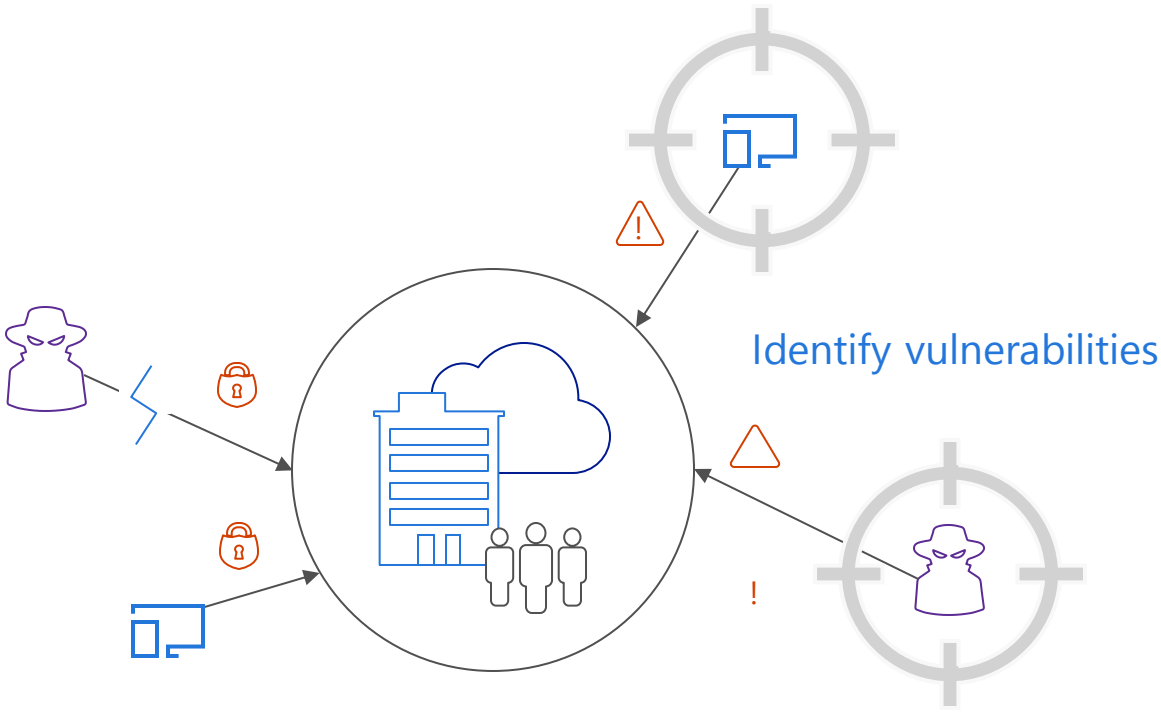
How to use this document

Getting started

The SAM Cybersecurity Engagement Kit walks you through the complete cycle of an engagement. The kit begins with a general introduction describing what a Cybersecurity engagement is and the stages involved to complete one. The rest of the kit focuses on how to proceed with each stage. This includes which deliverables represent billable milestones at the end of each stage. At the end of the kit, within the Appendix, you will find additional information to help you with the engagement process as well as links to resources that offer useful information and details.

Prerequisites

Partners that participate in a SAM engagement must be a registered SAM Gold Partner, or must have earned the SAM Solution Expertise criteria.



Cybersecurity

Introduction

SAM

SOFTWARE ASSET MANAGEMENT

Cyberattacks cost businesses around the world upwards of $400B annually.[1] Research estimates that number could climb to $2.1T by 2019.[2] Between apps being downloaded without approval, unmanaged devices being used within the corporate network, poor password protection programs, and more, too many businesses leave themselves vulnerable to attack. What they need is a clear understanding, visibility, and control of their IT infrastructure.

70% of major multi-national corporations will face significant cybersecurity attacks by 2019.

IDC 2017

Microsoft SAM Cybersecurity engagement

A Software Asset Management (SAM) Cybersecurity engagement provides customers with a comprehensive analysis of their cybersecurity infrastructure, including their current software deployment, usage, and licensing data. They receive a full inventory that they can use as the foundation for a more in-depth organizational security assessment. You gain the opportunity to help them improve their cybersecurity program and address any licensing issues identified with the engagement. This opens the door to a potentially larger opportunity.

Minimizing cyber risks helps organizations decrease costs from data loss, fraud associated with theft, loss in revenue, support, employee downtime, cost to locate and reinstall lost data, and a negative reputation. In addition, you can develop a long-term trusted advisor relationship with your customers by establishing credibility and demonstrating customer-focused problem-solving. You also increase customer satisfaction by helping your customers solve critical business challenges.

The engagement requires you to collect data and perform a full discovery and inventory outlining all Microsoft product deployments, usage, and entitlements using third-party tools, interviews with key customer stakeholders, and other sources to capture all relevant data.

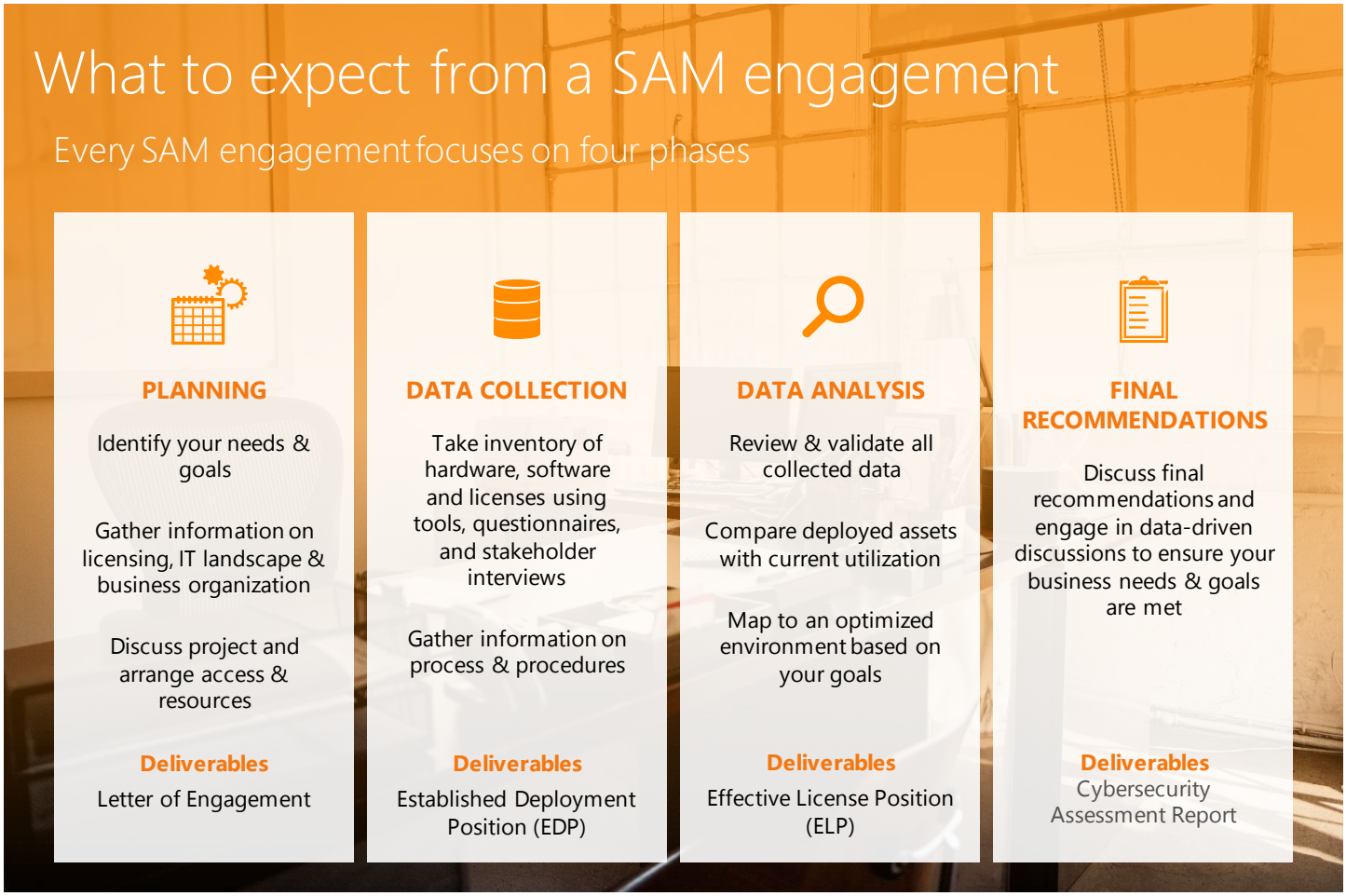
Partner benefits

- Minimize data loss, fraud, and employee downtime
- Save money combatting cyberattacks and increasing efficiencies
- Securely manage software assets and promote reliable cybersecurity practices
- Build a resilient IT infrastructure that can quickly respond to threats
- Ensure that you have a secure and effective defense against attacks

[1]Stephanie Gandel, "Lloyd's CEO: Cyber attacks cost companies $400 billion every year," http://fortune.com/, (January 23, 2015)
[2]Steve Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019," http://www.forbes.com/, (January 17, 2016)

Cybersecurity

Introduction



SAM Services Incentive Program

SAM Cybersecurity engagements are funded under the SAM Services Incentive Program, a worldwide offering designed to help Microsoft partners, such as you, increase customer adoption of SAM best practices. By participating in the program, you can engage with new customers or deepen existing relationships that can lead to new sales and opportunities.

It's required that you use Intelligent Asset Manager (I-AM) in this SAM Cybersecurity engagement to receive Channel Incentives. All work completed under this Statement of Work (SOW) will be provided in accordance with the I-AM Terms of Use ("TOU"), available here.

Please note that in this SAM Value engagement, the ELP deliverable is optional. You'll see components for the ELP broken out separately in each section of this kit. The choice of including the ELP belongs to the SAM engagement manager in discussions with the customer and you. Principally, the SAM Value engagement isn't an exercise to determine a licensing gap, but rather a way to identify specific opportunities to improve the customer's assets, 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.

For Proof of Execution (PoE), you must include the following deliverables), due to Microsoft, upon the completion of the SAM engagement. These materials serve as necessary PoE in order for you to collect Channel Incentives payment.

- Letter of Engagement
- Established Deployment Position (EDP)
- Cybersecurity Assessment Report
- Letter of Confirmation (only required for certain countries)
- Effective License Position (ELP) (optional)

How to file for a SAM Services Incentive Program

To learn how to file a SAM Services Incentive Program, visit Software Asset Management.

Additional support

After conducting a SAM Cybersecurity engagement, it may become apparent that the customer needs to conduct a more thorough overall cybersecurity assessment or line up additional help in resolving any uncovered issues. If this support is outside the boundaries of your business model, be aware of additional available resources, which you can recommend to help your customer. Some examples include:

Microsoft Consulting Services – Security Risk Assessment	• Datasheet • www.microsoft.com/microsoftservices • Contact your local Microsoft office for more information on local MCS services that are available.
Peer-to-peer networking through the International Association of Microsoft Channel Partners (IAMCP)	http://www.iamcp.org/

Additionally, if you would like to look into taking on new Microsoft Partner Network competencies to add to the services you provide, visit the Microsoft Partner Portal.

Cybersecurity

Step 1: Planning

SAM

SOFTWARE ASSET MANAGEMENT

A SAM engagement helps customers identify which licenses and software installations offer what level of security and features, develop a strategic plan for security and compliance, and ensure the right policies and procedures are put in place to effectively manage the implementation and minimize risk.

The first stage of such an engagement focuses on planning. Within this stage, you will achieve the following:

- **Identify customer needs and goals**
- **Gather information about customer environment**
- **Discuss and share security resources**
- **Discuss project and arrange access and resources**

Identify customer needs and goals

Discussing if, when, why, and what the customer wants to do about security will give you a better idea of how to deliver a Cybersecurity engagement. Goals and objectives inform how you define scope and configure your inventory tool to get the necessary information required to help identify technical readiness.

Here are some questions to consider to identify customer goals and objectives:

- **What are their objectives from the engagement?**
- **What is their vision for incorporating a new security strategy?**
- **What security solutions are they considering?**
- **What do they hope to achieve with an engagement?**
- **What is their timeline?**

Gather information about customer environment

In your first meeting with a customer, look to scope the company, culture, licensing, and IT landscape to gain a better understanding of the customer's environment and needs.

You should collect the following inputs from the customer's premises :

- The customer's IT vision and/or roadmap, including current cybersecurity concerns and plans.
- A complete background of the customer's existing IT infrastructure and environment, including on-premise, 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.
- Current IT infrastructure and organization diagrams including locations, IT group names, SAM tool(s) or supporting processes in use, and stakeholder names.
- The customer's IT policy manual related to managing cybersecurity (if one exists).
- 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: (an ELP provides details related to license entitlements and deployments and is generated using I-AM). An ELP requires you to collect the following inputs from the customer's premises:

- Entitlement data outside Microsoft Volume License Agreements from procurement and any applicable sources or suppliers which may include:
  - Original Equipment Manufacturer (OEM)
  - Full Packaged Product (FPP) / Retail
  - Outsourcer
  - Service provider (Hosters, etc.)
  - Additional reseller(s)
  - Changes to entitlements resulting from mergers, acquisitions or divestitures
  - Independent Software Vendors (ISV)
  - Any servers/environments managed by a Service Provider Licensing Agreement (SPLA)
- 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.
- 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.

Each organization has its own way of collecting and managing information. It is helpful to understand the customer's approach to gain a better understanding of the maturity of their cybersecurity processes. You can use the table below to help identify what data is tracked, what tool is used for tracking, how regularly the tool is run, and if policies are in place to manage the risk from a cybersecurity perspective.

Data type	Is data tracked?		What tool is used?	How often?	Are policies in place to manage risk?
	Yes	No			
People					
Assets					
Media					
Infrastructure					
Data and information					

When done, talk about additional security processes the customer has in place. See if their current processes match their organizational goals.

Typical questions you can ask are:

- Does your organization employ firewalls at each location?
- Do users have administrative rights on their workstations?
- Do you have a policy for deploying patches and updates to your PCs?
- Can users access the internet, and if so, are there restrictions on what they can download?
- What configuration management processes, such as passwords, are in place and how strong are they?

Discuss and share security resources

Promoting threat awareness can help you lay the groundwork for the engagement by pointing out current environmental risks and explaining how a SAM Cybersecurity engagement can help your customers protect their organization, software, and people.

One valuable resource you can share with your customers is the **Microsoft Security Intelligence Report (SIR).** This report offers the following features:

- Analyzes the threat landscape of exploits, vulnerabilities, and malware using data from Internet services and over 600 million computers worldwide
- Provides the most up-to-date information on exploitation trends as well as worldwide and regional threats

The SIR Volume 16 Key Findings provides a summary of the full report.

Visit www.microsoft.com/security/sir for the most current edition and for access to a Regional Threat Map, featured articles on security, and additional resources for managing risk.

Building the SAM Cybersecurity engagement around a well-known framework is important. The 20 Critical Security Controls framework offers one of the best examples. The Council on Cybersecurity, an independent, global non-profit entity committed to a secure and open Internet, is responsible for the stewardship and sustainment of the framework. Use this framework, or a similar one, to help promote the adoption of cybersecurity best practices by your customers.

When implemented, the CSC 20 should cover **80% or more** of the cyber threats that customers face today, and increasing the efficiency of each control increases the success rate of the defenses in the environment.

Discuss project and arrange access and resources

Based on the preliminary information you've gathered, you can create a full SOW. This plan will contain an outline for data collection and analysis, a detailed list of deliverables, and a timeline with deadlines. This establishes a customer's expectations and your accountability.

Deliverables

A Letter of Engagement is due to the customer and Microsoft at the beginning of the engagement. This letter provides the necessary Proof of Execution (PoE) in order for you to collect Channel Incentives payment.

The letter must include at a minimum:

- A SOW for the engagement being performed, including a list of all customer deliverables
- Scope of the engagement, including any scope limitations
- Dates and timelines
- Your project team members and their relevant Microsoft Certified Professional (MCP) credentials
- A list of key contacts that must include names, titles, phone numbers, and email addresses
- A planned disclosure of engagement deliverables to Microsoft
- A statement explaining that data collected by you from the customer's information system environment is transferred to Microsoft, and how Microsoft will use that data collected to generate reports necessary for you to effectuate the SAM services
- 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" in this instance means any information provided by Microsoft or collected by you in connection with this Agreement that (a) 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.
- The Microsoft SAM Engagement data usage and privacy information document (i.e. Data Usage Guide).
- Reference to the Data Usage Guide, where appropriate.

The Letter of Engagement must be in writing and signed by an authorized representative of your organization and the customer.

You also must notify the Microsoft SAM Engagement Manager when the Letter of Engagement is uploaded into the required system as designated by Microsoft (currently, CHIP).

Letter of Engagement	Explains what to expect during your SAM engagement.

View sample report here.

Cybersecurity

Step 2: Data collection

SAM

SOFTWARE ASSET MANAGEMENT

The objective of data collection is to develop a profile of the customer's current Microsoft software in their environment for analysis. Within this discovery stage, you'll take inventory of the customer's IT assets and licensing.

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 I-AM 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.

Take inventory of IT assets and licensing

You need to prepare for taking a full inventory of hardware and software deployments and licensing. This assessment includes how the technology is being used, and by whom. You can accomplish this through inventory tools, questionnaires, and stakeholder interviews. Before you can move forward however, you must first work with the customer to establish the following parameters:

- **Data collection requirements**
- **Choosing the right tool**
- **Scope inventory**
- **Implementing the inventory tool**
- **Points to keep in mind during inventory**
- **Mobile device security**

Data collection requirements

Data coverage means the percentage of total devices for which all required installation data has been obtained. Data coverage must reach at least 90% of all devices pertaining to this engagement. Where devices aren't 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:

- Complete extraction of user accounts from customer Active Directory (AD) domain(s) and Lightweight Directory Access Protocol (LDAP) and/or work
- Data extract must be cross-referenced against a minimum of one (1) additional data source, including but not limited to:
    - Records from existing network performance/security monitoring and management tools
    - Network management frameworks
    - Virtual machine performance monitoring
    - Customer Human Resources (HR) records
    - Security sources (anti-virus)
- All trust accounts must be extracted to ensure no domains are missed
- 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.

- Identification of active users in the past 90 days based upon the technique(s) employed by the customer (based on output from Step 1).
- Complete extraction of data from the customer's current management and inventory tools and the calculation of current coverage levels of existing tool(s).
- Inventory of any missing device, including but not limited to devices that:
  - Do not report inventory
  - Are non-networked
  - Are unmanaged device

Cybersecurity Assessment

Through data discovery, make sure to identify:

- Versions and editions of all Microsoft products discovered
- Windows Update availability on all machines (if using SCCM or other tool that captures this information as part of discovery process)
- 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)
- Firewall software on machines (if using SCCM or other tool that captures this information as part of discovery process)
- SQL Server Deviation Pack information
- Windows Server Deviation Pack information
- User password setting information from AD
- Operation system activations
- Browser version
- Enterprise Mobility and Security (EMS)

If an ELP is required

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

- Virtual environment mapping output including:
  - Clusters
  - Physical host(s) including processor and core information
  - 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.
- Identification of workstations and servers used by Microsoft Developer Network (MSDN®) subscribers and products installed on these devices and exclusions if appropriate. To facilitate the identification of devices covered by MSDN subscriptions, you can employ various methods such as determining preferred user for devices, linking last logged-on user to devices, or soliciting feedback from customer personnel that have an MSDN subscription (email template can be provided). This step should be completed as early as possible in the Data Collection phase.
- For server products that can be licensed in multiple ways (e.g., server/CAL or per processor or per core), the licensing metric applicable to each implementation must be identified.

- SQL Server output including:
  - Version and edition
  - License type required for each SQL Server instance for customers with mixed licensing metric (server/CAL, per processor or per core)
  - Confirmation of passive SQL Servers assigned Failover Rights
- Windows Server output includes:
  - Server name
  - Physical or virtual operating system environment
  - Operating system version and edition
  - Processor and core information
- System Center Server output includes:
  - Server name
  - Physical or virtual data
  - Component (e.g. System Center Configuration Manager (SCCM), System Center Virtual Machine Manager (SCVMM) version and edition)
  - Processor and core information

Choosing the right tool

With the right inventory tool, you can collect a wide range of data points including software versions, on-premises software usage, and an analysis of applications or services running in the Cloud. When choosing an inventory tool, keep in mind that each tool supplier has its own process framework. Tools don't all function the same way. Using multiple tools helps discover and analyze the data and provide a more robust view of a customer's environment. While in some cases the customer may already have an inventory tracking system, other tools may be able to augment the types of data that the customer's tool collects.

Some considerations to keep in mind when choosing or recommending an inventory tool:

- What inventory tools are already deployed within the organization? What scope of the environment do they cover? What data points are they capable of capturing and reporting?
- Will deploying an agent-less or agent-based tool be more effective?
- What are the strengths and weaknesses of the tools being considered? Will one or more of the tools collect all required data points—hardware, software, virtualization details across a variety of hypervisors (Hyper-V, VMware® and XenServer®, for example).
- Is it optimal to deploy and monitor a tool remotely or on-premises?
- How will the tool gather data from PCs, servers, and mobile devices that connect to the network remotely?
- If using an inventory tool that the customer already has in place, make sure it's configured correctly and can scan the full IT environment.
- Consider how the tool is licensed. The optimal tool will collect the right data and align with the customer's budget, whether the tool requires a license or subscription or is free.

Scope of inventory

For any SAM engagement, collecting all relevant inventory and licensing data across all Windows-based computers in the environment is a standard best practice. For Cybersecurity engagements, it is important to consider the minimum requirements based on customer goals.

Here is where you can conduct the CSC 20 security assessment. It is a good idea to review the CSC 20 list prior to beginning so you are familiar with what it covers since it begins with an inventory exercise covering hardware and software. The CSC 20 also provides guidance on the asset management aspect of cybersecurity.

Implementing the inventory tool

The standard approach for deploying an inventory tool for a Cybersecurity engagement includes:

- Define the scope of machines to be inventoried. The recommended scope would include servers and clients.
- Determine the scope of active devices that contain data to be collected. For customers running Active Directory Domain Services (or Directories in the case of multiple, separate domains/forests), include in scope all machines with Active Directory activity reported in the last 30 days (time frame can be adjusted according to customer circumstances).
- Prepare the environment for scanning and data collection. Attain a scan coverage of greater than 90 percent of the devices in the scope, using either a combination of available tools or iterative scans to continually increase coverage rates.
- Determine what additional data source can be used as the secondary data set to compare license counts. This is a standard SAM best practice and is important to validate licensing data gathered by the inventory tool. If user counts for the secondary data set vary significantly from the server and client counts, then a problem most likely exists. This is also useful in identifying any ghost servers or clients.

Agent-less tools

- Understand domain, network, firewall, and other considerations that will affect a tool's ability to access various portions of a customer's environment.
- Open firewalls, make firewall exceptions, deploy Group Policy Objects, open specific ports, and take other steps to ensure that the tool can access all targeted machines.
- Run agent-less tools multiple times, especially at different times of the day and days of the week, to catch the variety of users, shifts, time zones, and such.

Agent-based tools

- Ensure agents are communicating regularly so that data is fresh.
- Ensure agents are deployed to the scope of target machines.
- With the right refresh schedule and agent coverage, data collection from an agent-based tool should be a single snapshot extraction with no iterations necessary.
- Ensure data cleanliness. The quality of the scan coverage is a top priority, beginning with Active Directory Domain Services.

- Consider running third-party tools in addition to customer-provided tools to achieve proper cleansing.
- As a best practice, work with the customer to ensure there is a repeatable cleansing process in place going forward.

Points to keep in mind during inventory

- Data protection laws differ by locale/country. For example, if you are inventorying client PCs, and access to a particular machine is open to someone in another country, know what data laws come into play. Data protection is of paramount importance since data breaches typically occur around non-encrypted data.
    - Will data be sent offsite to a third party for review? If so, how is the data encrypted?
    - Does the tool encrypt? If not, are processes in place to ensure this? A number of tools will package and encrypt data. If using a tool that doesn't, protocols need to be put in place to ensure equivalent protection.
    - If data is transferred by USB or CD, what is the protocol?
- Data type is critical - licensing models that are user-based can introduce a cyberthreat because the data could include user name and other privacy details. In addition, access to some data types could be in breach of locale/country privacy laws. Be aware of any legal limitations around data to help protect yourself and your customer.
- Public-facing servers: Be sure public-facing servers, which is a server that can be accessed from the internet as opposed to one on a company's internal intranet, located outside the firewall are inventoried since they can introduce another risk opportunity.
    - Verify if all public-facing servers are in a de-militarized zone (DMZ). A DMZ is a separate network used for placing web servers, e-mail servers, FTP servers and other public servers to gain access from or to the internet.
    - Identify all open ports or other access points in these servers that tie back to the corporate network behind the firewall.
    - As a best practice, it is recommended that the number of these connections be kept to a minimum to reduce threat opportunities. Existing ports should be vetted - ask if each one is absolutely necessary and recommend that policies around opening future ports should be established going forward.
- It is not unusual for organizations to only track a percentage of their environment. If, for example, the customers only tracks 70% of their environment, the missing 30% can pose a significant security risk. It may not be possible in all cases to track 100% of an environment, but it is recommended that a minimum of 90% is tracked on a regular basis. Benchmark anti-virus reports against Active Directory and inventory data.
- If gaps are identified in this analysis, they should be flagged and forwarded to the appropriate departmental owner for review so processes can be put in place to resolve why the gap occurred in the first place. Supply the customer with any insights you have gained about the health and management of Active Directory through your analysis.

1) Inventory reports	If multiple inventory tools were used, combine into one report to make it easier to compare against Active Directory and anti-virus reports.
2) Active Directory	AD is a primary layer of asset management from a cybersecurity perspective. Query AD to define the scope of active users and clients to compare against inventory reports. AD data can identify trends that are not always apparent from inventory report data.
3) Anti-virus	Information extracted from an anti-virus tool is the third data set to be collected since it will give the most accurate list of the assets which should be reported in the environment. One method to collect this data is to ask the customer to supply it by giving them a simple Microsoft Excel worksheet where they can record basic information such as asset name, user, and when the last update occurred. An additional benefit to this approach is that you will get a good indication of how well the customer currently manages their environment based upon their ability to deliver the data or not.

Mobile device security

HR employee records are a valuable secondary source for active user counts. They can also be leveraged to help identify remote workers or those in mobile roles. There is an increased likelihood that BYOD devices accessing corporate networks may not have full security precautions in place - either from remote employees or employees bringing their own devices into the office.

Here are some questions to ask:

- How is data protection functionality instituted for corporate-owned mobile devices?
- Are data protections in place for BYOD devices and if so, what are they? Are current protections sufficient to meet the organization's risk tolerance level?

Tracking mobile devices is an essential part of securing an organization's environment. Once mobile assets are identified, work with the customer to ensure the right policies and processes are in place so they can manage how organizational assets are accessed.

See the Mobile Device Management SAM Engagement Kit for more information.

Deliverables

At the conclusion of this stage, you'll create a set of reports that summarize your findings including the following:

EDP (required)	Provides details related to all hardware and software currently deployed within the customer's IT infrastructure.

View sample report here.

The customer will have time to review and validate the preliminary reports and make final adjustments.

Cybersecurity

Step 3: Data analysis

SAM

SOFTWARE ASSET MANAGEMENT

The Cybersecurity SAM engagement 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:

- Reconciliation analysis between license entitlements and deployment data, including the application of license benefit and optimization rules (e.g. upgrades, downgrades, promotions, etc.).
- Aggregation and review of data from stakeholder interviews, noting any information that was either unavailable or challenging for the customer to gather.
- Assessment of the customer cybersecurity maturity, specifically related to asset management policies and procedures.
- 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.

This third stage of a SAM engagement focuses on achieving the following:

- **Review & validate all collected data**
- **Interpret inventory data**

Review and validate all collected data

A SAM engagement helps identify and document all product deployments, usage, and license entitlements. This includes combining the inventory data with other relevant data and information that may not be discoverable with most tools such as infrastructure that has reached end of support.

If an ELP is required:

This section lists steps you must take to complete the ELP. This includes comparing deployed assets to entitlements.

One key benefit of a SAM engagement is that it gives you a clear picture of a customer's entire IT landscape, which you can then share with them. This includes an accurate view of all of a customer's license entitlements. By understanding these entitlements, you can help customers identify over-licensed and under-licensed software so they can purchase any necessary additions to bridge licensing gaps. The SAM Cybersecurity engagement will also help to identify any license gaps eligible to be right-licensed while moving to the Cloud. This helps ensure that the customer is getting credit for everything they own.

In addition, the engagement helps highlight ways in which a subscription model can impact budgeting and procurement, taking into account direct, indirect, and hidden costs. Discussions around a customer's current licensing program and future needs will also help to identify the optimal Volume Licensing choices going forward.

Recommended areas of analysis for optimization include the following:

- **Assess** whether the customer's appropriately licensed for their current deployment and usage state. We can then provide recommendations for the best licensing options to align with their future business plans.
- **Analyze** the customer's SAM process and provide recommendations to develop or improve them in support of ongoing optimization, management, and compliance.
- **Determine** whether systems are ready for the Cloud in their current configurations by identifying the Windows operating system
- **Size the systems** being assessed to understand system utilization and anticipated resource needs in Virtual Machines. This requires collecting performance metrics, not simply a single scan of how a machine is running at a single point in time.
- **Look for areas of potential risk** pertaining to running older software that is out of date or past end of support. In particular, try and track the following information:
  - **Devices not running updated software**
  - **Devices running Windows XP**
  - **Devices running Windows Server 2008**

Recommended metrics include the following:

- Virtual Machine size
- Estimated monthly usage
- Network use (GB)
- Storage use (GB)
- CPU utilization (%)
- Memory utilization (MB)
- Disk I/O utilization (I/O operations per second)
- Network utilization—in/out (MB)

Interpret inventory data

- When reviewing the inventory tool output, look for anomalies such as client count results differing greatly from the number of employees. Question anything that seems unusual to ensure your analysis is an accurate representation of the customer's environment.
- Make sure you understand the relationships between on-premises systems (such as an employee database) and Cloud systems (such as payroll).
- Be aware that inventory data for Cloud computing may be accessed, delivered, and managed differently than data for on-premises solutions. Data from the inventory tool should be combined with data from other sources (IT service management and finance, for example) so informed decisions can be made that reflect all aspects of security, including the impact on total cost of ownership and return on investment.
- Let the customer know who is managing what in order to inventory assets properly. If the organization is using a service provider, clarify what was purchased and who is managing it.

Deliverables

Upon completion of this stage, you can offer key best practices to improve the customer's software asset management program going forward.

Optional:

ELP	Provides details related to license entitlements and deployments.
License Optimization Report (required with an ELP)	Presents recommendations on how to optimize your infrastructure and improve licensing efficiencies.

View sample report here.

Cybersecurity

Step 4: Final recommendations

SAM

SOFTWARE ASSET MANAGEMENT

Final results

At the conclusion of the SAM engagement, we sit down with the customer and go over a detailed set of reports that provide the following information:

- **Recommendations**
- **Governance fundamentals**
- **Next steps**

Recommendations

Recommendations cover a wide variety of topics. In general, you sit down with your customer and go over opportunities to modernize their infrastructure, with a specific focus on recommendations around security. An organization's ability to make the right business decision about security and compliance increases greatly with a clear understanding of its current IT environment.

A second area concerns providing ways for them to best manage their IT assets to help reduce waste, avoid unnecessary costs and business risks, and streamline the entire organization.

Governance fundamentals

Talk with your customers about the standard actions they should be taking to decrease their risk of being the victim of a cybercrime:

- **Frequently install security updates for all software.** This is the simplest, and perhaps most effective, way to protect an organization. Recommended updates should be downloaded directly from the manufacturer or publisher, or through the operating systems built-in update tool, to protect from spoof sites that masquerade as updates. The easiest way to do this is to set computers to automatically update when new security patches are released. This simple change in behavior can have tremendous impacts on the overall security of digital environments.
- **Keep anti-virus software active and up-to-date, running frequent security scans.** Protection from viruses and malware also means not opening suspect email or attachments from unknown sources. And users should perform at least one full scan of their computer a month, while software with real-time monitoring better protects online activities. Some newer operating systems, such as Windows 8.1, include virus and malware protection. Additionally, rebooting computers to complete all updates at least once a week ensure virus definitions and software is up-to-date and running correctly.
- **Whenever possible, use the newest versions of applications - they typically have much stronger security features.** As a response to existing or perceived future threats, newer products typically incorporate improved security features that more effectively mitigate techniques that are currently being used to exploit vulnerabilities. Deploying these product versions widely can mitigate the risk an organization faces from several of the most commonly detected exploits.
- **Manage Active Directory roles and access and validate the configuration management of applications to ensure there are no security gaps.** Processes should be in place to keep track of what is network accessible, identify if guest accounts are turned on unnecessarily, and check for open ports.

- **Monitor what software employees are bringing into the workplace and into the network environment.** Developing a policy for computer security with guidance for employees on acceptable software downloads and activity helps increase the likelihood that all parties are invested in the security of your digital environment.
- **Manage how employees employ personal devices at work.** Business imperatives to take advantage of the benefits of user mobility, and cultural changes in the way users expect a "from anywhere from any device experience" are creating a tidal wave of demand for bring-your-own-device (BYOD). A successful BYOD program needs to take into account data security risks and to put plans in place to protect company data.
- **Use genuine software.** The procurement and use of genuine software heightens protections from cybersecurity threats and is a top priority for organizations that want to effectively manage real and immediate cybersecurity risks. Because of the link between counterfeit software and IT security issues from malware, businesses risk losing time and money, and threatening critical infrastructure. The best prevention is to implement practices that ensure genuine software is used. See more in the Licensing section of this document.

Next steps

Within this final step, you help the customer review or write policies and procedures to ensure ongoing proper software asset management (SAM). Establishing standard practices can help reduce waste, avoid unnecessary costs and business risks, and streamline the entire organization.

Additionally, SAM must take into account the speed and ease with which new services can be provisioned, configured, and released. This ease of implementation introduces organizational risks by decentralizing IT services. Because Cloud services appeal directly to business users, the risk exists that these services may be purchased outside the traditional software procurement and SAM processes.

Deliverables

The following deliverable is **due to the customer** at the **end** of the engagement.

- **Cybersecurity Assessment Report.** This report must contain at a minimum:
  - An Executive Summary. A high-level summary of project background and scope, engagement result, recommendations and next steps.
  - An assessment of the customer's overall cybersecurity state, in relation to their current IT infrastructure including but not limited to:
    - SQL Server Service Pack deviations
    - Windows/SQL Server reboot age
    - Windows Server Service Pack deviations
    - Mainstream/Extended support analysis – Operating system and Microsoft software
    - Anti-virus software /Anti- malware running in environment
    - User account status
    - Password controls and last login dates
    - Operating system activation-related information
    - Stale domains and data sources
  - A cybersecurity roadmap to assist the customer in better protecting their IT assets, including all business, licensing and technology guidance.
  - An assessment of customer's cybersecurity-related SAM policies and procedures strengths, weaknesses and areas of opportunity, including recommendations for improvement.

  - Advice on how to engage with a cybersecurity professional, if needed, and a list of additional resources on cybersecurity, such as the Council on Cybersecurity, which would benefit the customer.
  - 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 summary of current or upcoming end-of-life products, with upgrade path recommendations
- **EDP.** A document with details related to all hardware and software currently deployed within the customer's IT infrastructure

If an ELP is required:

- **The ELP** is a spreadsheet that provides details related to license entitlements and deployments. The spreadsheet must be produced using I-AM (Note: Defined in Deliverables to Microsoft).
- **Licensing Optimization Recommendations 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:
- Identification of all of the customer's Volume License Agreements (VLAs) with Microsoft and a recommendation on any beneficial consolidation.
  - Consumption information, detailing installed products that are unused or underutilized (e.g., no use in last six months).
  - Recommendations for a repeatable, simplified inventory collection process for future True-ups (for Enterprise Agreement customers only).
  - Additional customer-specific recommendations based on captured data and insights.

The ELP must be finalized in the I-AM. An encrypted ELP must be uploaded into the designated tool (currently CHIP) as proof of execution.

The following deliverable is **due to Microsoft** at the **end** of the engagement.

- **Established Deployment Position (EDP).** The EDP, a I-AM 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 I-AM. The EDP will then be created by the partner using I-AM which is to be given to the customer and Microsoft. EDPs produced outside of I-AM 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.
- **Cybersecurity Assessment Report.** This must be the same Cybersecurity Assessment Report provided to the customer, as outlined above.

- **Letter of Confirmation** (only applicable for customer countries listed below):
  - Required: China
  - Advised: India, Malaysia, Indonesia, Philippines, and Vietnam

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>."

Due to customer

Required:

Letter of Engagement	Explains what to expect during your SAM engagement.
Cybersecurity Assessment Report	Contains an Executive Summary, summary of project background and scope, engagement results, recommendations and next steps.
EDP	Provides details related to all hardware and software currently deployed within the customer's IT infrastructure.

Optional:

ELP	Provides details related to license entitlements and deployments.
License Optimization Report (required with an ELP)	Presents recommendations on how to optimize your infrastructure and improve licensing efficiencies.

Due to Microsoft

Required:

Letter of Engagement	Provides the customer with an overview of the SAM engagement.
EDP	Provides details related to the customers' Microsoft software deployments and usage data.
Cybersecurity Assessment Report	Contains an Executive Summary, summary of project background and scope, engagement results, recommendations, and next steps (same report as given to customer).

Continued on next page

Letter of Confirmation (required for certain countries)	Requires customer's chop (stamp) or email from the customer's corporate domain confirming provision of the SAM engagement (see previous page for list of countries required this letter).

Required if an ELP is included the scope of the engagement:

ELP	Provides details related to license entitlements and deployments.

View sample report here.

SAM resources

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

View sample report here.

Appendix

Appendix

Resources

SAM

SOFTWARE ASSET MANAGEMENT

Resources

Microsoft Partner Network - SAM
https://mspartner.microsoft.com/en/us/pages/licensing/software-asset-management.aspx

SAM Partner Playbook
https://mspartner.microsoft.com/en/us/pages/licensing/downloads/SAM-Partner-Playbook.aspx

Microsoft Security Intelligence Report, Volume 16
http://www.microsoft.com/security/sir/

Microsoft Security and Identity Services
http://www.microsoft.com/en-us/microsoftservices/security_identity.aspx

Microsoft Security Risk Assessment
http://download.microsoft.com/download/5/D/0/5D06F4EA-EAA1-4224-99E2-0C0F45E941D0/Microsoft%20Security%20 Risk%20Asessment%20Datasheet.pdf

Identity and Access Competency
https://mspartner.microsoft.com/en/us/pages/membership/identity-and-access-competency.aspx

Microsoft Partner Portal
https://mspartner.microsoft.com/en/us/Pages/Locale.aspx

ISO/IEC 19770
www.19770.org

Microsoft SAM Tools
http://www.microsoft.com/sam/en/us/toolsoverview.aspx

Center for Internet Security
https://www.cisecurity.org/

Center for Internet Security Critical Controls
https://www.cisecurity.org/critical-controls/

Microsoft Security Intelligence Report Key Findings
http://download.microsoft.com/download/7/2/B/72B5DE91-04F4-42F4-A587-9D08C55E0734/Microsoft_Security_ Intelligence_Report_Volume_16_Key_Findings_Summary_English.pdf

Microsoft Security Essentials
http://www.microsoft.com/en-us/download/details.aspx?id=5201

Microsoft System Center

http://www.microsoft.com/systemcenter/en/us/service-manager.aspx

Appendix
Resources

Windows Intune
http://www.microsoft.com/windows/windowsintune/default.aspx

Microsoft Assessment and Planning (MAP) Toolkit
http://www.microsoft.com/sam/en/us/map.aspx

802.1X Authenticated Wired Access Overview
http://technet.microsoft.com/en-us/library/hh831831.aspx

AppLocker Overview
http://technet.microsoft.com/en-us/library/hh831409.aspx

Configuration Manager Software Metering
http://msdn.microsoft.com/en-us/library/jj218086.aspx

Microsoft Security Compliance Manager
http://technet.microsoft.com/en-us/library/cc677002.aspx

Active Directory Structure and Group Policy
http://technet.microsoft.com/en-us/library/cc978249.aspx

Microsoft Security Development Lifecycle
http://www.microsoft.com/security/sdl/default.aspx

SDL Tools
http://www.microsoft.com/security/sdl/adopt/tools.aspx

Configure 802.1X Wireless Access Clients by using Group Policy Management
http://msdn.microsoft.com/en-us/library/dd759173.aspx

Data Protection Manager
http://technet.microsoft.com/en-us/library/jj628208.aspx

Folder Redirection Overview
http://technet.microsoft.com/en-us/library/cc732275.aspx

StorSimple
http://azure.microsoft.com/en-us/documentation/services/storsimple/

IPsec
http://technet.microsoft.com/en-us/network/bb531150.aspx

Routing and Remote Access Service (RRAS)
http://technet.microsoft.com/en-us/library/dn614140.aspx

System Center Operations Manager
http://technet.microsoft.com/en-us/library/hh205987.aspx

Auditing and Logging
http://msdn.microsoft.com/en-us/library/ff649793.aspx

BitLocker
http://technet.microsoft.com/en-us/library/dn641993.aspx

Update Lifecycle
http://technet.microsoft.com/en-us/security/dn456534.aspx