

The Cost of Cyber Defense

Version 1.1

**An Executive Guide for
Implementation Group 1 (IG1)
of the CIS Critical Security Controls®**

April 2025

Acknowledgments

The Center for Internet Security® (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.

As a nonprofit organization driven by its volunteers, we are always in the process of looking for new topics and assistance in creating cybersecurity guidance. If you are interested in volunteering and/or have questions, comments, or have identified ways to improve this guide, please write us at: controlsinfo@cisecurity.org.

All references to tools or other products in this guide are provided for informational purposes only, and do not represent the endorsement by CIS of any particular company, product, or technology.

Editors

Valecia Stocchetti, CIS
Charity Otwell, CIS
Thomas Sager, CIS
Josh Franklin, CIS
Sarah Day, CIS

Contributors

Mark Allers, CimCor
Mike Burgard, Marco Technologies
Chris Cronin, Halock Security Labs
Richard Diver, Microsoft
Kevin Donohue, AWS
Gregory Carpenter, AWS
Mathew Everman, CIS
Jennifer Jarose, CIS
Jamie Kosempa, Echo Health Inc.
Philippe Langlois, Verizon

This work is licensed under a Creative Commons Attribution-Non Commercial-No Derivatives 4.0 International Public License (the link can be found at <https://creativecommons.org/licenses/by-nc-nd/4.0/legalcode>).

To further clarify the Creative Commons license related to the CIS Controls® content, you are authorized to copy and redistribute the content as a framework for use by you, within your enterprise and outside of your enterprise for non-commercial purposes only, provided that (i) appropriate credit is given to CIS, and (ii) a link to the license is provided. Additionally, if you remix, transform, or build upon the CIS Controls, you may not distribute the modified materials. Users of the CIS Controls framework are also required to refer to (<http://www.cisecurity.org/controls/>) when referring to the CIS Controls in order to ensure that users are employing the most up-to-date guidance. Commercial use of the CIS Controls is subject to the prior approval of the Center for Internet Security, Inc. (CIS®).

Contents

Executive Summary	1
Introduction	2
Methodology	3
Which Protections to Start With	4
IG1 Enterprise Profiles	5
Tooling and Associated Costs	7
Tools	7
CSP and MSP Tools and Services	8
Cost	11
CSP and MSP Costs	12
Conclusion	14
Appendix A: The 10 Areas of Cyber Defense	15
Asset Management	15
Data Management	16
Secure Configurations	18
Account and Access Control Management	19
Vulnerability Management	20
Log Management	22
Malware Defense	23
Data Recovery	24
Security Training	25
Incident Response	26
Appendix B: Some Observations on Tool Types	27
Appendix C: Life Cycle Considerations	28
Appendix D: IG1 Safeguards	29
Appendix E: IG1 Safeguards Covered by CIS and MS-ISAC Tools	31
Appendix F: CIS Controls	33
Appendix G: CSP Capability Mappings	35
Microsoft	35
Amazon	36

Google	37
Appendix H: CSP and MSP Detailed Cost Considerations	38
CSPs	38
MSPs	39
Appendix I: Links and Resources	40

Executive Summary

Enterprises looking to implement cyber defenses wish to know three things:

- 1 Which protections will we start with?
- 2 Which tools will be needed to implement those protections?
- 3 How much will an implementation cost?

In response, CIS published [The Cost of Cyber Defense: CIS Controls Implementation Group 1 \(IG1\) v1.0](#), to help answer those questions. The focus of the 1.0 release was to provide evidence-based research results on the cost of on-premises tools in relation to information technology (IT) and cybersecurity budgets. This guide, *The Cost of Cyber Defense: Implementation Group 1 (IG1) version 1.1*, is an update, with additional data and conclusions pertaining to tools and services offered by Cloud Service Providers (CSPs) and Managed Service Providers (MSPs), which expands the scope of this guide to now include outsourced and/or hybrid environments.

Every enterprise wants a reasonable starting point at a reasonable cost for cybersecurity. The CIS Critical Security Controls® (CIS Controls®) are a prioritized set of actions that can be implemented to form an effective cyber defense program. The key word here is *prioritized*. CIS recommends starting with [Implementation Group 1 \(IG1\)](#) of the CIS Controls, which constitutes *essential cyber hygiene* for any enterprise and is a “must do” list of actions to take as a foundation for more complex countermeasures, such as a security information and event management (SIEM) service, needed by larger enterprises that face more sophisticated adversaries and protect more sensitive data or services.

The v1.0 release of this guide organized the the CIS Safeguards from IG1 into 10 categories and identified the types of tools needed to deploy and maintain these security actions. Many tools offer more than one service which supported the use of these categories to simplify the findings for the end user. For example, asset management tool vendors often provide hardware and software inventory services as well as vendor management services. To estimate the cost to implement these Safeguards, we researched the cost of on-premises tools for each of the 10 categories covered in v1.0 of the guide.

Not all environments strictly utilize on-premises tools, however. In some cases, an enterprise will choose to use a tool bundled with a product, an open-source tool, a no-cost tool, or the tools might be selected by an MSP or CSP if some IT and/or security services are outsourced. In this updated version (v1.1) of the guide, we address this complex scenario with the intention of providing our readers with an estimate of how much an enterprise can expect to pay an MSP or CSP to implement IG1.

Our estimate shows that obtaining and deploying on-premises versions of the tools, using a CSP and/or MSP, or a combination of all three should be less than the IT budget (5% of annual revenue) and/or cybersecurity budget (20% of the IT budget) set forth by an IG1 enterprise of any size. Even with adding in the overhead of implementing the necessary policies to support them, IG1 Safeguards can provide a reasonable, necessary, and effective starting point for any enterprise.

The purpose of this guide is to provide enterprises with a picture into how realistic and cost-effective it can be to achieve essential cyber hygiene (IG1), whether that be in an entirely on-premises environment or a hybrid one. In turn, this information will help enterprises make informed and prioritized decisions when it comes to the cost associated with cyber defense. Several different audiences can benefit from this guide including members of the executive team (e.g., CEO, CFO, CISO, CIO) and IT administrators.

Introduction

CIS advocates that all enterprises start Implementation Group 1 (IG1) of the CIS Controls. These Safeguards are a set of protections that are sufficient for small and medium-sized enterprises (SMEs) that do not face sophisticated attacks. These Safeguards are also the required foundation for implementing more resource intensive protections that are found in the two higher Implementation Groups (IG2 and IG3), which are often applied to protect larger enterprises or enterprises with highly sensitive data and services.

Implementing Safeguards requires tools that might be obtained as open-source, built in-house, purchased with support from commercial vendors, or bundled into an IT or security product as an additional feature or capability. Windows® Server, for example, has many security management features and a powerful scripting language with security capabilities bundled into the product.

In this guide, the Safeguards from IG1 are broken out into 10 categories that make it easier to understand how to apply these security actions to your IT and enterprise. The types of tools needed to implement IG1 Safeguards are identified in [tables](#) organized by these categories.

The focus of this guide is to address the how and how much cost questions posed above. The guide leverages the research done in version 1.0 and considers additional data that includes hybrid environments leveraging CSPs and MSPs. When utilizing CSPs or MSPs to build a cybersecurity program, the methodology referenced within this guide can be applied, but the results are not as comparable as with the research presented in version 1.0. For this reason, we have added sections for the cost of both CSPs and MSPs within a separate subsection under the [Tooling and Associated Costs](#) section of this guide.

This guide offers data, insights, and a methodology for IT administrators, information security professionals, as well as C-Suite executives to make informed decisions in their journey to achieve IG1 for their enterprise.

How to Use this Guide

This guide has four main sections. The first section describes our methodology for estimating the cost of implementing IG1 for enterprises of different sizes. The second section briefly discusses the Safeguards themselves and where to start. The third section outlines the IG1 Enterprise Profiles. The fourth section identifies the types of tools needed to implement the Safeguards and estimates the cost of deploying on-premise tools and cost considerations for CSPs and MSPs.

In addition, practitioners can find valuable information in [Appendix A](#) of this guide that can help to further break down the cost for each tool as well as provide some insight into several considerations while procuring these tools. Also, a [spreadsheet](#) is available for users to download if they wish to use it for budgeting and/or implementation purposes.

Methodology

To get us to the ultimate question — “How much does it cost to implement IG1?” — the methodology is simple. Start with the basics.

The first step was to divide the CIS Controls into 10 categories of activities: *Asset Management, Data Management, Secure Configurations, Account and Access Control Management, Vulnerability Management, Log Management, Malware Defense, Data Recovery, Security Training, and Incident Response*. The Safeguards in IG1 were then placed into the appropriate categories.

From here, Safeguards were mapped to tool types. An example of a tool type is an Enterprise and Software Asset Management Tool that provides services for a group of seven Safeguards corresponding to asset management. Tooling names vary from vendor to vendor.

One of the challenges with providing general costs of tools is that each vendor has its own pricing model – often priced by device, user, usage (e.g., hours, gigabytes (GB), megabytes (MB), or another factor). To simplify this pricing and also to provide deeper insight for enterprises of different sizes, three different hypothetical Enterprise Profiles were created for IG1 – Tier 1, Tier 2, and Tier 3.

It is possible that within these tiers, an enterprise will fall below or above depending on their specific enterprise’s structure and that is OK. Tiers can, and will, be affected by factors such as: sector, industry, revenue, and employee count. For enterprises that fall within one of these tiers and wish to obtain a more precise amount to calculate their cybersecurity and IT budgets, we also provide guidance in the [Tooling and Associated Costs](#) section of this guide as to how much, on average, an enterprise can estimate to spend per person/per year on IT and cybersecurity when implementing IG1 Safeguards. This way, an enterprise that may fall in between a tier or outside of a tier can still obtain a clear picture as to whether they are spending too much or too little on IT and cybersecurity.

Once the tiers were created, pricing was obtained for over 200 vendor-specific tools based on the Enterprise Profile attributes. In some cases, an enterprise will choose to use a tool bundled with a product, an open-source tool, or a utility that is provided as freeware, or the tools might be selected by an MSP or CSP if some IT and/or cybersecurity services are outsourced. A slightly different methodology was applied when calculating costs for MSPs and CSPs. In order to obtain these data sets, we used the IG1 Enterprise Profiles and publicly available data to determine costs. The findings for this research are represented within the [Tooling and Associated Costs](#) subsection of this guide.

Naturally, many costs need to be considered and budgeted for to properly implement, secure, and maintain tools. Examples include costs associated with labor, tool updates, physical hardware or virtual assets, training, license renewals, integration, testing, consulting, advertising, and more.¹

Some tools and services will satisfy several Safeguards, and others will satisfy only one. For this guide, a comprehensive list of vendor tools that can be used to implement IG1 is out of scope. CIS has published an additional guide, [Establishing Essential Cyber Hygiene \(v8.1\)](#), which provides several no-cost and open-source tools for implementing IG1. There are also many tools and services produced and published by CIS. A mapping of these tools and services can be found in [Appendix E](#) of this guide and on our [website](#).

¹ These costs are much more difficult to calculate in a general sense and therefore were not included in the cost calculations shown in this guide. However, the absence of these cost estimates does not diminish their importance. They should be accounted for when generating a budget of any kind.

Which Protections to Start With

Every enterprise is encouraged to implement a cybersecurity framework. The National Institute of Standards and Technology® (NIST®) Cybersecurity Framework (CSF) 2.0 simplified what this means into six security functions. Every enterprise must make a reasonable effort to:

- 1 **Govern** to provide the structure needed to steer a cybersecurity program toward achieving their enterprise goals.
- 2 **Identify** (track) what data it has and prioritize which pieces require the greatest protection.
- 3 **Protect** what it has commensurate to the harm that could occur if there is an attack.
- 4 **Detect** attacks.
- 5 **Respond** to attacks to minimize damage to their assets and possible harm to all stakeholders.
- 6 **Recover** from attacks.

These six security functions are the same as in the physical world. What is different here is how to carry them out on networks in the digital world.

The CIS Controls® are a prioritized set of technical and procedural activities that all enterprises can implement to defend against top threats. Reflected in the Controls, and in particular IG1, are the most critical Safeguards that enable an enterprise to *govern, identify, protect, detect, respond to, and recover* from cyber threats.

Over the years, we have brought more data, rigor, and transparency to the process of best practice recommendations. As a result, CIS has released the [Community Defense Model \(CDM\) v2.0](#), which is our most data-driven approach so far. The CDM looks at the conclusions from a variety of threat intelligence reporting to identify the top five attack types (malware, ransomware, web-application hacking, insider and privilege misuse, and targeted intrusions). We describe those attacks using the [MITRE Adversarial Tactics, Techniques, and Common Knowledge \(MITRE ATT&CK®\) Framework](#) to create attack patterns (or specific combinations of Tactics and Techniques used in those attacks), which allows us to analyze the value of individual defensive actions (i.e., Safeguards) against those attacks.

The [CIS Controls](#) are broken out into 18 areas of activity (i.e., Controls) for the security management of an enterprise's IT and networks. For each Control, there is a set of specific actions, which we call Safeguards, to achieve the security goals for each area. The Safeguards span a range of difficulty and cost to implement based on the expected threat, the complexity of what is being protected, and the value of the services and data at risk.

The set of Safeguards in [Implementation Group 1 \(IG1\)](#) is what we refer to as “*essential cyber hygiene*.” These are the set of cyber defense Safeguards that every enterprise should apply to guard against the most common attacks. Our CIS CDM v2.0 provides the technical underpinning for that declaration, where IG1 alone can effectively defend against 74% of the attack techniques found in the MITRE ATT&CK framework.² IG1 lays the groundwork to implement higher-level Safeguards found in IG2 and IG3.

For simplicity within this guide, we organized the set of Controls from IG1 into 10 areas of activity. Those areas, along with a mapping of the tools to the Safeguards in each area, are provided in the [Tooling and Associated Costs](#) section, which includes on-premises tools and CSP/MSP tools and services.

² [CIS Community Defense Model v2.0](#)

IG1 Enterprise Profiles

Defining what a small and medium-sized enterprise (SME) looks like is a challenging task, as there is no single profile that can define an SME. Several factors can be used to classify an SME. For example, according to the U.S. Small Business Administration (SBA), sizing standards can be measured in millions of dollars or by the number of employees.³

To estimate the cost of IG1 Safeguards, we first looked toward the tools that are needed to implement them. Tools are priced in many ways, with the most common being by: number of employees, number of users, number of workstations/servers, and/or usage (e.g., MB, GB, hours). In order to price tools appropriately, three enterprise profiles (Tier 1, Tier 2, Tier 3) were created. Shown below are the tiers, along with the employee count, number of IT team members, number of servers and workstations, number of total systems, size of logs, annual revenue, annual IT budget (5% of revenue), and annual cybersecurity budget (20% of IT budget). While 20% of an IT budget dedicated to cybersecurity spend may seem high, a report from the 2022 *Hiscox Cyber Readiness Report* highlighted that enterprises have increased their cybersecurity budgets from 17% to now 20% of the IT spend for SMEs.⁴ This is welcome news that cybersecurity budgets for SMEs are increasing, as they are typically known to be resource-constrained.

These tiers were created using data from various sources, such as the U.S. SBA, U.S. Census Bureau, and others. However, the tiers are not meant to be concrete. They are intended to assist with the process of calculating costs for IG1. Each enterprise will have a budget that is structured differently. For example, some may have an IT budget of 10% and a cybersecurity budget of 5%.

Table 1. IG1 Enterprise Profiles

Company Size	Employee Count	Number of IT Staff	Number of Servers	Number of Workstations	Number of Total Systems	Size of Logs ⁵	Annual Revenue	Annual IT Budget (5%)	Annual Cyber-security Budget (20% of IT Budget)
Tier 1	1 to 10	1 ⁶	1 to 2	1 to 12	1 to 14	0–100 GB/ Month	\$0–\$5,000,000	\$0–\$250,000	\$0–\$50,000
Tier 2	10 to 100	1 to 2	2 to 5	12 to 115	14 to 120	100–300 GB/ Month	\$5,000,001–\$50,000,000	\$250,001–\$2,500,000	\$50,001–\$500,000
Tier 3	100 to 999	2 to 10	5 to 50	115 to 1,149	120 to 1,199	Up to 1,500 GB/Month	\$50,000,001–\$500,000,000	\$2,500,001–\$25,000,000	\$500,001–\$5,000,000

Some enterprises using this guide may find that they fall within a tier but would like to obtain a more accurate number for their cybersecurity budget. In this instance, enterprises may use an average of \$5,000 per person/ per year to calculate their cybersecurity budget, which was also used for the ranges shown in Table 1 above. It is important to note that the amount spent on cybersecurity will be higher or lower depending on the tools selected, the costs associated with those tools, and what is within the enterprise's means from a people/process/technology standpoint. So, while we use \$5,000 per person and demonstrate ranges, these should be viewed as an estimated starting point in determining your own expected costs.

³ U.S. Small Business Administration: Table of Small Business Size Standards Matched to North American Industry Classification System Codes

⁴ <https://www.hiscox.com/documents/Hiscox-Cyber-Readiness-Report-2022.pdf>

⁵ Size of logs on a monthly basis.

⁶ For SMEs in Tier 1, IT services are often outsourced.

It is worth noting that both IT and cybersecurity budgets can have crossover, as some tools may actually be allocated under IT but are also used in cybersecurity. For example, an IT asset management tool may also be used for incident response purposes, making it a multipurpose tool. Enterprises will need to take this into consideration when budgeting. This is especially true when it comes to MSPs and CSPs, as much of the cost for these services will fall under the IT budget as compared to the cybersecurity budget.

Tooling and Associated Costs

Tools

IG1 consists of 56 Safeguards. However, this does not translate to 56 individual tools needed to implement IG1. Many of the Safeguards can be accomplished under a singular tool; alternatively, multiple tools may be required for some layered implementations of tools to meet Safeguards. To simplify the analysis underpinning this guide, the CIS Controls were grouped into 10 categories, as shown in Table 2 below. From there, a set of generic tool types were created, along with the policies needed to support them, and were mapped to IG1 Safeguards. These tools are not vendor-specific, but rather are general names that were used to group Safeguards together that require similar tooling. For example, obtaining an “Enterprise and Software Asset Management Tool” can be used to satisfy Safeguards 1.1, 1.2, 2.1, 2.2, 2.3, 9.1, and 12.1. The IG1 Safeguards defined within the CIS Controls can be found in [Appendix D](#) for quick reference.

Shown below is the mapping of generic tools and supporting policies to IG1 Safeguards. The table indicates that a small number of resources, specifically 10 policies/processes and 16 tools, are needed to implement IG1. [Appendix A](#) goes into detail about which Safeguards fall into each category and provides the cost estimate for the tools to implement that category’s Safeguards. It is noteworthy that based on analysis conducted for this guide, implementing all IG1 Safeguards, which is more than one-third of the total number of Safeguards in the CIS Controls, can be accomplished by employing a small number of tools and policies.

Prior to procurement and implementation, enterprises should review which tools may already be in place (or can be easily added on to preexisting platforms). If an additional tool is needed, research the functionality of the tool in question, as some vendors will integrate several tools into one platform. In these instances, it might not be necessary to procure single-use tools.

Table 2. IG1 Tooling

Category	Tool	Safeguards						
Asset Management	Enterprise Asset Management Policy/Process	1.1						
	Enterprise and Software Asset Management Tool	1.1	1.2	2.1	2.2	2.3	9.1	12.1
	Software Asset Management Policy/Process	2.1						
	Service Provider Management Tool	15.1						
Data Management	Data Management Policy/Process	3.1						
	Data Management Tool	3.2	3.4					
	Data Disposal Tool	3.5						
	Encryption Tool	3.6						
Secure Configurations	Secure Configuration Policy/Process	4.1	4.2					
	Configuration Management Tool	4.1	4.2	4.3	4.6	4.7	5.4	10.3
	Firewall	4.4	4.5					

Category	Tool	Safeguards					
Account and Access Control Management	Account and Credential Management Policy/Process	6.1	6.2				
	Identity and Access Management Tool	3.3	5.1	5.3	5.4		
	Password Management Tool	5.2					
	Multi-Factor Authentication Tool	6.3	6.4	6.5			
Vulnerability Management	Vulnerability/Patch Management Policy/Process	7.1					
	Vulnerability/Patch Management Tool	7.2	7.3	7.4			
Log Management	Log Management Policy/Process	8.1					
	Log Management Tool	8.2	8.3				
Malware Defense	Anti-Malware Software	10.1	10.2				
	DNS Service/Server	9.2					
Data Recovery	Data Recovery Policy/Process	11.1					
	Data Backup and Recovery Tool	11.2	11.3	11.4			
Security Training	Security Training and Awareness Policy/Process	14.1					
	Security Training and Awareness Tool(s)	14.2	14.3	14.4	14.5	14.6	14.7
Incident Response	Incident Response Planning	17.1	17.2	17.3			

It is important to emphasize that the enterprise may already have the tools in place (or can easily add on to preexisting platforms) to implement some of the Safeguards in IG1. For example, enterprises using Microsoft products may already have the built-in or added capabilities to achieve many of these actions (e.g., BitLocker®, Active Directory).

Enterprises may also consider other factors during tool selection, such as whether the implementation process is manual or automated. For example, an enterprise may choose to use a spreadsheet to track enterprise assets and software. However, as that enterprise grows, they may make the decision to move to an automated tool for inventory, adding to the cost.

All tools come with a cost. If an enterprise chooses to select all no-cost or open-source software, they may be spending more on vulnerability management or labor to ensure the software is safe to use. On the other hand, if an enterprise chooses to use a commercially-supported tool, they may be spending more on renewal costs, support costs, or integration costs. It is important not to get distracted with the tool and instead, focus on the activity. Enterprises can then find the tool that best fits their needs. The Safeguards broken out into categories in [Appendix A](#) also contain several questions that can help jump-start the process of creating policies and selecting tools to implement IG1.

CSP and MSP Tools and Services

SMEs can face a variety of IT challenges: insufficient funding, constantly evolving technologies, growing legal and regulatory requirements, and a lack of skilled and trained IT employees. Oftentimes, these enterprises rely on third parties, like MSPs and CSPs, for portions, or in some cases all, of their IT infrastructure and security services so that they can focus on other operations. As enterprises grow and evolve, implementation or use of these third-party services becomes essential.

The CIS Controls can be implemented in a hybrid environment, with some Safeguards satisfied internally and others satisfied by a CSP or an MSP. Additionally, there are a growing number of MSPs that are offering cloud services, creating a truly unique hybrid environment for enterprises to sustain. Securing enterprise IT systems while using CSP or MSP services is challenging since the responsibility for software and hardware security is

split between multiple parties and dependent upon service level agreements (SLAs). It is essential for enterprise leaders and personnel to understand SLAs and review them with their service providers. These agreements outline shared responsibilities, especially in cases of security breaches and incident response times. CSPs and MSPs add new services and tools at a fast pace, so it is often prudent to tailor a cybersecurity program to leverage a range of these services, third-party options, and in-house expertise.

Service providers (CSPs and MSPs) offer an ever-growing range of tools and services, encompassing IT, security, and other functionalities. There are many advantages to using service providers, especially for SMEs, as the fundamental offerings will provide capabilities SMEs are unlikely to be able to design, build, and support by themselves. Service providers can also offer significant cost savings and allow an SME's services to be both scalable and flexible. From an IT and security standpoint, service providers can lighten the load. Their platforms will be updated and maintained regularly, meaning that platform vulnerabilities in servers and other systems will be remediated in a timely manner. Data can be regularly backed up, ensuring business continuity in the face of disruption. Authentication portals will often be well built, be thoroughly tested, and use the latest protocols. In short, there is a lot they have to offer, and as a result, service providers are a popular choice for many enterprises.

CSP and MSP services often satisfy CIS Safeguards across multiple Implementation Groups (IGs) – IG1, IG2, IG3 – or they might fall outside the scope of CIS Controls altogether (e.g., threat intelligence services). Additionally, some services simply might not be relevant or beneficial for every enterprise.

Shown below in Table 3 is a list of offerings, based off of Table 2 above, typically offered by MSPs and CSPs. Research has found that implementation of 100% of IG1 Safeguards can be accomplished by outsourcing services to an MSP. With CSPs, research has found that there is 80% coverage of IG1 simply because policy creation is generally not something a CSP would handle.

To help enterprises with the adoption of one or more CSPs, a listing of tools and services mapped to the three main CSP providers (Amazon, Microsoft, and Google) can be found in [Appendix G](#) of this guide.

Table 3. CSP and MSP Offerings

Category	Tool	CSP	CSP Offering	MSP	MSP Offering
Asset Management	Enterprise Asset Management Policy/Process		Tracking and managing all the enterprise assets within a cloud environment, helping enterprises maintain visibility over their resources	●	Write security program policies. Track and manage enterprise assets within scope. Create a vendor inventory and conduct risk monitoring.
	Enterprise and Software Asset Management Tool	●		●	
	Software Asset Management Policy/Process			●	
	Service Provider Management Tool			●	
Data Management	Data Management Policy/Process		Data security and data privacy services for discovering, protecting, disposing, and encrypting sensitive data.	●	Write security program policies. Data security and data privacy services for discovering, protecting, disposing, and encrypting sensitive data.
	Data Management Tool	●		●	
	Data Disposal Tool	●		●	
	Encryption Tool	●		●	

Category	Tool	CSP	CSP Offering	MSP	MSP Offering
Secure Configurations	Secure Configuration Policy/Process		Tools that can be used to automatically deploy custom images that are pre-hardened to a set of secure configurations, or measure against a set of secure configurations to identify areas of improvement to meet specific standards. Additionally, firewalls that monitor, and control incoming and outgoing network traffic based on predetermined security rules.	●	Write security program policies. Conduct initial assessments to establish a initial baseline of configurations and harden settings to establish a secure baseline.
	Configuration Management Tool	●		●	
	Firewall	●		●	
Account and Access Control Management	Account and Credential Management Policy/Process		Managing user identities and controls access to company resources, ensuring that only authorized users can access specific data and applications.	●	Write security program policies. Managing user identities and controls access to company resources, ensuring that only authorized users can access specific data and applications.
	Identity and Access Management Tool	●		●	
	Password Management Tool	●		●	
	Multi-Factor Authentication Tool	●		●	
Vulnerability Management	Vulnerability/Patch Management Policy/Process		Tools to scan for vulnerabilities as well as apply patches within cloud environments. Platforms to easily manage from a security and risk management perspective.	●	Write security program policies. Tools to scan for vulnerabilities as well as apply patches within an enterprise's environment.
	Vulnerability/Patch Management Tool	●		●	
Log Management	Log Management Policy/Process		Collecting, storing, and analyzing logs from various cloud resources, crucial for monitoring, security, and compliance.	●	Write security program policies. Implement a Security Information and Event Management System to collect and store logs from all sources within scope.
	Log Management Tool	●		●	
Malware Defense	Anti-Malware Software	●	Detecting, preventing, and removing malicious software from affecting cloud assets. Additionally, providing DNS resolution services with added protection against malicious activities and attacks.	●	Detecting, preventing, and removing malicious software from enterprise assets. Additionally, providing DNS resolution services with added protection against malicious activities and attacks.
	DNS Service/Server	●		●	
Data Recovery	Data Recovery Policy/Process		Data storage and backup solutions, ensuring data is safe and recoverable in case of loss or corruption.	●	Write security program policies. Data storage and backup solutions, ensuring data is safe and recoverable in case of loss or corruption.
	Data Backup and Recovery Tool	●		●	
Security Training	Security Training and Awareness Policy/Process		Security and other types of training for an enterprise's workforce to take and expand their skillsets, while also earning certifications.	●	Recurring simulated phishing engagements with social engineering training. Additional security awareness topics available.
	Security Training and Awareness Tool(s)	●		●	
Incident Response	Incident Response Planning		—	●	Write security program policies.

Our research found that CSP and MSP tools and services mapped to multiple Safeguards in part or fully. Similar to a CSP, leveraging the tools and services of an MSP may fulfill many, but not all, of the IG1 Safeguards completely. Understanding and documenting the division of effort will be essential to establish a cybersecurity program in which all IG1 Safeguards are covered.

For example, enterprises using a CSP will likely still have some on-premises systems that are not cloud-based, creating a hybrid environment. Specific examples where a CSP alone may not fully address all of the IG1 Safeguards include:

- **Asset Management:** It will be difficult for all the inventory requirements from IG1 to be met by a cloud platform (e.g., enterprise assets, software, data, accounts). A CSP can help inventory systems connected to it, but there will inevitably be some portion of the network or some group of devices within an enterprise that the cloud platform is unaware of, such as on-premises devices.
- **Account Management:** Depending on tooling, account management can be performed within or outside of the cloud platform, so it may be difficult for an external entity to create and maintain an account inventory in one centralized place for hybrid environments.
- **Customization:** Some cloud platforms have limited customization and flexibility for users, potentially making it difficult to tailor the platform to their needs as compared to an on-premises solution.

While CSPs and MSPs can be valuable tools in the IT and security tool chest, enterprises must still provide some degree of management and/or support. CIS has released guidance to help enterprises with this challenge. The guide, [Establish Basic Cyber Hygiene Controls Through a Managed Service Provider \(MSP\)](#), can help SMEs ensure that many of their essential cyber hygiene needs are met by their service provider.

Cost

Working off of the generic tools identified in Table 2 above, v1.0 of this guide obtained prices for over 200 IT and/or cybersecurity single-use tools to determine the cost to implement IG1 using the attributes from the [three tier model in Table 1 above](#) as a guide. A wide selection of tools were priced including no-cost, commercially-supported, and open-source tools. Many enterprises reading this guide may be interested in learning more about which tools can be used to implement IG1 Safeguards. While out of scope for this guide, CIS has published an additional guide, [Establishing Essential Cyber Hygiene \(v8.1\)](#), which provides several no-cost and open-source tools for implementing IG1. Additionally, a small list of CIS and MS-ISAC⁷ tools and resources mapped to IG1 can be found in [Appendix E](#) of this guide and on our [website](#).

Shown below in Table 4 are the costs associated with each of the 10 categories. The prices shown reflect the annual cost to implement tools quoted in each category and are organized by no-cost tools, the lowest quoted commercially-supported tool, and the highest quoted commercially-supported tool. Note that these numbers are not averages, but are based on pricing that was obtained from various vendors for single-use tools using the data points from the [IG1 Enterprise Profiles](#). These costs will vary depending on several factors, such as the number of users, the number of devices managed by the enterprise, or if the tool is multipurpose. Costs may also decrease over time as some of the up-front costs may go away after the first year. Other savings may include bulk discounts, industry-specific pricing, and multi-year discounts. Additionally, [Appendix C](#) cautions all enterprises to plan for the costs of obsolescence and other life cycle considerations. Many cyberattacks are successful because an enterprise cannot afford to update enterprise assets or software when needed.

Readers will also notice Table 4 does not identify CSP and MSP pricing. That analysis is addressed separately in the next section below since many service providers combine tools, making them multipurpose, and therefore it is difficult to calculate the costs using the 10 categories shown in Table 2.

7 Multi-State Information Sharing and Analysis Center® (MS-ISAC®)

Table 4. Cost of IG1

Category	Cost Range Tier 1			Cost Range Tier 2			Cost Range Tier 3		
	Max Cyber Budget: \$50,000			Max Cyber Budget: \$500,000			Max Cyber Budget: \$5,000,000		
	No-Cost	Low	High	No-Cost	Low	High	No-Cost	Low	High
Asset Management	\$0	\$556	\$2,044	\$0	\$690	\$3,896	\$0	\$790	\$18,414
Data Management	\$0	\$1,148	\$14,566	\$0	\$11,192	\$41,918	\$0	\$87,027	\$387,867
Secure Configurations	\$0	\$968	\$9,008	\$0	\$4,710	\$47,494	\$0	\$18,138	\$269,263
Account and Access Control Mgmt.	\$0	\$1,579	\$4,025	\$0	\$7,063	\$39,240	\$0	\$29,412	\$388,728
Vulnerability Management	\$0	\$345	\$1,969	\$0	\$845	\$7,200	\$0	\$5,285	\$64,746
Log Management	\$0	\$88	\$2,520	\$0	\$632	\$10,866	\$0	\$3,543	\$54,000
Malware Defense	\$0	\$452	\$1,399	\$0	\$5,591	\$10,799	\$0	\$44,870	\$107,898
Data Recovery	\$0	\$650	\$2,143	\$0	\$2,925	\$11,888	\$0	\$28,275	\$118,701
Security Training	\$0	\$120	\$450	\$0	\$1,440	\$3,660	\$0	\$3,420	\$36,570
Incident Response	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
TOTAL	\$0	\$5,906	\$38,124	\$0	\$35,088	\$176,961	\$0	\$220,760	\$1,446,187

Based on the findings shown in Table 4 and in looking back at the IG1 Enterprise Profiles, it is evident that IG1 can be implemented for a relatively low cost when compared to the wide coverage of attacker techniques that it can defend against. Enterprises are reminded that while these costs appear to be well below the maximum cybersecurity budget, other costs⁸ will also need to be accounted for, in addition to the cost of the tool alone.

CSP and MSP Costs

The cost of CSP and MSP services is dependent upon a variety of factors. This includes the number of end-users supported, number of endpoints supported, applications, and scope of services. For more in-depth practitioner-level information on these factors and services see [Appendix H](#) and the accompanying [spreadsheet](#). The costs shown in Table 4 above illustrate what an enterprise could spend on on-premises tools. When introducing service providers, such as CSPs and MSPs, the costs become increasingly complex to calculate. Often, CSP and MSP pricing is highly dependent on the enterprise's environment, especially when it comes to the volume of data being accessed, stored, or transmitted to a service provider.

Further complicating pricing structures is that no two CSPs or MSPs offer the exact same set of services, even though they may have similar names or business objectives. For the costs illustrated in this guide, CIS used publicly available data for popular CSPs and MSPs to estimate costs for IG1 enterprises. Since MSPs and CSPs offer a variety of different IT and security tools, this accounted for a wide range of pricing when calculating MSP and CSP costs.

This cost comparison is complicated due to the reasons explained above; however, in Table 5 below, we include an example set of cost ranges for each of the three tiers to demonstrate possible costs based on the size and complexity of an enterprise. Additionally, it is worth noting that since much of the MSP and CSP tools and services will heavily fall under the IT budget in a typical enterprise, these costs should be compared against the maximum IT and/or cybersecurity budgets shown in Table 5 below and not solely compared to the maximum cybersecurity budget. This is promising as IT budgets are comparatively much larger than cybersecurity budgets.

⁸ Other costs include those associated with labor, tool updates, physical hardware or virtual assets, training, license renewals, integration, testing, consulting, advertising, and more. These costs are much more difficult to calculate in a general sense and therefore were not included in the cost calculations shown in this guide. However, the absence of these cost estimates does not diminish their importance when creating a budget.

Table 5. CSP and MSP Costs (as compared to on-premises tooling)

	Tier 1 min.	Tier 1 max.	Tier 2 min.	Tier 2 max.	Tier 3 min.	Tier 3 max.
Max. Cybersecurity Budget	\$50,000		\$500,000		\$5,000,000	
Max. IT Budget	\$250,000		\$2,500,000		\$25,000,000	
On-Premise Tools (Costs from v1.0)	\$5,906	\$38,124	\$35,088	\$176,961	\$220,760	\$1,446,187
MSP Pricing	\$23,000	\$41,000	\$44,000	\$200,000	\$208,000	\$1,800,000
CSP Pricing (Low Data Usage)	\$23,000	\$47,000	\$94,000	\$222,000	\$246,000	\$1,600,000
CSP Pricing (High Data Usage)	\$26,000	\$255,000	\$255,000	\$2,000,000	\$2,000,000	\$16,000,000

Tier 1 IG1 enterprises should expect to spend about \$23,000 - \$255,000 annually on CSP services or \$23,000 - \$41,000 on MSP services and their baseline security offerings, which will fulfill most of the IG1 Safeguards. Estimated costs for Tier 2 and 3 enterprises leveraging a CSP and/or MSP for their IT and cybersecurity programs can be seen in Table 5 above as well. Understanding the roles, responsibilities, and agreements between a service provider and enterprise are essential to establishing an IT and cybersecurity program in which all IG1 Safeguards are covered to the fullest extent possible.

Conclusion

Our findings reinforce that the Safeguards in IG1 can be implemented for a relatively low cost and are a foundational and achievable set of security actions for even the smallest of enterprises. Additionally, enterprises can implement IG1 and defend against a wide array of threats with a relatively small number of tools. Many cyber insurers are beginning to insist that many of the Safeguards in IG1 be implemented as a requirement for coverage. In return, enterprises rightfully expect to receive a discount on their coverage compared to those enterprises that do not implement these defenses.

Our additional findings in this updated guide further reinforce the complexity of CSP and MSP costing considerations when incorporating them into IT and cybersecurity budgets. Despite the variables that each individual enterprise needs to evaluate, we have provided a starting point to forecasting the tools and services required, as well as the costs associated with the implementation of IG1 Safeguards in hybrid environments. Our research shows that obtaining and deploying on-premises versions of the tools, using a CSP and/or an MSP, or a combination of all three should be less than the IT budget (5% of annual revenue) and/or cybersecurity budget (20% of the IT budget) set forth by an IG1 enterprise of any size.

We believe that the CIS Controls are the first security framework to publish a mapping of costs associated with implementing our framework. In the future, we will seek to refine our findings based on industry feedback and advancements in technology to expand the scope of what our community seeks to know. For example, "Which IG1 tools can be used to implement IG2 and IG3 Safeguards?" This guide is a starting point to answer this and many more questions that enterprises want answered when implementing defenses. As with many other initiatives we are involved in, we will use the data from this project to inform Safeguard prioritization within the IGs and update the Controls and/or Safeguards, where appropriate.

The most important thing is that enterprises start now. Do not wait to become a victim of a breach or incident. Use the information in this guide to help make informed and prioritized decisions to get the defenses in place before an incident occurs.

Appendix A

The 10 Areas of Cyber Defense

In this section, the Safeguards are broken out into 10 areas of activity. Each area will require a policy and/or process, which is essentially a document outlining who will carry out the actions and be accountable for doing so. Some enterprises will outsource some security management to an MSP or a CSP. Many of these activities will be performed by personnel as additional activities. For example, there should be a strict policy about who can install enterprise assets or software, and there should be a process for ensuring that additional software or enterprise assets are tracked in an inventory. The costs in the sections below mirror those from Table 4 above, Cost of IG1. They are representative of the wide sampling of tools investigated for this guide.

Asset Management

To satisfy the IG1 Safeguards listed in Asset Management, enterprises will need to create policies for both enterprise and software asset management. Many asset management tools generally track both enterprise and software assets. However, due to the unique requirements to manage both enterprise and software assets, the policies themselves are generally kept separate, which is why two separate policies are listed in the table below. Additionally, many tools will incorporate a contract management solution within their platform. If this is the case, it can satisfy Safeguard 15.1 – “Establish and Maintain an Inventory of Service Providers.”

Common tool names in the asset management category may vary. Some alternative tool names that an enterprise may come across during procurement include: helpdesk software, IT asset management (aka ITAM) tool, IT inventory management tool, network inventory and discovery, and network IP (Internet Protocol) scanner.

Tool	Safeguards						
Enterprise Asset Management Policy/Process	1.1						
Enterprise and Software Asset Management Tool	1.1	1.2	2.1	2.2	2.3	9.1	12.1
Software Asset Management Policy/Process	2.1						
Service Provider Management Tool	15.1						

Considerations

When procuring tools to perform enterprise and software asset inventory, tool options can range anywhere from a spreadsheet all the way up to a fully automated tool. It is up to the enterprise to determine what type of tool best fits their needs. Some items to consider when implementing Safeguards in the Asset Management category include:

- Does the enterprise have an asset management policy (for both enterprise and software assets)?
- How many assets does the enterprise have on their network approximately?
- Are there any assets that are classified as BYOD (Bring Your Own Device)?
- Are there remote assets connected to the network (e.g., mobile or portable end-user devices)?
- What type(s) of environment(s) are the assets in (e.g., on-premises, cloud, hybrid)?
- Is there an additional tool that is required to completely automate the process? For example, if the enterprise gets a network scanner, will it only export results into a spreadsheet or can results be imported into a database or other data repository?

- Does the tool perform other functions (e.g., vendor/contract management, establishing secure configurations, vulnerability management)?
- Is the tool agent-based or agentless?
- Does the tool track both enterprise and software assets?

Cost

Many asset management tools will inventory both enterprise assets as well as software assets. This is key when it comes down to pricing. However, there may be some tools an enterprise selects that only manage one or the other. If this is the case, then two separate tools would need to be procured. Additionally, some asset management tools will also have the ability to manage service providers and other vendors. This is another item to consider when procuring asset management tools.

Based on the considerations listed above, an enterprise can opt to go with no-cost tools all the way up to a licensed and fully automated tool. Whichever tool you choose, keep in mind that every selection has trade-offs. For example, an enterprise with 500+ people will likely not select a tool that is manual, such as a spreadsheet. This could result in a significant amount of time and resources to even get a preliminary inventory, much less to keep it up to date. The best thing to do is select the tool that is most appropriate for the enterprise, while not exceeding costs to the point where no money is left to implement other defenses.

Tool	Cost Range Tier 1			Cost Range Tier 2			Cost Range Tier 3		
	No-Cost	Low	High	No-Cost	Low	High	No-Cost	Low	High
Enterprise Asset Management Policy/ Process	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Enterprise and Software Asset Management Tool	\$0	\$400	\$1,549	\$0	\$195	\$2,600	\$0	\$295	\$15,474
Software Asset Management Policy/ Process	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Service Provider Management Tool	\$0	\$156	\$495	\$0	\$495	\$1,296	\$0	\$495	\$2,940
SUBTOTAL	\$0	\$556	\$2,044	\$0	\$690	\$3,896	\$0	\$790	\$18,414

Data Management

To implement Safeguards within the data management category, a policy must first be put in place surrounding the data management process. Once this policy is created, an enterprise can begin to explore tools that can inventory data. For IG1, we recommend to first focus on sensitive data, as that is the most critical to protect. Once sensitive data is inventoried, less sensitive data may be accounted for. As with most data, eventually it will need to be disposed of. Note that different types of data may have different retention policies that are set either by a regulating body or by the enterprise itself. Some enterprises can simply invest in an appropriate shredder or procure a secure document destruction service. Some enterprises may require special disposal requirements, such as physical destruction or secure wipes of hard drives. Each enterprise's needs will vary.

Along with inventorying and destroying the data, efforts must be made to encrypt the data to protect its confidentiality. Some operating systems will already incorporate an encryption tool. For example, BitLocker is available on Microsoft Windows Professional versions and up. However, it is not available on Windows Home versions. Instead, Windows Device Encryption is available. These differences are important to note as features may vary depending on the software selected. Other options for an enterprise include procuring software outside of the operating system to encrypt and centrally manage device-level encryption. Whichever solution(s) are chosen, ensure that they incorporate all of the elements from the tools shown below.

Common tool names in the data management category may vary. Some alternative tool names that an enterprise may come across during procurement include: governance, risk and compliance (GRC) tool, Data Loss Prevention (DLP) tool, or eDiscovery tool.

Tool	Safeguards	
Data Management Policy/Process	3.1	
Data Management Tool	3.2	3.4
Data Disposal Tool	3.5	
Encryption Tool	3.6	

Considerations

Data management tooling can be tricky. Many vendors do not necessarily advertise their tools as performing data inventory. Rather, due to more legislation around data breach compliance and other laws and regulations, many use a GRC tool to perform their data inventory. Other tools may be advertised as a DLP tool or an eDiscovery platform. Many tools can be used to satisfy these Safeguards; however, it may not be appropriate for an enterprise to procure certain tools that could become extremely costly. Enterprises can instead use something as simple as a spreadsheet to track sensitive data. Some questions to consider when procuring data management tools include:

- Does the enterprise have a data management policy in place?
- What type(s) of data does the enterprise handle?
- Where is that data stored (e.g., file server, database)?
- What is the sensitivity level of the data?
- What type(s) of environment(s) is the data stored in (e.g., cloud, on-premises, hybrid)?
- Is there a process in place for how to dispose of the data? Is a specific tool needed to do so?
- Is device-level encryption available within the operating system itself or is a separate tool required?
- Is tooling already in place to centrally manage encryption? If not, does a tool need to be procured?
- Is the enterprise legally required to comply with certain standards, laws, or regulations?

Cost

The biggest determinant of cost for data management tools is whether it is performed manually or automated with a tool. Additionally, since several different types of tools can be used to inventory data, it is up to the enterprise to select an appropriate tool for their needs. Also consider that some tooling may already be baked into the operating system, such as device encryption.

Tool	Cost Range Tier 1			Cost Range Tier 2			Cost Range Tier 3		
	No-Cost	Low	High	No-Cost	Low	High	No-Cost	Low	High
Data Management Policy/Process	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Data Management Tool	\$0	\$742	\$12,600	\$0	\$6,360	\$28,800	\$0	\$63,547	\$287,760
Data Disposal Tool	\$0	\$129	\$299	\$0	\$2,499	\$3,999	\$0	\$5,999	\$8,995
Encryption Tool	\$0	\$277	\$1,667	\$0	\$2,333	\$9,119	\$0	\$17,481	\$91,112
SUBTOTAL	\$0	\$1,148	\$14,566	\$0	\$11,192	\$41,918	\$0	\$87,027	\$387,867

Secure Configurations

As with most Controls, always start with establishing a secure configuration process by creating a policy. Once that is complete, enterprises will want to determine how to securely configure their devices. This can vary between enterprises. For example, some vendors provide secure configuration guidelines for their software. Other vendors provide none, leaving it up to the enterprise to create their own set of secure configurations. Enterprises can also turn to other trusted sources to obtain secure configuration guidelines, such as those set forth in the CIS Benchmarks®, Defense Information Systems Agency Security Technical Implementation Guides (DISA STIGs), or Microsoft Security Baselines, as examples. Wherever an enterprise decides to obtain these recommendations, ensure that they address basic security tenets, such as removing/disabling default accounts, encryption, logging, and protecting devices that are exposed directly to the internet.

In addition to implementing the secure configurations, this also includes managing configurations in a secure manner. Examples include using version-controlled infrastructure-as-code (IaC) and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS).

Another important area to focus on when securing an enterprise's network is a firewall. This includes implementing a firewall for end-user devices and servers, which may be protected with different types of firewalls (e.g., host-based firewall, virtual firewall, third-party firewall agent). Additionally, securely configuring the firewall is equally important. This means using the trusted secure configurations mentioned previously to protect it.

Common tool names in the secure configuration category may vary. Some alternative tool names that an enterprise may come across during procurement include: configuration assessment/management, endpoint management, or configuration settings.

Tool	Safeguards						
Secure Configuration Policy/Process	4.1	4.2					
Configuration Management Tool	4.1	4.2	4.3	4.6	4.7	5.4	10.3
Firewall	4.4	4.5					

Considerations

Establishing secure configurations can be tricky, depending on how the enterprise chooses to deploy them. For example, recommendations can be deployed manually from workstation to workstation. For a 10-endpoint enterprise, that may not be a heavy lift. However, for an enterprise with 100+ endpoints, that may be an insurmountable task to deploy and maintain, even for the most skilled person. Some considerations to keep in mind when implementing these Safeguards include:

- Does the enterprise have a secure configuration policy in place?
- What type of deployment does the enterprise want (e.g., manual, fully-automated, semi-automated)?
- What environment(s) need to be securely configured (e.g., on-premises, cloud, hybrid)?
- Are there vendor-provided secure configurations or are they provided by a third-party?
 - Is the third-party reputable?
- Does the enterprise have a set of security configurations that are considered “baseline”?
- How does the enterprise plan on tracking configuration changes to the baseline?
- How will the secure configuration be validated and maintained?
- Does the enterprise need to comply with standards or regulations surrounding secure configurations?
- Can the tool deploy configurations automatically, centrally, remotely?

Cost

Configuration management tool costs will differ depending on the type of deployment that the enterprise needs. When selecting the tool, ensure that it is able to ingest the configuration settings that the enterprise needs, whether manually or automatically. If automation is desired, inquire if it can deploy and be managed centrally and/or to remote devices.

Additionally, firewalls can vary in price. For example, some operating systems have host-based firewalls embedded into the platform. However, servers may require a different level of protection. This may require the purchase of both software and physical hardware.

Tool	Cost Range Tier 1			Cost Range Tier 2			Cost Range Tier 3		
	No-Cost	Low	High	No-Cost	Low	High	No-Cost	Low	High
Secure Config. Policy/Process	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Configuration Mgmt. Tool	\$0	\$468	\$3,990	\$0	\$2,400	\$31,800	\$0	\$14,376	\$189,263
Firewall	\$0	\$500	\$5,018	\$0	\$2,310	\$15,694	\$0	\$3,762	\$80,000
SUBTOTAL	\$0	\$968	\$9,008	\$0	\$4,710	\$47,494	\$0	\$18,138	\$269,263

Account and Access Control Management

As with the other categories, it is best practice to start with establishing an access and credential management policy. Next, ensure that a process is in place for granting and revoking accounts and privileges. Some of this can be done with tooling, but putting a process in place is imperative to instruct personnel on what to do and when to do it. This is especially important with privileged accounts (e.g., administrator). Ideally, enterprises should restrict administrator privileges to dedicated administrator accounts.

Enterprises may find that one tool or several tools may be needed to manage accounts. Additionally, common tool names in the account and access control management category may vary. Some alternative tool names that an enterprise may come across during procurement include: Identity and Access Management (IAM) tool, Privileged Access Management (PAM), account discovery tool, identity management, user management, password manager, or two-factor authentication.

Tool	Safeguards			
Account and Credential Management Policy/Process	6.1	6.2		
Identity and Access Management Tool	3.3	5.1	5.3	5.4
Password Management Tool	5.2			
Multi-Factor Authentication Tool	6.3	6.4	6.5	

Considerations

Account and access control management can be achieved through a number of different tools. Some may even overlap in functionality, performing configuration management, credential management (including multi-factor authentication (MFA)), and/or single sign-on (SSO).⁹ Each tool will have different degrees of functionality, which can also translate to a higher or lower cost. For example, Microsoft Active Directory can be used to push configuration changes via Group Policy Objects (GPOs), keep inventory of user accounts, and control access to

⁹ <https://www.cisecurity.org/insights/blog/authentication-and-authorization-using-single-sign-on>

certain files or directories, among other functions. However, some enterprises may find that third-party tooling is needed to integrate other functions that might not be directly covered by Active Directory (e.g., MFA). Some questions to consider when implementing Safeguards in account and access control management include:

- Does the enterprise have a policy in place for account and access management?
- How many accounts does the enterprise currently manage?
- Which type(s) of accounts are they (e.g., service, user, administrator)?
- Which accounts require administrative privileges?
- What type(s) of environment(s) does the enterprise have accounts in (e.g., on-premises, cloud, hybrid)?
- Does the enterprise have a process in place for managing accounts and access controls upon onboarding and offboarding?

Cost

Costs for tools relating to account and access control management can range significantly depending on the features and functionality of the tool. Additionally, costs can vary depending on how many accounts the enterprise manages, with some commercially-supported tools offering full access at no cost for up to a certain number of accounts. Other tools may already be integrated into the software itself, such as Microsoft Active Directory.

Tool	Cost Range Tier 1			Cost Range Tier 2			Cost Range Tier 3		
	No-Cost	Low	High	No-Cost	Low	High	No-Cost	Low	High
Account and Credential Management Policy/Process	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Identity and Access Management Tool	\$0	\$595	\$1,630	\$0	\$595	\$21,600	\$0	\$1,104	\$216,000
Password Management Tool	\$0	\$480	\$1,387	\$0	\$4,788	\$9,000	\$0	\$11,508	\$86,400
Multi-Factor Authentication Tool	\$0	\$504	\$1,008	\$0	\$1,680	\$8,640	\$0	\$16,800	\$86,328
SUBTOTAL	\$0	\$1,579	\$4,025	\$0	\$7,063	\$39,240	\$0	\$29,412	\$388,728

Vulnerability Management

A vulnerability management process is best established by first creating a policy. Once the policy is established, it can be operationalized. Additionally, a remediation process should be put into place to determine how often remediation should occur and how patches should be prioritized. For example, a patch with a risk rating of "HIGH" that is assigned by the vendor, may be prioritized, if the patch is applicable to the enterprise. As patch management is a subset of vulnerability management, some tools may also include services such as vulnerability scanning, whereas other tools may only perform patch management. Note that vulnerability scanning is out of scope for an IG1 enterprise; however, it may be appropriate for the enterprise to implement if they move into an IG2 or IG3.

Common tool names in the vulnerability management category may vary. Some alternative tool names that an enterprise may come across during procurement include: vulnerability management, endpoint/client management, or automatic updates.

Tool	Safeguards
Vulnerability/Patch Management Policy/Process	7.1
Vulnerability/Patch Management Tool	7.2 7.3 7.4

Considerations

Patch management can be a complex process. Tooling is one part of the process; however, the other part is dependent on time and resources to push out the patches. As with many of these controls, keeping up with a regular cadence (e.g., monthly) will help to stay on top of patches. Of course, there are times when a patch may need to be pushed out sooner rather than later. It is worth noting that most vendors have some kind of prioritization schema (e.g., low, medium, high) to classify a patch's level of urgency. However, each enterprise will need to determine if the patch is applicable to their specific enterprise and if it is appropriate to implement, as not all patches can or should be deployed. For example, a patch that is for a technology not used by the enterprise or a patch that would adversely impact the system's functionality may not be deployed. However, for a patch that is categorized as high, the IT team may consider patching outside of the regular cycle to reduce the risk of exploitation to the enterprise. Some considerations to keep in mind when implementing Safeguards for patch management include:

- Does the enterprise have a vulnerability management policy already in place?
- How many devices does the enterprise currently have that will need regular patches?
- Are there legacy systems that may be affected during the patch management life cycle?
 - Should/can those systems be rebuilt to receive patches?
 - If not, what compensating controls need to be in place to reduce the risk of exploitation?
- Will patches be deployed manually or automated?
- Will patches be deployed and centrally managed?
- Can patches be pushed to remote devices?
- What type(s) of environments are being managed (e.g., cloud, on-premises, hybrid)?
- Is the tool that is being considered a multipurpose tool (e.g., also performs vulnerability management)?
- How often will the enterprise deploy patches?
- Can the enterprise detect if a patch has not been applied (via a tool)?
- Will patches be tested prior to deployment? If so, which ones should be tested and where will they be tested (e.g., testing environment)?
- What time of day will patches be deployed?
- What type of communication, if any, will be sent out to personnel notifying them of the patches?

Cost

Automation or lack thereof will significantly affect cost. By procuring tooling to automate the patch management process, an enterprise can have significant cost savings in labor; however, the tool itself will likely be at a higher price point. Alternatively, if an enterprise chooses to deploy patches manually (e.g., for a 10-device enterprise), they may have cost savings on tooling but spend more on labor, depending on how long it takes to patch each system. Each enterprise's needs will be different.

Tool	Cost Range Tier 1			Cost Range Tier 2			Cost Range Tier 3		
	No-Cost	Low	High	No-Cost	Low	High	No-Cost	Low	High
Vulnerability/Patch Management Policy/Process	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Vulnerability/Patch Management Tool	\$0	\$345	\$1,969	\$0	\$845	\$7,200	\$0	\$5,285	\$64,746
SUBTOTAL	\$0	\$345	\$1,969	\$0	\$845	\$7,200	\$0	\$5,285	\$64,746

Log Management

Starting off with a log management policy to inform tooling/personnel is always the best bet, as we have discussed throughout this guide. Once the policy is in place, the log management tool can be selected. As previously mentioned, log management tools will vary greatly from the way that other tools are procured, mostly based on usage (e.g., MB, GB). However, when moving from on-premises to cloud, they are generally priced in similar ways, since the cloud is also based on usage. Setting retention limits and determining a log storage solution are also key when it comes to log management. An enterprise does not want to run into a scenario where logs are only being stored for 30 seconds!

Common tool names in the log management category may vary. Some alternative tool names that an enterprise may come across during procurement include: event log manager, security information and event management (SIEM), and security information management (SIM).

Tool	Safeguards	
Log Management Policy/Process	8.1	
Log Management Tool	8.2	8.3

Considerations

Costing out log management tools is unique as compared to most other tools within this guide, in that they are commonly priced based on the size of logs ingested. Which logs to collect is also an important consideration here, as collecting a large number of less impactful logs may drive up the size and cost. Additionally, the length of time the logs are stored may also play a role in cost. Log retention is a tricky detail to get “right.” Store logs for too long and they may never be needed. Store logs for too short a time and the value of information contained within them may not be helpful to draw any type of conclusion. Some questions to ask when implementing log management Safeguards include:

- Which assets should the enterprise collect logs from?
- What type(s) of logs should the enterprise “turn on”?
- Which logs are required for regulatory, legal, or contractual reasons?
- What is the approximate size of the logs?
- How much space will be needed to store the logs?
- Will the logs be stored on the system itself or sent to a centralized logging server?
- Will the logs be stored on-premises or in the cloud?
- Who should have access to view/modify the logs?
- Does the enterprise need a disaster recovery plan in the event the log server is compromised?
- What log information needs only to exist short-term and what needs to remain longer?

Cost

Costs will vary greatly depending on the size of the logs ingested into the tool, the size of the logs being stored/retained, the length of time they are stored, and where they are being stored (e.g., on-premises, cloud, off-site). Additionally, if logs are backed up to multiple locations, this will also affect the cost.

Tool	Cost Range Tier 1			Cost Range Tier 2			Cost Range Tier 3		
	No-Cost	Low	High	No-Cost	Low	High	No-Cost	Low	High
Log Management Policy/Process	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Log Management Tool	\$0	\$88	\$2,520	\$0	\$632	\$10,866	\$0	\$3,543	\$54,000
SUBTOTAL	\$0	\$88	\$2,520	\$0	\$632	\$10,866	\$0	\$3,543	\$54,000

Malware Defense

There are two main tools used in malware defense: anti-malware software and a Domain Name System (DNS) service. The most important thing to keep in mind is that malware defenses are most efficient when executed using automated tooling. Automation allows anti-malware software to respond more quickly to detected threats, allowing more time for the enterprise to respond, and recover from a potential incident. Additionally, regardless of the tool that is procured, ensure that it receives regular updates (e.g., signature updates) so that it can detect the latest malware variants.

DNS service is a fairly simple tool that can be implemented by changing the DNS servers to point to a reputable vendor¹⁰ (e.g., Quad9, OpenDNS) that can block DNS requests that reach out to known malicious sites. It is worth noting that there are also DNS services/tools that can offer more granular control and contain reports and analytics for the enterprise to use. These fall out of the scope for an IG1 enterprise, but may be valuable for your enterprise.

Common tool names in the malware defense category may vary. Some alternative tool names that an enterprise may come across during procurement include: anti-virus, endpoint detection and response (EDR), endpoint protection platform (EPP), or endpoint security services (ESS).

Tool	Safeguards	
Anti-Malware Software	10.1	10.2
DNS Service/Server	9.2	

Considerations

Anti-malware software is one of the most popular malware defense tools. However, no two pieces of anti-malware software will operate in the same way. In order for malware to be detected, it needs to have some type of indicator for it to trigger on. For an IG1 enterprise, anti-malware software that is signature-based is the minimum requirement. However, some enterprises may consider using behavior-based anti-malware software if their enterprise warrants it. Some commonplace names for behavior-based anti-malware software may include EDR or EPP. When it comes to implementing malware defense Safeguards, these are some questions that an enterprise should consider:

- What types of threats is the enterprise at risk for?
- Does the enterprise need/want a cloud-based or on-premises tool?
- Does the enterprise have a process in place to instruct personnel what to do when potentially malicious activity is suspected and/or detected?
- Does the tool detect threats based on signatures, behaviors, or both?
- Is the anti-malware software centrally managed?
- Can the anti-malware software be managed on remote devices?

Cost

Costs will vary with these tools based on the functionality of the software and the enterprise's needs. For example, if the enterprise chooses to procure an EDR solution as compared to a traditional, signature-based anti-malware solution, the price will be vastly different. Alternatively, if the enterprise chooses to use a no-cost solution, they may have trade-offs such as limited signature updates or poor detection rates. The key here is that the enterprise should procure a tool that is appropriate to detect the risks applicable to them. If an enterprise is a small 10-device shop that sells flowers, then procuring an EDR solution may not be appropriate. However, if that 10-device shop is actually a provider of IT services to other enterprises, then perhaps it is appropriate depending on the offerings

¹⁰ The information about vendors contained in this publication do not constitute endorsement, recommendation, or favoring by CIS. It is your responsibility to verify and investigate vendors and services. CIS assumes no liability of any kind for the use of any vendors mentioned in this publication.

to the clients. Likewise, with the DNS tooling, if an enterprise simply chooses to use a reputable vendor's DNS servers, then the cost is generally no-cost minus the labor to push out the change. However, if the enterprise chooses to procure a tool to manage DNS requests at an enterprise level, then the cost will go up.

Tool	Cost Range Tier 1			Cost Range Tier 2			Cost Range Tier 3		
	No-Cost	Low	High	No-Cost	Low	High	No-Cost	Low	High
Anti-Malware Software	\$0	\$150	\$979	\$0	\$2,999	\$7,199	\$0	\$18,971	\$71,928
DNS Service/Server	\$0	\$302	\$420	\$0	\$2,592	\$3,600	\$0	\$25,899	\$35,970
SUBTOTAL	\$0	\$452	\$1,399	\$0	\$5,591	\$10,799	\$0	\$44,870	\$107,898

Data Recovery

Tooling for data recovery can be achieved with two main tools – a policy/process and a data backup and recovery tool. Data backup and recovery tool pricing can vary depending on how they are structured (e.g., on-premises via network segmentation, off-site, cloud), how long the backups are kept, the types of backups (e.g., full, incremental), and the size of the backups, among other factors. In addition to having a backup tool, the enterprise should ensure that it can perform encrypted backups and that infrastructure is in place to keep the backups isolated from the enterprise environment.

Common tool names in the data recovery category may vary. Some alternative tool names that an enterprise may come across during procurement include: backup software, backup manager, data recovery, or backup and recovery software.

Tool	Safeguards		
Data Recovery Policy/Process	11.1		
Data Backup and Recovery Tool	11.2	11.3	11.4

Considerations

Selecting a tool to perform data backup and recovery is one of the most important areas that an enterprise should focus on. If all other controls fail, having (or not having) a backup could make or break an enterprise. When implementing a backup solution, keep in mind how the network is structured and where the backups lie within that network. For example, some enterprises may choose to store their backups in the cloud. However, remember that cloud infrastructure might be tied to the enterprise's main network, depending on how it is set up. If they are not kept separate (e.g., through network segmentation or other means), it is possible that the backups an enterprise once relied on will also become encrypted. Some questions to consider when implementing data recovery Safeguards include:

- Does the enterprise have a data recovery policy already in place?
- How many devices does the enterprise need to back up?
 - What is the sensitivity level of the data contained on the devices?
- How often should backups be executed on the devices?
- What type(s) of backups does the enterprise want to make (e.g., full, incremental)?
- Where will the backups be stored (e.g., off-site, cloud, on-premises in a different network segment)?
- How much space is needed to store the backups?
- How long will backups be kept?
- Will backups be centrally managed?

- Is there version control for the backups?
- Can backups be run on remote devices?
- Will backups be run automatically or manually?

Cost

Costs will range from no-cost backup tools that could already be embedded into the operating system, to an entirely separate platform used to manage the backup process. The cost will also vary depending on whether the backups run automatically or if they need to be manually performed. For example, a small office home office (SOHO) or micro enterprise will likely be able to back up a small number of systems manually, if that is their only option. However, an enterprise of 100+ systems may find that type of manual task to be extremely difficult to complete on a regular basis. The amount of storage needed will also need to be factored into the cost, as some tools include a small amount of storage in their price, and other tools will price it à la carte.

Tool	Cost Range Tier 1			Cost Range Tier 2			Cost Range Tier 3		
	No-Cost	Low	High	No-Cost	Low	High	No-Cost	Low	High
Data Recovery Policy/Process	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Data Backup and Recovery Tool	\$0	\$650	\$2,143	\$0	\$2,925	\$11,888	\$0	\$28,275	\$118,701
SUBTOTAL	\$0	\$650	\$2,143	\$0	\$2,925	\$11,888	\$0	\$28,275	\$118,701

Security Training

As with most other categories, having a policy in place is important when it comes to establishing a security training and awareness program. The “tool” itself can actually come in various forms. There are so many no-cost resources (e.g., videos, links, articles, online exercises) available online that many enterprises don’t actually have to spend a large sum of money to educate their personnel on cybersecurity.

Tool	Safeguards							
Security Training and Awareness Policy/Process	14.1							
Security Training and Awareness Tool(s)	14.2	14.3	14.4	14.5	14.6	14.7	14.8	

Considerations

When selecting a tool or set of resources, ensure that they cover the following areas: social engineering, authentication best practices, data handling best practices, how to recognize and report security incidents, how to spot potential vulnerabilities (e.g., device not receiving updates), and the dangers of connecting an enterprise asset to an insecure network. These topics should be considered the baseline and enterprises are encouraged to expand the scope based on the enterprise’s needs. Some questions to ask when implementing security training Safeguards include:

- Does the enterprise have a security training and awareness policy already in place?
- How many people does the enterprise employ?
- Will third-party vendors and service providers also require training?
- Will the training be conducted on-site, virtual, or both?
- Are there any positions (e.g., executives, IT administrators, developers) that require additional skills training?
- Will the enterprise be using no-cost tools or a commercially-supported tool that provides a wide variety of training materials and reports in one platform?

- How often will the training program take place (e.g., annually)?
- Who will conduct the training (e.g., internal personnel, a third-party)?
- Are there reports and dashboards available within the tool?

Cost

Costs can vary widely depending on whether this security training is handled internally or whether no-cost or commercially-supported tools are used to implement these Safeguards. There are many good resources, both online and in-person, for security awareness programs. Depending on which skills the enterprise has internally, it might also make sense for them to put together their own program. As the allocated time to produce a security training program may be labor-intensive, consider that when factoring in costs. It might be worth outsourcing some of the work depending on the availability and skillsets of personnel.

Tool	Cost Range Tier 1			Cost Range Tier 2			Cost Range Tier 3		
	No-Cost	Low	High	No-Cost	Low	High	No-Cost	Low	High
Security Training and Awareness Policy/Process	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0	\$0
Security Training and Awareness Tool(s)	\$0	\$120	\$450	\$0	\$1,440	\$3,660	\$0	\$3,420	\$36,570
SUBTOTAL	\$0	\$120	\$450	\$0	\$1,440	\$3,660	\$0	\$3,420	\$36,570

Incident Response

There are some elements that IG1 enterprises should do during incident response planning, at a minimum. This includes activities such as designating personnel to manage incident handling, establishing a contact list in the event of an incident, and establishing a process for reporting incidents. All of these elements can contribute to a strong incident response policy, an IG2 Safeguard, should the enterprise decide to go above and beyond to create a policy/process. However, if the enterprise chooses to do the minimum, these can easily be achieved without tooling and would only require time to put the above activities in place.

Tool	Safeguards		
Incident Response Planning	17.1	17.2	17.3

Considerations

- When incident response planning, the following should be considered:
- Will internal personnel or a third-party be responsible for managing incidents?
- Who will need to be contacted in the event of an incident (e.g., legal, human resources, IT, communications/public relations, law enforcement)?
- How will personnel report an incident (or suspected incident)?
- How will the above information be communicated to personnel?
- How quickly must backups be usable and available?

Cost

As there is no formal tooling associated with incident response planning, no costs are associated with this category. Much of the cost will be associated with time (e.g., labor costs).

Appendix B

Some Observations on Tool Types

The type of tool that an enterprise selects will largely depend on the needs of the enterprise and what is within their limits (e.g., budget, resources, time). There are several types of tools in the industry including no-cost, commercially-supported, and open-source. Regardless of the tool that is selected, enterprises should weigh the risks and benefits of each of them prior to procurement.

For example, an enterprise may choose to use open-source software because they want to save on the cost of tooling. It is often misconstrued that open-source software is “free.” It may be true that the code or software is free; however, implementing open-source software can become as costly as a commercially-supported tool, as the cost of hardware, consulting fees, and other third-party software may be required for it to be fully operational. The benefit is that it can be highly customizable in an environment and is transparent, allowing the enterprise to examine the code completely should they choose to do so.

No-cost tools are another popular option that enterprises may choose to use, but no-cost tools can come with risks. Some no-cost tools may not regularly publish updates or patches or can have advertisements or add-ons embedded in the software, leaving the enterprise vulnerable to a cyberattack. The benefit of no-cost tools is just that – they are no-cost! For many enterprises that are not allocated a cybersecurity budget or have very small budgets, going with no-cost tools to implement some Safeguards may be the best option.

Commercially-supported tools offer benefits such as licensing, graphical user interfaces (GUIs), more formalized release schedules for updates, support for multiple platforms, and End-User License Agreements (EULAs) to help protect the rights of the owner (e.g., the enterprise). Commercial tools may also help to cut down on development time that is likely unavoidable with open-source software.

It is also important to consider that the enterprise may already have the tools in place (or can easily add on to preexisting platforms) to implement some of the Safeguards in IG1. For example, enterprises using Microsoft products may already have the built-in or added capabilities to achieve many of these actions (e.g., BitLocker, Active Directory).

Enterprises may also consider other items during tool selection, such as whether the implementation process is manual or automated. For example, an enterprise may choose to use a spreadsheet to track enterprise assets and software. However, as that enterprise grows, they may have to make the decision to move to an automated tool for inventory, adding to the cost.

No matter which tool is selected, they all come with a cost. If an enterprise chooses to select all no-cost or open-source software, they may be spending more on vulnerability management or labor to ensure that the software is safe to use. On the other hand, if an enterprise chooses to use a commercially-supported tool, they may be spending more on renewal costs, support costs, or integration costs. It is important not to get distracted with the tool and instead, focus on the activity. Enterprises can then find the tool that best fits their needs. In [Appendix A](#) of this guide, all of the 10 categories contain several questions the enterprise can consider that can help jump-start the process of implementing processes and tooling in IG1 (essential cyber hygiene).

Appendix C

Life Cycle Considerations

It is critical to budget for the life cycle costs of cybersecurity brought on by advances in IT, software depreciation, and the need for additional training. Survey your inventory of software and enterprise assets. What will eventually need replacing or updating? It is not uncommon to determine that software needs to be re-sourced from a different vendor or rebuilt on a new server. Some costs cannot be postponed or put on a schedule, such as costs resulting from a major vulnerability in a third-party tool or critical application.

Ask important questions. Has the vendor indicated the last support date? If the software was developed in-house, do you have the source code and the technical support to make feature and security changes? It is imperative to make allowance for these anticipated and unforeseeable life cycle costs into your IT and cybersecurity budgets. It is far too easy to rationalize away the need to replace unsupported software or enterprise assets when no planning has been done for obsolescence or inadequacy.

Software from any source often has open-source components. Make certain to know if your software does – and which ones it has – so that security updates can be made when serious flaws are found. Ideally, track these open-source components in your inventory of software and enterprise assets. Do not develop or procure software that cannot be supported with security updates.

Assess the true cost of your cybersecurity tools.

Commercially-supported tools should come with documentation, be compatible with your platforms and software, and provide a clear promise of how long the tools will be supported. Ask questions about whether tools can be managed centrally and with what security credentials. Will security updates be included in the price? Many platforms have versions of the needed security tools integrated into their platform. Assess what are the advantages of a competing third-party product. It might be that their product is more compatible with another platform. Consider the security training of your personnel. What expertise do they already have, and what will it take to come up to speed on another tool?

If your enterprise falls under a compliance regimen, such as General Data Protection Regulation (GDPR) or Payment Card Industry Data Security Standard (PCI DSS), check their websites for the security policies that need to be in place and the features that are needed in the security tools to support them. If you have cyber insurance, reach out to your insurer to find out which tools they recommend. Ask what discounts are available for implementing the Safeguards in IG1 and for deploying those tools. If you are looking to select cyber insurance, try to find coverage that factors in your efforts to put in place good security practices. How will the insurer help if there is an incident? Both the insurer and insured benefit if a small amount is spent upfront to prevent an attack or make recovery less expensive.

Appendix D

IG1 Safeguards

CIS Control	CIS Control Title	CIS Safeguard / Title	
Control 1	Inventory and Control of Enterprise Assets	1.1	Establish and Maintain Detailed Enterprise Asset Inventory
		1.2	Address Unauthorized Assets
Control 2	Inventory and Control of Software Assets	2.1	Establish and Maintain a Software Inventory
		2.2	Ensure Authorized Software is Currently Supported
		2.3	Address Unauthorized Software
Control 3	Data Protection	3.1	Establish and Maintain a Data Management Process
		3.2	Establish and Maintain a Data Inventory
		3.3	Configure Data Access Control Lists
		3.4	Enforce Data Retention
		3.5	Securely Dispose of Data
		3.6	Encrypt Data on End-User Devices
Control 4	Secure Configuration of Enterprise Assets and Software	4.1	Establish and Maintain a Secure Configuration Process
		4.2	Establish and Maintain a Secure Configuration Process for Network Infrastructure
		4.3	Configure Automatic Session Locking on Enterprise Assets
		4.4	Implement and Manage a Firewall on Servers
		4.5	Implement and Manage a Firewall on End-User Devices
		4.6	Securely Manage Enterprise Assets and Software
		4.7	Manage Default Accounts on Enterprise Assets and Software
Control 5	Account Management	5.1	Establish and Maintain an Inventory of Accounts
		5.2	Use Unique Passwords
		5.3	Disable Dormant Accounts
		5.4	Restrict Administrator Privileges to Dedicated Administrator Accounts
Control 6	Access Control Management	6.1	Establish an Access Granting Process
		6.2	Establish an Access Revoking Process
		6.3	Require MFA for Externally-Exposed Applications
		6.4	Require MFA for Remote Network Access
		6.5	Require MFA for Administrative Access
Control 7	Continuous Vulnerability Management	7.1	Establish and Maintain a Vulnerability Management Process
		7.2	Establish and Maintain a Remediation Process
		7.3	Perform Automated Operating System Patch Management
		7.4	Perform Automated Application Patch Management

CIS Control	CIS Control Title	CIS Safeguard / Title
Control 8	Audit Log Management	8.1 Establish and Maintain an Audit Log Management Process
		8.2 Collect Audit Logs
		8.3 Ensure Adequate Audit Log Storage
Control 9	Email and Web Browser Protections	9.1 Ensure Use of Only Fully Supported Browsers and Email Clients
		9.2 Use DNS Filtering Services
Control 10	Malware Defenses	10.1 Deploy and Maintain Anti-Malware Software
		10.2 Configure Automatic Anti-Malware Signature Updates
		10.3 Disable Autorun and Autoplay for Removable Media
Control 11	Data Recovery	11.1 Establish and Maintain a Data Recovery Process
		11.2 Perform Automated Backups
		11.3 Protect Recovery Data
		11.4 Establish and Maintain an Isolated Instance of Recovery Data
Control 12	Network Infrastructure Management	12.1 Ensure Network Infrastructure is Up-to-Date
Control 13	Network Monitoring and Defense	
Control 14	Security Awareness and Skills Training	14.1 Establish and Maintain a Security Awareness Program
		14.2 Train Workforce Members to Recognize Social Engineering Attacks
		14.3 Train Workforce Members on Authentication Best Practices
		14.4 Train Workforce on Data Handling Best Practices
		14.5 Train Workforce Members on Causes of Unintentional Data Exposure
		14.6 Train Workforce Members on Recognizing and Reporting Security Incidents
		14.7 Train Workforce on How to Identify and Report if Their Enterprise Assets are Missing Security Updates
		14.8 Train Workforce on the Dangers of Connecting to and Transmitting Enterprise Data Over Insecure Networks
Control 15	Service Provider Management	15.1 Establish and Maintain an Inventory of Service Providers
Control 16	Application Software Security	
Control 17	Incident Response Management	17.1 Designate Personnel to Manage Incident Handling
		17.2 Establish and Maintain Contact Information for Reporting Security Incidents
		17.3 Establish and Maintain an Enterprise Process for Reporting Incidents
Control 18	Penetration Testing	

Appendix E

IG1 Safeguards Covered by CIS and MS-ISAC Tools

Category	Tool	Safeguards	CIS and MS-ISAC Tools
Asset Management	Enterprise Asset Management Policy/Process	1.1	<ul style="list-style-type: none"> • CIS Enterprise Asset Management Policy Template
	Enterprise and Software Asset Management Tool	1.1, 1.2, 2.1, 2.2, 2.3, 9.1, 12.1	<ul style="list-style-type: none"> • CIS Asset Tracking Spreadsheet
	Software Asset Management Policy/Process	2.1	<ul style="list-style-type: none"> • CIS Software Asset Management Policy Template
	Service Provider Management Tool	15.1	
Data Management	Data Management Policy/Process	3.1	<ul style="list-style-type: none"> • CIS Data Management Policy Template
	Data Management Tool	3.2, 3.4	<ul style="list-style-type: none"> • CIS Asset Tracking Spreadsheet
	Data Disposal Tool	3.5	
	Encryption Tool	3.6	
Secure Configurations	Secure Configuration Policy/Process	4.1, 4.2	<ul style="list-style-type: none"> • CIS Secure Configuration Management Policy Template
	Configuration Management Tool	4.1, 4.2, 4.3, 4.6, 4.7, 5.4, 10.3	<ul style="list-style-type: none"> • CIS Benchmarks (PDF versions) – Best Practice Guidance • CIS-CAT¹¹ Lite – Tool for Implementing Best Practice Guidance • CIS SecureSuite[®] Membership (Includes CIS-CAT Pro, CIS Build Kits, and CIS Benchmarks in Word, Excel, XML versions) - No-Cost to SLTTs¹² • CIS Hardened Images[®]
	Firewall	4.4, 4.5	<ul style="list-style-type: none"> • CIS Benchmarks (PDF versions) – Best Practice Guidance • CIS-CAT Lite – Tool for implementing Best Practice Guidance • CIS SecureSuite Membership (Includes CIS-CAT Pro, CIS Build Kits, and CIS Benchmarks in Word, Excel, XML versions) – No-Cost to SLTTs - Best Practice Guidance • CIS Hardened Images
Account and Access Control Management	Account and Credential Management Policy/Process	6.1, 6.2	<ul style="list-style-type: none"> • CIS Account and Credential Management Policy Template
	Identity and Access Management Tool	3.3, 5.1, 5.3, 5.4	
	Password Management Tool	5.2	<ul style="list-style-type: none"> • CIS Password Policy Guidance
	Multi-Factor Authentication Tool	6.3, 6.4, 6.5	

¹¹ CIS Configuration Assessment Tool (CIS-CAT[®])

¹² U.S. State, Local, Tribal, and Territorial (SLTT) government entities

Category	Tool	Safeguards	CIS, MS/EI-ISAC Tools
Vulnerability Management	Vulnerability/Patch Management Policy/Process	7.1	<ul style="list-style-type: none"> • CIS Vulnerability Management Policy Template
	Vulnerability/Patch Management Tool	7.2, 7.3, 7.4	
Log Management	Log Management Policy/Process	8.1	<ul style="list-style-type: none"> • CIS Audit Log Management Policy Template
	Log Management Tool	8.2, 8.3	<ul style="list-style-type: none"> • CIS Benchmarks (PDF versions) – Best Practice Guidance • CIS-CAT Lite – Tool for implementing Best Practice Guidance • CIS SecureSuite Membership (Includes CIS-CAT Pro, CIS Build Kits, and CIS Benchmarks in Word, Excel, XML versions) – No-Cost to SLTTs • CIS Hardened Images
Malware Defense	Anti-Malware Software	10.1, 10.2	<ul style="list-style-type: none"> • CIS Endpoint Security Services (ESS) - SLTTs only
	DNS Service/Server	9.2	<ul style="list-style-type: none"> • Malicious Domain Blocking and Reporting (MDBR) service - MS-ISAC Members only
Data Recovery	Data Recovery Policy/Process	11.1	<ul style="list-style-type: none"> • CIS Data Recovery Policy Template
	Data Backup and Recovery Tool	11.2, 11.3, 11.4	
Security Training	Security Training and Awareness Policy/Process	14.1	<ul style="list-style-type: none"> • CIS Security Awareness Skills Training Policy Template
	Security Training and Awareness Tool(s)	14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8	<ul style="list-style-type: none"> • MS-ISAC Advisories - Available to Everyone • MS-ISAC Cybersecurity Awareness Toolkit – SLTTs only
Incident Response	Incident Response Planning	17.1, 17.2, 17.3	<ul style="list-style-type: none"> • MS-ISAC Service: Cyber Incident Response Team (CIRT) - SLTTs only

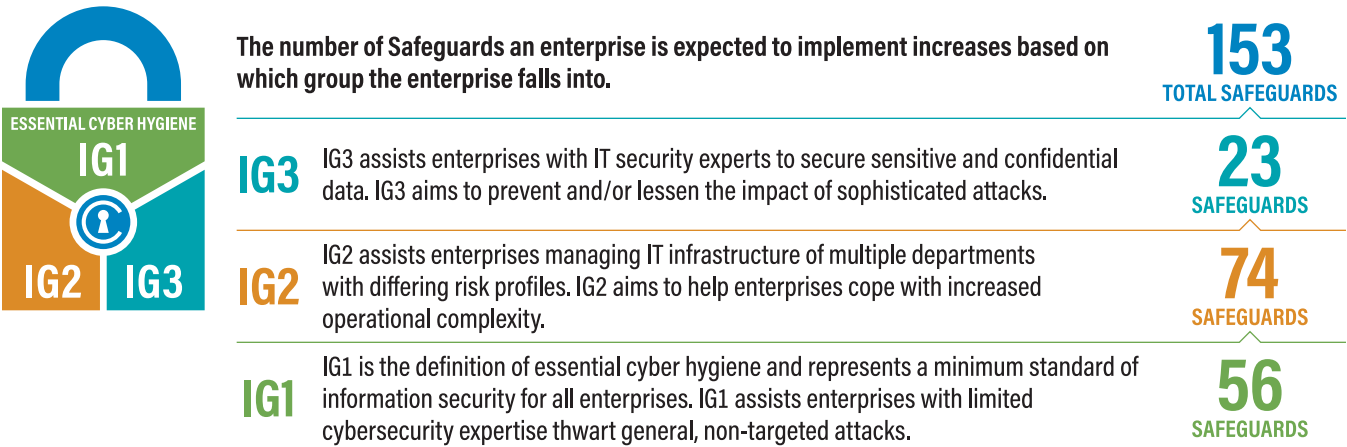
Appendix F

CIS Controls

The CIS Controls are a prioritized set of actions which collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. They are developed by a community of information technology (IT) experts who apply their first-hand experience as cyber defenders to create these globally accepted security best practices. The experts who develop the CIS Controls come from a wide range of sectors, including retail, manufacturing, healthcare, education, government, defense, and others. It is important to note that while the CIS Controls address general best practices that enterprises should implement to protect their environment, some operational environments may present unique requirements not addressed by the CIS Controls or require deviations from best practices.

Implementation Groups

The Implementation Group methodology was developed as a new way to prioritize the CIS Controls. These IGs provide a simple and accessible way to help enterprises of different classes focus their scarce security resources, while still leveraging the value of the CIS Controls program, community, and complementary tools and working aids. More about the Implementation Groups can be found in our [Guide to Implementation Groups \(IG\): CIS Critical Security Controls v8.1](#).



IG1

An IG1 enterprise is small to medium-sized with limited IT and cybersecurity expertise to dedicate toward protecting IT assets and personnel. The principal concern of these enterprises is to keep the business operational, as they have a limited tolerance for downtime. The sensitivity of the data that they are trying to protect is low and principally surrounds employee and financial information. Safeguards selected for IG1 should be implementable with limited cybersecurity expertise and aimed to thwart general, non-targeted attacks. These Safeguards will also typically be designed to work in conjunction with small or home office commercial off-the-shelf (COTS) hardware and software.

IG2

An IG2 enterprise employs individuals responsible for managing and protecting IT infrastructure. These enterprises support multiple departments with differing risk profiles based on job function and mission. Small enterprise units may have regulatory compliance burdens. IG2 enterprises often store and process sensitive client or enterprise

information and can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs. Safeguards selected for IG2 help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

IG3

An IG3 enterprise employs security experts that specialize in the different facets of cybersecurity (e.g., risk management, penetration testing, application security). IG3 assets and data contain sensitive information or functions that are subject to regulatory and compliance oversight. An IG3 enterprise must address availability of services and the confidentiality and integrity of sensitive data. Successful attacks can cause significant harm to the public welfare. Safeguards selected for IG3 must abate targeted attacks from a sophisticated adversary and reduce the impact of zero-day attacks.

If you would like to know more about how the CIS Controls and Implementation Groups pertain to enterprises of all sizes, visit our website at <https://www.cisecurity.org/controls/cis-controls-list/>.

Appendix G

CSP Capability Mappings

CSPs offer an ever-growing range of services that may or may not align with the CIS Controls. After reviewing CSP offerings, CIS has mapped many of these applicable tools and services to the Safeguards. This is done on a per-service or per-offering basis, and many of these capabilities may expand, shrink, or be removed altogether over time. The CSPs included are Microsoft, Amazon, and Google.

Microsoft

Tool / Service	Safeguard Mapping															
Azure Resource Manager	1.1	1.2	3.3													
Microsoft Defender for Cloud (+ Secure Score)	1.1	1.2	2.1	2.2	2.3	4.1	4.2	4.3	4.7	5.4	9.1	9.2	10.1	10.2	10.3	12.1
Microsoft Azure Purview	3.2	3.3	3.4	3.5												
Azure SQL Azure SQL Data Discovery	3.2															
Microsoft Entra	3.3	3.4	4.1	4.2	4.3	4.6	4.7	5.1	5.2	5.3	5.4	6.3	6.4	6.5		
Azure Disk Encryption	3.6															
Azure ARC	4.1	4.2	4.3	4.7												
Azure Security Benchmark	4.1	4.2	4.3	4.7	5.4	10.3										
Azure Policy	4.1	4.2	4.3	4.7	5.4	10.3										
Azure Blueprints	4.1	4.2	4.3	4.7	5.4	10.3										
Microsoft Security Baselines	4.1	4.2	4.3	4.7	5.4	10.3										
Azure Automation	4.1	4.2	4.3	4.7	5.4	7.2	7.3	7.4	10.3							
Azure Update Manager	7.2	7.3	7.4													
Windows Firewall (Server)	4.4															
Azure Firewall	4.4															
Secure RDP available on Windows	4.6															
Azure Bastion Host	4.6															
Key Vault	5.2															
Azure Blob Storage	8.2	8.3														
Azure Data Explorer	8.2	8.3														
Azure Monitor - Log Analytics	8.2	8.3														
Microsoft Sentinel	8.2	8.3														
Azure DNS	9.2															
Microsoft Antimalware for Azure	10.1	10.2														
Azure Backup	11.2	11.3	11.4													
Microsoft Unified (Support Agreement)	14.2	14.3	14.4	14.5	14.6	14.7	14.8									

Amazon

Tool / Service	Safeguard Mapping																		
AWS Billing (Cost and Usage Reports)	1.1	1.2																	
AWS IoT Device Management	1.1	1.2	2.1	2.2	7.3														
Amazon Inspector	1.2	2.1	2.2	2.3	4.1	4.2	4.4	4.7	7.2	7.3	7.4	12.1							
Amazon Simple Storage Service (S3)	3.4	3.5	8.3																
AWS Backup	11.2	11.3	11.4																
AWS Config	1.1	4.1	4.2	4.3	4.4	4.6	4.7	5.2	5.3	5.4	6.3	6.4	6.5	7.2	7.3	7.4	10.3	12.1	
AWS Systems Manager Inventory	1.1	1.2	2.1	2.2	2.3	4.1	4.2	4.4	4.7	7.2	7.3	7.4	9.1	12.1					
Amazon Macie	3.2																		
AWS Identity and Access Management (IAM)	3.3	5.1	5.2	5.3	5.4	6.3	6.4	6.5											
Data Protection and Privacy (throughout)	3.4	3.5																	
Amazon Lightsail	4.1																		
Amazon EC2 Image Builder	4.1	4.2	4.3	4.4	4.7														
AWS WAF	4.1	4.2	4.4	4.7															
AWS Shield	4.1	4.2	4.4	4.7															
AWS Network Firewall	4.1	4.2	4.4	4.7															
AWS Firewall Manager	4.1	4.2	4.4	4.7															
Amazon Route 53 Resolver DNS Firewall	4.1	4.2	4.4	4.7	9.2														
AWS Secrets Manager	4.1	4.2	4.4	4.7	5.2														
AWS Security Hub	4.1	4.2	7.2	7.3	7.4	12.1													
AWS Resource Access Manager	4.1	4.6																	
AWS Cloudformation	4.2	11.2	11.3	11.4															
AWS Key Management Service	4.6																		
AWS IAM Identity Center	5.2	5.3	5.4	6.3	6.4	6.5													
Amazon ECR (Elastic Container Registry)	7.2	7.3	7.4	12.1															
Amazon Kinesis Data Firehose	8.2	8.3																	
Amazon Security Lake	8.2	8.3																	
Amazon CloudTrail (and CloudTrail Lake)	8.2	8.3																	
Amazon CloudWatch	8.2	8.3																	
Amazon GuardDuty	10.1	10.2																	
Amazon EBS Snapshots	11.2	11.3	11.4																

Tool / Service	Safeguard Mapping							
AWS CodeCommit	11.2	11.3	11.4					
AWS Control Tower	11.2	11.3	11.4					
AWS Elastic Disaster Recovery	11.2	11.3	11.4					
Amazon S3 ObjectLock	11.3	11.4						
AWS Skill Builder / Workshops	14.2	14.3	14.4	14.5	14.6	14.7	14.8	

Google

Tool / Service	Safeguard Mapping											
Cloud Asset Inventory	1.1	1.2	2.1	2.2	2.3	9.1	12.1					
Cloud Identity	1.1	3.3	3.6	4.7	5.1	5.2	5.3	5.4	6.3	6.4	6.5.	
Cloud DLP	3.2	3.3	4.1	4.2								
Virtual Private Cloud (VPC)	3.3	4.1	4.2									
Identity and Access Management (IAM)	3.3	5.1	5.2	5.3	5.4	6.3	6.4	6.5				
Access Context Manager	3.3	5.1	5.4									
Data Protection and Privacy (throughout)	3.4	3.5										
Cloud Firewall	4.1	4.2	4.4									
Policy Intelligence	4.1	4.2	4.3	4.6	4.7	5.4	10.3					
Secret Manager	5.2											
Security Command Center	7.2	7.3	7.4	10.7	10.2							
Cloud Logging (Ingestion)	8.2	8.3										
Cloud Logging (Storage)	8.2	8.3										
Safe Browsing	9.2											
Cloud DNS	9.2											
Web Risk	9.2											
Cloud IDS	10.1	10.2										
Google Cloud Backup and DR	11.2	11.3	11.4									
Mandiant Academy	14.2	14.3	14.4	14.5	14.6	14.7	14.8					

Appendix H

CSP and MSP Detailed Cost Considerations

Below is an expansion on some details for cost considerations for CSP and MSP services that are more tailored for the practitioner. These details from our research are helpful for some technical implementers to understand.

CSPs

For CSPs, costs can vary greatly depending on several factors. For example, an enterprise that wishes to use the cloud for their backup solution may find that the amount of data and the length of time to store that data may or may not result in a higher cost as compared to an on-premises solution. Alternatively, enterprises may find that for systems that do not necessarily need to be up and running 24x7x365, the cloud may be a better alternative since the systems can easily be turned on and off during specific time periods. Another benefit is that certain tasks may be managed more easily in the cloud since it does not rely on physical access to the system and can be accessed remotely. The following is a sample list of factors that generally affect CSP costs:

- **Service Model:** The type of service (Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Software as a Service (SaaS), Function as a Service (FaaS) an enterprise chooses impacts the cost. For instance, IaaS might charge for raw compute and storage resources, while SaaS pricing often includes application licensing fees.
- **Resource Usage:** This includes CPU and GPU resources, volatile memory, and storage space. Cost often depends on the capacity required and the duration of use. This can be challenging to get right when planning a budget, and enterprises will often be able to somewhat modify this after procurement.
- **Network Usage:** Data transfer costs, both in and out of the cloud environment, will drastically affect pricing. Some providers offer a certain amount of free data transfer, but enterprises will incur charges beyond that limit.
- **Storage Type and Performance:** The cost varies depending on whether you need high-performance solid-state drive (SSD) storage, standard disk storage, or archival storage like cold or glacier storage for infrequently accessed data.
- **Scaling and Elasticity:** Auto-scaling services, which automatically adjust resources based on demand, can add to costs but also prevent overpaying for underused resources.
- **Additional Services and Features:** Advanced offerings such as machine learning, big data processing, and applications of artificial intelligence will often add to the cost.
- **Support Plans and SLAs:** The level of support and service agreements will impact cost. More comprehensive and responsive support plans cost more.
- **Geographic Region:** Costs vary depending on the region of the data centers due to local economic factors, energy prices, and demand.
- **Compliance and Security Features:** Additional security and compliance features, such as enhanced encryption or compliance with specific standards (like HIPAA, GDPR), will incur extra costs.
- **Backup and Disaster Recovery:** Services for data backup and disaster recovery solutions are usually priced separately.
- **Software Licenses:** Licensing fees may apply to enterprises running commercial software on cloud infrastructure.
- **Long-term Commitments:** Some cloud providers offer discounts for longer-term commitments compared to pay-as-you-go pricing.

MSPs

The cost of MSP services is dependent upon a variety of factors. This includes the number of end-users being supported, number of endpoints being supported, applications used, and scope of services. Some MSPs focus on network management including routers, switches, firewalls, servers, workstations, and other endpoints, while also managing user accounts (Microsoft Active Directory, for example), email configuration and backups, patch management, broad-scope backups, and help desk functions. Other MSPs have tiered services such as security hygiene including policy development, vulnerability management, SIEM solutions, threat intelligence, and more.

Some enterprises choose to outsource only specific functions to MSPs, relying on their internal expertise for most of the enterprise. For example, enterprises may serve the user environments, endpoints, patching, backups, and other core functionality on their own, but do not have the budget or resources to support a SIEM system to collect and store logs from various sources. This piece is commonly outsourced to an MSP that has expertise and staffing.

Similar to the discussion above for CSPs, maintaining well-defined and documented roles, responsibilities, and policies is essential when employing the services of MSPs to fulfill security and IT operational requirements. For example, while creation of organizational policies as they relate to the IT environment or security can be written by MSPs, the responsibility will still fall to the enterprise to manage and maintain them over time. As with any third-party, managing the relationship with an enterprise's service provider is crucial to the success of the enterprise's IT and cybersecurity program.

Appendix I

Links and Resources

CIS Critical Security Controls (CIS Controls) v8.1:

Learn more about the CIS Controls, including how to get started, why each Control is critical, procedures and tools to use during implementation, and a complete listing of Safeguards for each Control.

CIS Controls Policy Templates: Policy templates geared toward Safeguards found in IG1 of the CIS Controls.

A Roadmap to the CIS Controls: There is a broader ecosystem that surrounds the CIS Controls that offers guidance, tools, resources, mappings, and more to help facilitate the adoption and implementation of the framework. This guide will help adopters understand what is available to them, where to start, and how to put it all together.

Establishing Essential Cyber Hygiene: IG1 is essential cyber hygiene and represents a minimum standard of information security for all enterprises. This guide will help enterprises establish essential cyber hygiene.

Guide to Asset Classes: In v8.1, CIS restructured Asset Classes and their respective definitions to ensure consistency throughout the Controls. Learn more about our naming conventions and what they mean.

Guide to Implementation Groups (IG): IGs are the recommended guidance to prioritize implementation of the CIS Controls. In an effort to assist enterprises of every size, IGs are divided into three groups. Learn more about the five factors that can impact IG selection for an enterprise.

CIS Controls Assessment Specification: Provides an understanding of what should be measured in order to verify that the Safeguards are properly implemented.

CIS Controls Navigator: Learn more about the Controls and Safeguards and see how they map to other security standards (e.g., CMMC, NIST SP 800-53 Rev. 5, PCI DSS, MITRE ATT&CK). Available for CIS Controls versions 8.1, 8, and 7.1.

CIS Controls Self Assessment Tool (CIS CSAT):

Enables enterprises to assess and track their implementation of the CIS Controls for Versions 8.1, 8, and 7.1.

CIS Community Defense Model (CDM) v2.0: A guide published by CIS that leverages the open availability of comprehensive summaries of attacks and security incidents, and the industry-endorsed ecosystem that is developing around the MITRE ATT&CK Framework.

CIS Risk Assessment Method (CIS RAM) v2.1: An information security risk assessment method that helps enterprises implement and assess their security posture against the CIS Controls.

CIS SecureSuite Membership: Membership with access to CIS-CAT Pro, CIS Build Kits, CIS Benchmarks, and more.

CIS Benchmarks: Secure configuration guidelines for 100+ technologies, including operating systems, applications, and network devices.

CIS Configuration Assessment Tool (CIS-CAT)

Pro: Tool to scan for proper CIS Benchmark configurations for applications, operating systems, and network devices.

CIS Build Kits: ZIP files that contain a Group Policy Object (GPO) for each profile within the corresponding CIS Benchmark.

CIS Hardened Images: Virtual machine images securely pre-configured to the CIS Benchmarks.

CIS WorkBench: Get involved in one of our many communities.


CIS Password Policy Guide: CIS guidance for secure usage of passwords in an enterprise.

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 Critical Security 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. To learn more, visit [CISecurity.org](https://cisecurity.org) or follow us on X: @CISecurity.

 cisecurity.org

 email@cisecurity.org

 518-266-3460

 Center for Internet Security

 @CISecurity

 TheCISecurity

 cisecurity

