Vulnerability Management Policy Template

CIS Critical Security Controls

November 2022

Contents

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.

Editors:

Joshua M Franklin, CIS

Contributors:

Tony Krzyzewski, SAM for Compliance Ltd
Staffan Huslid, Truesec
Diego Bolatti, Information Systems Engineer, Universidad Tecnológica Nacional (Argentina)
Bryan Chou, CISSP, GSEC, GCED, GCIH
Bryan Ferguson
Gavin Willbond, SSS - IT Security Specialists
Ken Muir
Keala Asato
Robin Regnier, CIS
Jon Matthies

Introduction

Cybersecurity professionals are constantly challenged by attackers actively searching for vulnerabilities within enterprise infrastructure to exploit and gain access. Defenders must leverage timely threat information available to them about software updates, patches, security advisories, threat bulletins, etc., and they should regularly review their environment to identify these vulnerabilities before the attackers do. Understanding and managing vulnerabilities is a continuous activity, requiring focus of time, attention, and resources.

Purpose

The CIS Critical Security Controls® (CIS Controls®) recommend multiple information security policies that an enterprise should have in place. This includes a vulnerability management policy. This policy is meant as a "jumping off point" for organizations needing to draft their own policies to govern vulnerability management. Enterprises are encouraged to use this policy template in whole or in part. With that said, there are multiple decision points and areas that must be tailored to your enterprise. In CIS Controls v8, Safeguards 7.1 and 7.2 state:

> ***7.1 - Establish and Maintain a Vulnerability Management Process***
>
> *Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.*
>
> ***7.2 - Establish and Maintain a Remediation Process***
>
> *Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.*

To support this Safeguard, it is important for an enterprise to develop its own vulnerability management and remediation process. This document supports the development of those processes in accordance with the CIS Controls.

Types of Vulnerabilities in Assets

There are many types of enterprise assets that may contain vulnerabilities. The CIS Controls define an asset as all end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers, in virtual, cloud-based, and physical environments. Essentially any device owned, or system used by, an organization. Vulnerabilities may exist in all of these assets. All enterprise assets will contain vulnerabilities at some point in their lifecycle.

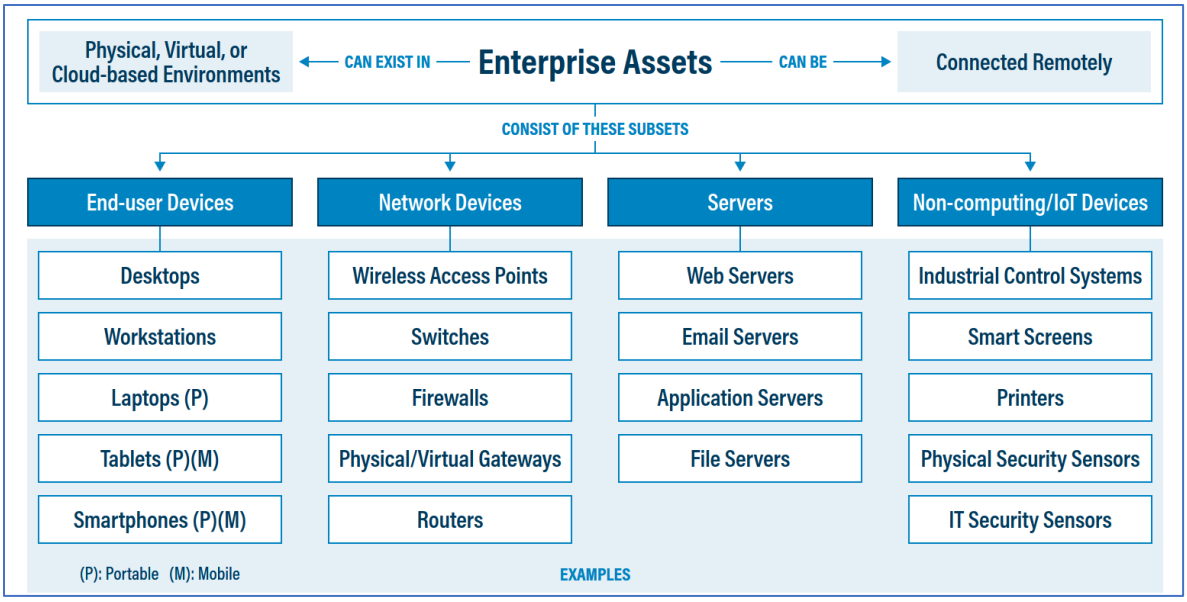


Figure 1. Enterprise assets, as defined in CIS Controls v8

Scope

This policy template is meant to supplement the CIS Controls v8. The policy statements included within this document can be used by all CIS Implementation Groups (IGs), but are specifically geared towards Safeguards in Implementation Group 1 (IG1). In Appendix D, Safeguards unique to IG1 are specifically highlighted for ease of use. For more information on the CIS Implementation Groups, see Appendix C. Additionally, a glossary in Appendix B is provided for guidance on terminology used throughout the document. Future versions of this template may expand the scope to both Implementation Group 2 (IG2) Safeguards. IG2 and IG3 enterprises may feel the need to add sections that go beyond IG1, and are welcome to do so. Depending on an enterprise's sector or mission, other policy statements may also need to be added or removed. This is encouraged as this policy needs to be molded and fit to the enterprise's needs.

Vulnerability Management Lifecycle

This vulnerability management policy is divided into multiple sections based on usage patterns of assets within an enterprise. These sections are shown below in Figure 2 are the high-level “steps” of the *Vulnerability Management Lifecycle*, followed by a detailed description of what each step entails.

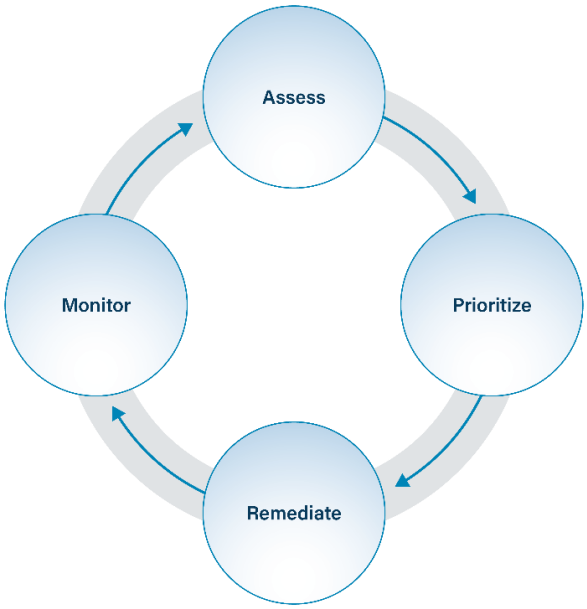


Figure 2. Vulnerability Management Lifecycle

- **Assess** – A combination of automated scanning, manual analysis, and leveraging threat intelligence to ascertain if vulnerabilities exist in enterprise systems and software.
- **Prioritize** – Creating a prioritized list of vulnerabilities that should be remediated in a specific order. This may simply be identifying and fixing critical vulnerabilities first, or using a scoring system such as the Common Vulnerability Scoring System (CVSS).
- **Remediate** – Fixing or patching vulnerabilities to ensure they are removed or mitigated in some other way.
- **Monitor** – Ensuring that remediated vulnerabilities are no longer affecting systems or did not introduce more problems that must be solved.

Assess

Enterprises that do not assess their infrastructure for vulnerabilities and proactively address discovered flaws face a significant likelihood of having their enterprise assets compromised. A large number of vulnerability scanning tools are available to evaluate the security configuration of enterprise assets. Some enterprises have also found commercial services using remotely managed scanning appliances to be effective. Finally, threat intelligence sources often provide email lists, blogs, open-source intelligence (OSINT), or other data sources to alert companies about vulnerabilities in products. To help standardize the definitions of discovered vulnerabilities across an enterprise, it is preferable to use vulnerability scanning tools that map vulnerabilities to industry-recognized vulnerability rating, configuration, and classification schemes/languages described in the Further Discussion portion of this document.

In order to approach vulnerability management from a holistic perspective, it is necessary to have a written plan in place. A vulnerability management plan must be developed and maintained. This plan should detail scanning

strategies, vulnerability prioritization, and remediation (to include patch management). Roles and responsibilities for various departments and positions should be detailed to ensure all employees understand their role in the vulnerability management process.

Prioritize

Once vulnerabilities are identified, they must be fixed, or remediated. But in what order? Effective enterprises link their vulnerability scanners with problem-ticketing systems that track and report progress on fixing vulnerabilities. This can help highlight unmitigated critical vulnerabilities to senior management to ensure they are resolved. Enterprises can also track how long it took to remediate a vulnerability, after identified, or a patch has been issued. These can support internal or industry compliance requirements. Some mature enterprises will go over these reports in IT security steering committee meetings, which bring leaders from IT and the business together to prioritize remediation efforts based on business impact.

In selecting which vulnerabilities to fix, or patches to apply, an enterprise should augment CVSS with data concerning the likelihood of a threat actor using a vulnerability, or potential impact of an exploit to the enterprise. Information on the likelihood of exploitation should also be periodically updated based on the most current threat information. For example, the release of a new exploit, or new intelligence relating to exploitation of the vulnerability, should change the priority through which the vulnerability should be considered for patching. Various commercial systems are available to allow an enterprise to automate and maintain this process in a scalable manner.

Remediate

Security patches are updates to a computer's operating system (OS) or installed software applications and are a basic part of Information Technology (IT) maintenance. The patches that developers provide often contain new features, but also contain fixes to recently discovered security vulnerabilities. Over time, operating systems go "stale" and need to be updated. Without a constant stream of security patches, computer systems can be infected by malware that can read or modify sensitive company data, or simply destroy it. Accordingly, patching operating systems and applications is one of the primary ways an enterprise can protect itself from attackers. Patching can be performed with patching tools or be configured in the operating system of a device. Patching tools may or may not be distinct tools for scanning for vulnerabilities. Assessing your patching status on a regular basis is important and many would say that the entire point of vulnerability scans is to test the effectiveness of your patch management efforts.

Some operating systems can help to remind users to update certain applications, especially those obtained within the application marketplace that is part of the operating system. With today's platforms, app stores are not just on mobile devices. Microsoft® Windows® 10 has an app store called Windows Apps and Apple's® store is called the MacApp® Store. Both stores can be configured to automatically install software updates from the application developer that were initially installed via an app store. Software obtained outside of an app store must be updated in an entirely different manner. Third-party software distributed outside the app store requires dedicated management software to patch it. In the end, keeping the total number of programs installed on a computer to the smallest number possible, helps with both management and security by reducing attack surface.

Monitor

A quality assurance process needs to exist to verify that patches and updates are implemented correctly and across all relevant enterprise assets. Monitoring should ensure that patches correctly fixed identified issues and affected assets no longer require further service. This will likely include the continuous process of re-evaluating assets that have already completed the vulnerability management process, which then leads back to the asset assessment process. As this occurs, data can be collected, stored, and analyzed that can further identify vulnerabilities through Security Information and Event Management (SIEM) systems and other technology.

Further Discussion

The Vulnerability Management Ecosystem

A large number of vulnerability scanning tools and standards are available to evaluate the security configuration of enterprise assets. Some enterprises have also found commercial services using remotely managed scanning appliances to be effective. To help standardize the definitions of discovered vulnerabilities across an enterprise, it is preferable to use vulnerability scanning tools that map vulnerabilities to one or more of the following industry-recognized vulnerability, configuration and platform classification schemes and languages:

- Common Vulnerabilities and Exposures (CVE®): This is a dictionary or glossary of known vulnerabilities. Through CVE, these vulnerabilities are all given a unique number, like an International Standard Book Number (ISBN). Each vulnerability is given the name format of "CVE" + "Year" + "unique_number". An example is CVE-2022-123456.
- Common Platform Enumeration (CPE): CPE is a naming scheme for specific types of enterprise assets and software. It enables the assigning of vulnerabilities to specific hardware and software stacks.
- Common Vulnerability Scoring System: This is an open framework for rating the severity of vulnerabilities. Note that CVSS scores can be easily used for deciding which vulnerabilities should be fixed first

The Vulnerability Management Ecosystem

Vulnerability notifications inform those responsible for caring for enterprise assets of vulnerabilities in those assets. This may take the form of a searchable web application, mailing list, or as part of a product. Vulnerability notifications can also be acquired through a variety of paid and free means. These notifications will inform system administrators of vulnerabilities in commercial products popular in the marketplace.

The National Vulnerability Database from the National Institute of Standards & Technology (NIST) provides a free, live feed of vulnerabilities known in the cybersecurity community. It leverages CVE, CPE, and CVSS to create an easily searchable list of vulnerabilities that is open to the world. Since the NVD contains a massive, ever-expanding list of vulnerabilities, it can be difficult to narrow down which ones you should be specifically worried about. The Known-Exploited Vulnerabilities Catalog from the Cybersecurity and Infrastructure Security Agency (CISA) helps to do just that. It informs organizations which vulnerabilities are being actively used and is a fantastic place to start looking for vulnerabilities in products you own. An example of a vulnerability notifications include an example of a service is the **Multi-State Information Sharing and Analysis Center®** (MS-ISAC®) Threat Intelligence Platform (TIP).[1] The MS-ISAC collects CTI from more than 200 different sources, such as by analyzing freely available threat information, commercial partners (e.g., Flashpoint, FireEye™ iSight, The Digital Forensics and Incident Response (DFIR) Report), and internal ISAC internal sources (e.g., Albert, Endpoint Detection and Response (EDR), Malicious Domain Blocking and Reporting (MDBR), Open sources (e.g., Spamhaus, Alienvault OTX™, social media).

Vulnerability Exceptions

How to handle exceptions will need to be covered in a vulnerability management plan. Exceptions allow a system to continue operate while vulnerabilities are known to exist within that system. Although allowing this to go on is not necessarily best practice, it is generally a fact of life for most organizations. Systems will need to operate to provide mission critical services. Exception processes should be properly documented with specific time frames for review and approval, and compensating controls should be identified and implemented as appropriate. While exceptions should be kept to a minimum, an enterprise that is not aware of their own vulnerabilities has unknown blindspots.

[1] Note that the MS-ISAC TIP is only available for US-based organizations.

Vulnerability Management Policy Template

Purpose

Vulnerability management is the process of searching for, prioritizing, and remediating vulnerabilities in enterprise systems and software. The Vulnerability Management Policy provides the processes and procedures for ensuring enterprise assets do not contain vulnerabilities. This policy applies to all departments and all assets connected to the enterprise network.

Responsibility

The IT business unit is responsible for all vulnerability management functions. Specifically, administrators are responsible for assessment and application of patching. Necessary vulnerability information must be relayed to other business units within the enterprise such as finance, accounting, and cybersecurity as required or needed. IT is responsible for informing all users of their responsibilities in the use of any assets assigned to them, such as applying updates in a regular manner or restarting their systems.

Exceptions

Exceptions to this policy are likely to occur. Request for exceptions may include to not scan a device, or additional time to remediate vulnerabilities, or to let certain systems function normally with vulnerabilities in place. Exception requests must be made in writing and must contain:

- The reason for the request,
- Risk to the enterprise of not following the written policy,
- Specific mitigations that will not be implemented,
- Technical and other difficulties in applying patches, and
- Date of review

Policy

Assess

1. A process for performing vulnerability management must be established.
    a. This process must be documented and approved.
    b. At a minimum, the vulnerability management process must be reviewed on an annual basis or following significant changes within the enterprise.
    c. IT must monitor vulnerability announcements and emerging threats applicable to enterprise asset inventory.
    d. All systems connected to the enterprise network must be scanned for vulnerabilities.

Prioritize

1. Identified vulnerabilities must be prioritized, with more critical vulnerabilities addressed first.

Remediate

1. A process for remediating identified vulnerabilities must be established.
    a. This process must be documented and approved.

b. At a minimum, this process must be reviewed on an annual basis or following significant changes within the enterprise.

c. Vulnerabilities that cannot be remediated must be submitted through the vulnerability exception process.

2. Operating systems must be configured to automatically update, unless an alternative approved patching process is used.
3. Applications must be configured to automatically update, unless an alternative approved patching process is used.
4. All users of enterprise assets have a duty to install updates for business systems and applications in a timely manner.
5. All users must ensure required reboots occur within a reasonable timeframe to ensure updates are properly installed.
6. High severity vulnerabilities must be addressed as a matter of priority.

Monitor

1. IT should subscribe to a threat information service to receive notifications of recently released patches and other software updates.
2. IT must notify the decision-making authority if vulnerabilities are not mitigated in a timely manner.
3. Every month, IT must create a report containing the status of all known vulnerabilities within the enterprise.

Revision History

Each time this document is updated, this table should be updated
.

Version	Revision Date	Revision Description	Name

Appendix A: Acronyms and Abbreviations

CIS	Center for Internet Security
CIS Controls	Center for Internet Security Critical Security Controls
CISA	Cybersecurity and Infrastructure Security Agency
COTS	Commercial-off-the-shelf
CPE	Common Platform Enumeration
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DFIR	Digital Forensics and Incident Response
EDR	Endpoint Detection and Response
IG	Implementation Group
IoT	Internet of Things
ISAC	Information Sharing and Analysis Center
ISBN	International Standard Book Number
IT	Information Technology
MAC	Media Access Control
MDBR	Malicious Domain Blocking and Reporting
MS-ISAC	Multi-State Information Sharing and Analysis Center
NIST	National Institute of Standards & Technology
OS	Operating System
OSINT	Open-source intelligence
NVD	National Vulnerability Database
SIEM	Security Information and Event Management

Appendix B: Glossary

Asset	Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards). Source: Asset(s) - Glossary | CSRC (nist.gov)
Asset inventory	An asset inventory is a register, repository or comprehensive list of an enterprise's assets and specific information about those assets. Source: Asset Inventory | FTA (dot.gov)
Asset owner	The department, business unit, or individual responsible for an enterprise asset. Source: CIS
Cloud environment	A virtualized environment that provides convenient, on-demand network access to a shared pool of configurable resources such as network, computing, storage, applications, and services. There are five essential characteristics to a cloud environment: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service. Some services offered through cloud environments include Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).
Enterprise assets	Assets with the potential to store or process data. For the purpose of this document, enterprise assets include end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers in virtual, cloud-based, and physical environments. Source: CIS Controls v8
End-user devices	Information technology (IT) assets used among members of an enterprise during work, off-hours, or any other purpose. End-user devices include mobile and portable devices such as laptops, smartphones, and tablets as well as desktops and workstations. For the purpose of this document, end-user devices are a subset of enterprise assets. Source: CIS Controls v8
Enterprise asset identifier	Often a sticker or tag with a unique number or alphanumeric string that can be tracked within an enterprise asset inventory. Source: CIS
Mobile end-user devices	Small, enterprise-issued end-user devices with intrinsic wireless capability, such as smartphones and tablets. Mobile end-user devices are a subset of portable end-user devices, including laptops, which may require external hardware for connectivity. For the purpose of this document, mobile end-user devices are a subset of end-user devices. Source: CIS Controls v8

Network devices	Electronic devices required for communication and interaction between devices on a computer network. Network devices include wireless access points, firewalls, physical/virtual gateways, routers, and switches. These devices consist of physical hardware as well as virtual and cloud-based devices. For the purpose of this document, network devices are a subset of enterprise assets. Source: CIS Controls v8
Non-computing/Internet of Things (IoT) devices	Devices embedded with sensors, software, and other technologies for the purpose of connecting, storing, and exchanging data with other devices and systems over the internet. While these devices are not used for computational processes, they support an enterprise's ability to conduct business processes. Examples of these devices include printers, smart screens, physical security sensors, industrial control systems, and information technology sensors. For the purpose of this document, non-computing/IoT devices are a subset of enterprise assets. Source: CIS Controls v8
Physical environment	Physical hardware parts that make up a network, including cables and routers. The hardware is required for communication and interaction between devices on a network. Source: CIS Controls v8
Portable end-user devices	Transportable, end-user devices that have the capability to wirelessly connect to a network. For the purpose of this document, portable end-user devices can include laptops and mobile devices such as smartphones and tablets, all of which are a subset of enterprise assets. Source: CIS Controls v8
Remote devices	Any enterprise asset capable of connecting to a network remotely, usually from public internet. This can include enterprise assets such as end-user devices, network devices, non-computing/Internet of Things (IoT) devices, and servers. Source: CIS Controls v8
Servers	A device or system that provides resources, data, services, or programs to other devices on either a local area network or wide area network. Servers can provide resources and use them from another system at the same time. Examples include web servers, application servers, mail servers, and file servers. Source: CIS Controls v8
User	Employees (both on-site and remote), third-party vendors, contractors, service providers, consultants, or any other user that operates an enterprise asset. Source: CIS
Virtual environment	Simulates hardware to allow a software environment to run without the need to use a lot of actual hardware. Virtualized environments are used to make a small number of resources act as many with plenty of processing, memory, storage, and network capacity. Virtualization is a fundamental technology that allows cloud computing to work. Source: CIS Controls v8

Appendix C: Implementation Groups

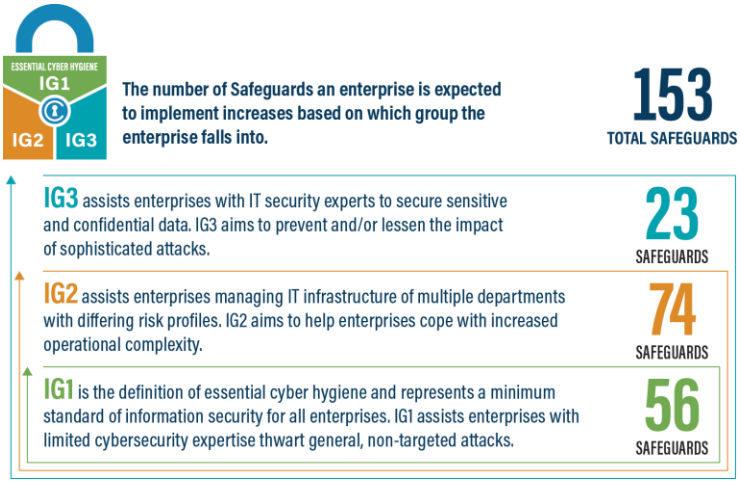
As a part of our most recent version of the CIS Controls, v8, we created Implementation Groups (IGs) to provide granularity and some explicit structure to the different realities faced by enterprises of varied sizes.

IG1

An IG1 enterprise is small- to medium-sized with limited IT and cybersecurity expertise to dedicate towards 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 they 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 the Implementation Groups and how they pertain to enterprises of all sizes, there are many resources that explore the Implementation Groups and the CIS Controls in general on our website at https://www.cisecurity.org/controls/cis-controls-list/.

Appendix D: CIS Safeguards Mapping

CIS Controls & Safeguards Covered by this Policy

This policy helps to bolster IG1 Safeguards in CIS Control 7: *Continuous Vulnerability Management*. Table 1 shows which IG1 Safeguards are covered by this policy as written.

Table 1 - Safeguards covered by IG1

CIS Control	Policy Statement	CIS Safeguard	CIS Safeguard Description
7.1	Assess 1 Monitor 1	Establish and Maintain a Vulnerability Management Process	Establish and maintain a documented vulnerability management process for enterprise assets. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard
7.2	Prioritize 1 Remediate 1, 4, 5, 6 Monitor 2	Establish and Maintain a Remediation Process	Establish and maintain a risk-based remediation strategy documented in a remediation process, with monthly, or more frequent, reviews.
7.3	Remediate 2	Perform Automated Operating System Patch Management	Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.
7.4	Remediate 3	Perform Automated Application Patch Management	Perform application updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.

Appendix E: References and Resources

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

CIS Critical Security Controls®
https://www.cisecurity.org/controls/

CIS Controls v8 Guide to Enterprise Assets and Software
https://www.cisecurity.org/insights/white-papers/guide-to-enterprise-assets-and-software

Cybersecurity and Infrastructure Security Agency
https://www.cisa.gov/known-exploited-vulnerabilities-catalog

MS-ISAC Threat Intelligence (TIP)
https://www.cisecurity.org/ms-isac/services/real-time-indicator-feeds

National Vulnerability Database
https://nvd.nist.gov/vuln/search