CIS Center for Internet Security®

CIS Controls

Establish Basic Cyber Hygiene

Through a Managed Service Provider

Contents

Acknowledgments

CIS would like to thank the many security experts who volunteer their time and talent to support the CIS Critical Security Controls® (CIS Controls®) and other CIS work. CIS products represent the effort of a veritable army of volunteers from across the industry, generously giving their time and talent in the name of a more secure online experience for everyone.

Editor
Ginger E. Anderson, CIS

Contributors
Walter McKay, CIS
Justin Burr, CIS
Greg Carpenter, AWS
Paul Campbell, Knock CRM

Summary

Small and medium enterprises often face the need to outsource their information technology infrastructure and services. Managed Service Providers (MSPs) offer the ideal solution of providing the services at an affordable cost and allow enterprises to focus on other aspects of their operations. Despite the convenience, relying on a third party for all of an organization's technology needs can leave an organization feeling uncertain, vulnerable, or provide a false sense of security. The current threat landscape indicates a particular cyber threat actor interest in these third-party providers. The providers serve as attractive targets for cyber-attacks due to the level of access they afford actors into the clients' networks and the ease with which actors can affect multiple victims by compromising one entity. This paper provides an overview of the CIS Critical Security Controls® (CIS Controls®) and provides small and medium enterprises with a guideline questionnaire to ensure their basic cyber hygiene needs are met by their managed service provider.

Introduction

Small and medium enterprises often face a variety of information technology (IT) challenges: lack of funding, constantly evolving technologies, increasing legal and regulatory requirements, and lack of skilled and trained IT employees. As a result, these enterprises oftentimes rely on third-party providers such as MSPs for portions or, in some cases, all of their IT infrastructure and services. The enterprise decision to outsource IT, computer support, and network and management is an alternative to hiring in-house IT specialists and allows the enterprise to focus on other operations. MSPs, from a security perspective, can help enterprises reduce the risk of understaffed and underfunded in-house solutions. They offer a wide range of solutions and services that include, but are not limited to, those listed to the right.

MSP Services and Solutions

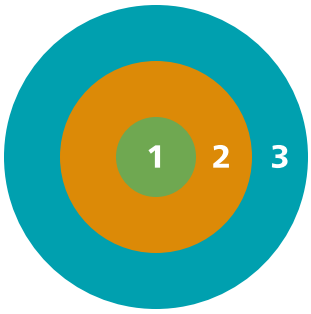
- Anti-virus, anti-spam, anti-phishing, and anti-malware services
- Data backup services
- Network monitoring services
- Software configuration and provisioning services
- Cloud computing services (applications, services, resources, management)
- Hardware configuration and implementation services
- Network infrastructure configuration, implementation, and enhancement services
- Patch, repair, and update management services
- On-demand augmentation of incumbent staff/expertise

Due to their offerings, MSPs are highly attractive to potential clients. What is there not to love, right? In recent years the cybersecurity community has published guidance and threat intelligence products that show an increase in cyber threat actor (CTA) targeting of MSPs. It turns out that the same services that attract clients, also, unfortunately, attract CTAs. MSPs are high-value targets as they often have extensive access to multiple clients' networks and systems. A compromised MSP can provide CTAs access to multiple organizations' data, systems, and proprietary information, which can result in disruption of operations, thus maximizing their "bang for the buck." According to open source reporting, these attacks often exploit authentication, patching, architectural weaknesses, and other control deficiencies at MSPs.

How can small and medium enterprises protect themselves? Avoiding MSPs altogether is not the answer, but asking the MSPs the appropriate questions when shopping for a provider can help inform an enterprise's decision. This guide will take a look at the CIS Controls and provide a baseline of questions to ask MSPs. Both the implementation of Controls at the MSP and knowing which Controls the MSP implements for its clients are relevant.

CIS Controls

The CIS Critical Security Controls® (CIS Controls) are a prioritized set of defensive actions that mitigate the most common attacks against systems and networks. In the most recent version of the CIS Controls, CIS took a horizontal look at the Sub-Control or Safeguard level and introduced Implementation Groups (IGs). IGs provide an "on ramp" making it easier for small and medium enterprises to get started when implementing the CIS Controls. The 171 Sub-Controls are separated into three IGs as a new way to prioritize the Controls with a combination of technical and procedural defenses.



Definitions	1	2	3
Implementation Group 1 CIS Sub-Controls for small, commercial off-the-shelf or home office software environments where sensitivity of the data is low will typically fall under IG1. IG1 represents basic cyber hygiene for all organizations including those in IG2 and IG3.	●		
Implementation Group 2 CIS Sub-Controls (safeguards) focused on helping organizations handling more sensitive assets and data. IG2 safeguards should also be followed by organizations in IG3.	●	●	
Implementation Group 3 CIS Sub-Controls (safeguards) are necessary for organizations that handle critical assets and data. IG3 encompasses safeguards in IG1 and IG2.	●	●	●

IG1

IG1 is aimed towards small and medium enterprises with limited resources and consists of 43 Sub-Controls, both technical and procedural, that enterprises should perform. The Safeguards in IG1 are the groundwork for an effective cyber defense. IG1, if properly implemented, can help enterprises defend against the top five most common attacks, as outlined by the Verizon Data Breach Investigations Report. For additional information, please reference the CIS Community Defense Model.

IG2

IG2 is geared towards enterprises that have a grasp on the basics and need to defend against more advanced threats. It is the largest IG and contains 140 Sub-Controls. This IG tends to be more technical and builds on IG1. IG2 includes Safeguards such as formal vulnerability management processes, advanced logging, and Domain-based Message Authentication, Reporting and Conformance (DMARC).

IG3

IG3 helps to defend against advanced persistent threats, zero days, and other sophisticated nation state attacks and is generally meant for well-funded enterprises. IG3 contains 31 Sub-Controls that build off the previous IGs. It is heavily technical and requires advanced IT knowledge to put into place and maintain.

Basic Cyber Hygiene Questionnaire

The Safeguards in IG1 provide a guideline for basic cyber hygiene controls for all enterprises. In particular, IG1 is implementable by small and medium enterprises. The Safeguards in IG1 can help organizations protect their IT infrastructure, systems, and data from most cyber-attacks. For a complete list of IG1 Safeguards, see Appendix B. Using IG1 as a guide, CIS compiled a list of questions that organizations shopping for an MSP can use to inform their selection and ensure their basic cyber hygiene needs are met. Keep in mind, the list is meant to be descriptive and not necessarily prescriptive. A questionnaire template is provided in Appendix C. This template can be modified to address an enterprise's concerns before sending to the MSP.

1 **Does the MSP maintain documentation describing the environment used to administer customer environments?** **(Sub-Controls: 1.4, 1.6, 12.1, 12.4)**

- **a** How often is the documentation updated?
- **b** Does the MSP assess against a framework to protect their own and customers' environments?

Objective

The MSP should be able to provide documentation upon request and, at a minimum, indicate the use of a framework to guide protective and detective controls implemented in the environment. An enterprise with the technical knowledge to understand the documentation should look for the MSP to demonstrate an intentional architecture for their infrastructure with documented controls to protect their environment and that of their customers. The documentation should be up-to-date and should reflect the current environment. Diagrams, descriptive narratives, or other documentation should include, without limitation, network and infrastructure topology, identification of protective and detective controls, and demonstration of environment segmentation.

2 **Is my (customer) network isolated from other networks within the MSP's environment?** **(Sub-Controls: 2.2, 7.1, 7.7, 8.2, 8.4, 8.5, 9.4, 11.4, 19.6)**

- **a** Does the MSP have a defense-in-depth approach to protect the MSP and customer environments?
- **b** Is there a process in place to ensure all devices are up-to-date?
- **c** Does the MSP use a framework to guide these efforts?

Objective

The MSP will likely maintain a single control environment, but customer networks should be isolated within their own networks and protected by discrete logical or physical firewalls. Firewalls deployed at multiple layers (i.e., network, host, and application) demonstrate an MSP that plans defense-in-depth. The MSP should be able to describe the firewalls operated in the environment and should ensure they are up-to-date. Look for sophisticated controls, such as IDS and NAC, which demonstrate a high security maturity MSP. At a minimum, the MSP should be able to indicate a framework used to guide the controls implemented.

3 **Does the MSP have a backup and system recovery strategy for itself and customers? (Sub-Controls: 19.1, 19.3, 19.5, 19.6)**

- **a** Can the strategy be customized?
- **b** Are my (customer) high-value assets and data backed up more frequently?

Objective

The MSP should be able to talk to both their own systems and their customers'. The MSP should have a process to capture customer input to tailor these strategies, as each enterprise is unique. The MSP should prioritize high-value data with more frequent backups, and it is normal for low-value systems to have no automated backup mechanism.

4 **Does the MSP manage and restrict access to management systems within the environment and into customer environments? (Sub-Controls: 4.3, 6.2, 14.6)**

- **a** Does the MSP have a list of processes that require recurring access to the customers' systems?
- **b** Is the access restricted to only those individuals responsible for those specific processes?
- **c** Does the MSP monitor the use of these accounts?

Objective

The MSP should be able to detail the level of access required to perform these functions and explain the access control mechanisms. It should be able to describe the process by which recurring access of the customers' systems is conducted to ensure permissions are granted on a "need-to-know" basis. The MSP should ensure access reports are generated and reviewed periodically and also track, log, and audit usage of each account.

5 **Do you (MSP) have change management processes for MSP administration systems and customer environments? (Sub-Controls: 3.4, 3.5)**

- **a** Is the process documented?
- **b** Are customers made aware of changes being made within their environments?

Objective

An MSP should be able to demonstrate control of changes to their own environment and their customers'. Look for a documented procedure when updating critical network infrastructure, servers, and applications. Determine if you, as a customer, will have access to tickets worked in your own environment.

6 **Does the MSP have a process for customers to enroll in specific applications and services provided by the MSP? (Sub-Controls: 4.2, 16.8, 16.9, 16.11)**

- **a** Does the MSP have and enforce a password policy?
- **b** Is the usage of each account monitored?

Objective

An MSP should be able to describe the initial enrollment process, and password policies and procedures to include, without limitation, a password expiration, length of password, password revocation, invalid logon attempt threshold, etc. The MSP should be tracking, logging, and auditing the usage of each account. It should provide a process for customers to authenticate to each application. For additional guidance on best practices for password policies, please reference the CIS Password Policy Guide: Passphrases, Monitoring, and More.

7 **Does the MSP have a process for its administrative environment, and the environments of its customers, to harden and patch systems and applications? (Sub-Controls: 4.3, 5.1)**

- **a** Do you (MSP) have a secure baseline for servers, endpoints, systems, network, software, and mobile devices to include virtual and cloud environments?
- **b** Are customers made aware of changes being made within their environments?
- **c** Does the MSP have clearly defined roles and responsibilities for the personnel conducting and managing these functions?

Objective

At a minimum, the MSP should be able to share a standard that includes changing default passwords, disabling unused services and unencrypted management ports, and encrypting data at rest. The MSP should be able to demonstrate a patching methodology, such as patching operating systems and applications weekly, and demonstrate effective communication around those updates to customers. The MSP should have clearly defined roles and responsibilities for the personnel conducting and managing these functions. It should be able to provide a comprehensive list of tools and level of access required to complete these functions and demonstrate tracking, logging, and auditing of these accounts.

8 **Please describe the processes and mechanisms by which the MSP tracks software inventory and patch level. (Sub-Controls: 2.1, 2.2, 2.6)**

Objective

The MSP should have a process in place to track the various software in use and provide details of the last update. If necessary, it should be able to provide the inventory and outline which software is necessary to meet business operational requirements. Those not necessary should be removed if the environment allows.

9 **Please describe data encryption, in transit and at rest, for the MSP administrative systems and customer environments. For printed materials, please describe physical security controls.** **(Sub-Controls: 13.6, 15.7, 15.10)**

Objective

The MSP should protect wireless networks using WPA2, as it employs modern encryption and is robust against attack. The MSP should employ full disk encryption, such as BitLocker or FileVault, on all desktops and laptops. Server volumes are not often encrypted, but databases generally are.

10 **Do you (MSP) have security and privacy policies and related trainings for MSP staff?** **(Sub-Controls: 13.1, 13.2, 17.5, 17.6, 17.7, 17.8, 17.9)**

- **a** Do the policies address protection of customers' sensitive data?
- **b** Are all staff trained on the policies and general security and privacy practices?

Objective

The MSP should be able to demonstrate documented policies to govern their environment, configuration of customer environments, and interaction with customer environments. The MSP should train its staff on the policies or, at least, on general security and privacy practices.

11 **Please provide the results of any security or privacy audits conducted on or by the MSP in the preceding 18 months.**

- **a** Do you (MSP) have a cyber insurance policy?

Objective

Audit reports should be available for any MSP employing more than 200 people, but are not as common for small MSPs. Look for the most common and appropriate certifications and reports such as ISO 27001 and SOC 2 Type II. In case of a data breach or cyber-related incident, such as ransomware, a cyber insurance policy may help protect the MSP. Ensure the policy covers the MSP's customers.

APPENDIX A:

Abbreviations and Acronyms

AES	Advanced Encryption Standard
CIS	Center for Internet Security
CTA	Cyber Threat Actor
IDS	Intrusion Detection System
IG	Implementation Group
IT	Information Technology
MSP	Managed Service Provider
NAC	Network Access Control

CIS Controls

APPENDIX B:
IG1 Sub-Controls

Sub-Control	Sub-Control Title	IG1
1.4	Maintain Detailed Asset Inventory	•
1.6	Address Unauthorized Assets	•
2.1	Maintain Inventory of Authorized Software	•
2.2	Ensure Software is Supported by Vendor	•
2.6	Address Unapproved Software	•
3.4	Deploy Automated Operating System Patch Management Tools	•
3.5	Deploy Automated Software Patch Management Tools	•
4.2	Change Default Passwords	•
4.3	Ensure the Use of Dedicated Administrative Accounts	•
5.1	Establish Secure Configurations	•
6.2	Activate Audit Logging	•
7.1	Ensure Use of Only Fully Supported Browsers and Email Clients	•
7.7	Use of DNS Filtering Services	•
8.2	Ensure Anti-Malware Software and Signatures Are Updated	•
8.4	Configure Anti-Malware Scanning of Removable Devices	•
8.5	Configure Devices Not to Auto-Run Content	•
9.4	Apply Host-Based Firewalls or Port Filtering	•
10.1	Ensure Regular Automated Backups	•
10.2	Perform Complete System Backups	•
10.4	Ensure Protection of Backups	•
10.5	Ensure Backups Have at Least One Non-Continuously Addressable Destination	•
11.4	Install the Latest Stable Version of Any Security-Related Updates on All Network Devices	•
12.1	Maintain an Inventory of Network Boundaries	•
12.4	Deny Communication over Unauthorized Ports	•
13.1	Maintain an Inventory of Sensitive Information	•
13.2	Remove Sensitive Data or Systems Not Regularly Accessed by Organization	•
13.6	Encrypt the Hard Drive of All Mobile Devices	•
14.6	Protect Information through Access Control Lists	•

Sub-Control	Sub-Control Title	IG1
15.7	Leverage the Advanced Encryption Standard (AES) to Encrypt Wireless Data	•
15.10	Create Separate Wireless Network for Personal and Untrusted Devices	•
16.8	Disable Any Unassociated Accounts	•
16.9	Disable Dormant Accounts	•
16.11	Lock Workstation Sessions After Inactivity	•
17.3	Implement a Security Awareness Program	•
17.5	Train Workforce on Secure Authentication	•
17.6	Train Workforce on Identifying Social Engineering Attacks	•
17.7	Train Workforce on Sensitive Data Handling	•
17.8	Train Workforce on Causes of Unintentional Data Exposure	•
17.9	Train Workforce Members on Identifying and Reporting Incidents	•
19.1	Document Incident Response Procedures	•
19.3	Designate Management Personnel to Support Incident Handling	•
19.5	Maintain Contact Information for Reporting Security Incidents	•
19.6	Publish Information Regarding Reporting Computer Anomalies and Incidents	•

CIS Controls

APPENDIX C:
Basic Cyber Hygiene Questionnaire Template

The following can be used to gather information from MSPs in order to inform an enterprise's decision to conduct business with said MSP. It can be modified to meet an enterprise's need.

1. **Does the MSP maintain documentation describing the environment used to administer customer environments?**
   - **a** How often is the documentation updated?
   - **b** Does the MSP assess against a framework to protect its own and customers' environments?

2. **Is my (customer) network isolated from other networks within the MSP's environment?**
   - **a** Does the MSP have a defense-in-depth approach to protect the MSP and customer environments?
   - **b** Is there a process in place to ensure all devices are up to date?
   - **c** Does the MSP use a framework to guide these efforts?

3. **Does the MSP have a backup and system recovery strategy for itself and customers?**
   - **a** Can the strategy be customized?
   - **b** Are my (customer) high-value assets and data backed up more frequently?

4. **Does the MSP manage and restrict access to management systems within the environment and into customer environments?**
   - **a** Does the MSP have a list of processes that require recurring access to the customers' systems?
   - **b** Is the access restricted to only those individuals responsible for those specific processes?
   - **c** Does the MSP monitor the use of these accounts?

5. **Do you (MSP) have change management processes for MSP administration systems and customer environments?**
   - **a** Is the process documented?
   - **b** Are customers made aware of changes being made within their environment?

6. **Does the MSP have a process for customers to enroll in specific applications and services provided by the MSP?**
   - **a** Does the MSP have and enforce a password policy?
   - **b** Is the usage of each account monitored?

7 **Does the MSP have a process for its administrative environment, and the environments of its customers, to harden and patch systems and applications?**

- **a** Do you (MSP) have a secure baseline for servers, endpoints, systems, network, software, and mobile devices to include virtual and cloud environments?
- **b** Are customers made aware of changes being made within their environment?
- **c** Does the MSP have clearly defined roles and responsibilities for the personnel conducting and managing these functions?

8 **Please describe the processes and mechanisms by which the MSP tracks software inventory and patch level.**

9 **Please describe data encryption, in transit and at rest, for the MSP administrative systems and customer environments. For printed materials, please describe physical security controls.**

10 **Do you (MSP) have security and privacy policies and related trainings for MSP staff?**

- **a** Do the policies address protection of customers' sensitive data?
- **b** Are all staff trained on the policies and general security and privacy practices?

11 **Please provide the results of any security or privacy audits conducted on or by the MSP in the preceding 18 months.**

- **a** Do you (MSP) have a cyber insurance policy?

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation. We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices. To learn more, visit CISecurity.org or follow us on Twitter: @CISecurity.

cisecurity.org
info@cisecurity.org
518-266-3460
Center for Internet Security
@CISecurity
TheCISecurity
cisecurity