# A Roadmap to the CIS Critical Security Controls

November 2024

CIS Center for Internet Security®

CIS Controls™

## 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 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.

### Editor

Valecia Stocchetti, CIS

### Contributor

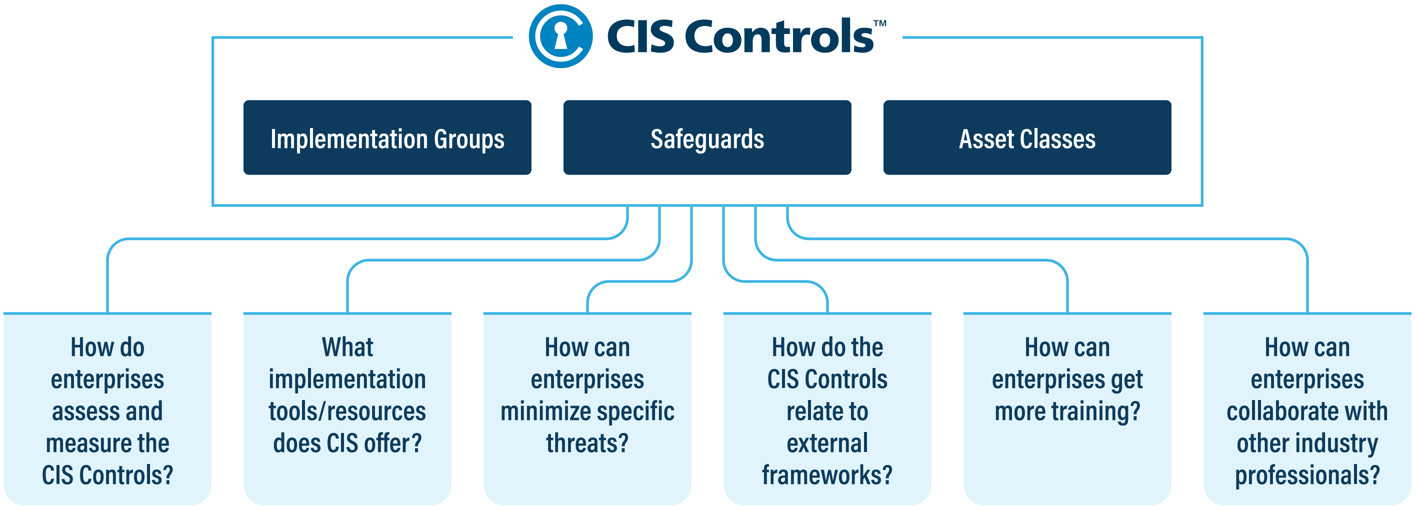
Robin Regnier, CIS

# Contents

# Introduction

The CIS Critical Security Controls (CIS Controls) are a set of best practice recommendations that defend against the most common cyber attacks. The CIS Controls themselves are the framework. However, there is a broader ecosystem that surrounds the CIS Controls which offers guidance, tools, resources, mappings, and more to help facilitate the adoption and implementation of the framework.

At times, it can be overwhelming to implement any security framework. Challenges arise such as deciding what to do first, what tools are available for implementation/measurement, and how to get help, if needed. CIS has developed this guide to help adopters of the CIS Controls to understand what is available to them, where to start, and how to put it all together. Shown below are just a few questions the CIS Controls can help to answer. This guide is broken down into six main sections that will help to answer each of these questions: *Assess and Measure*, *Implementation Resources/Tools*, *Minimization of Threats*, *External Frameworks*, *Collaboration*, and *Training and Speaking Engagements*. Note that the resources mentioned throughout this guide support adoption of CIS Controls v8.1, v8, and/or v7.1.


CIS Controls™
Implementation Groups
Safeguards
Asset Classes
How do enterprises assess and measure the CIS Controls?
What implementation tools/resources does CIS offer?
How can enterprises minimize specific threats?
How do the CIS Controls relate to external frameworks?
How can enterprises get more training?
How can enterprises collaborate with other industry professionals?

# Getting Started

At a high level, the CIS Controls are best practice recommendations that consist of a prioritized set of actions to defend against the most common attacks. In version 8.1 of the Controls, there are 18 top-level Controls, followed by a subset of 153 “actions” called Safeguards. As a part of our core documentation, when the CIS Controls are downloaded (at no cost), users can expect to receive different formats (Adobe® PDF, Microsoft® Excel®) of the Controls, as well as other information such as the Change Log for moving from a previous Controls version to a current version (e.g., v8 → v8.1).

**Figure 1** | **The CIS Critical Security Controls**

CONTROL 1
Inventory and Control of Enterprise Assets
5 Safeguards: IG1 2/5 IG2 4/5 IG3 5/5

CONTROL 2
Inventory and Control of Software Assets
7 Safeguards: IG1 3/7 IG2 6/7 IG3 7/7

CONTROL 3
Data Protection
14 Safeguards: IG1 6/14 IG2 12/14 IG3 14/14

CONTROL 4
Secure Configuration of Enterprise Assets and Software
12 Safeguards: IG1 7/12 IG2 11/12 IG3 12/12

CONTROL 5
Account Management
6 Safeguards: IG1 4/6 IG2 6/6 IG3 6/6

CONTROL 6
Access Control Management
8 Safeguards: IG1 5/8 IG2 7/8 IG3 8/8

CONTROL 7
Continuous Vulnerability Management
7 Safeguards: IG1 4/7 IG2 7/7 IG3 7/7

CONTROL 8
Audit Log Management
12 Safeguards: IG1 3/12 IG2 11/12 IG3 12/12

CONTROL 9
Email and Web Browser Protections
7 Safeguards: IG1 2/7 IG2 6/7 IG3 7/7

CONTROL 10
Malware Defenses
7 Safeguards: IG1 3/7 IG2 7/7 IG3 7/7

CONTROL 11
Data Recovery
5 Safeguards: IG1 4/5 IG2 5/5 IG3 5/5

CONTROL 12
Network Infrastructure Management
8 Safeguards: IG1 1/8 IG2 7/8 IG3 8/8

CONTROL 13
Network Monitoring and Defense
11 Safeguards: IG1 0/11 IG2 6/11 IG3 11/11

CONTROL 14
Security Awareness and Skills Training
9 Safeguards: IG1 8/9 IG2 9/9 IG3 9/9

CONTROL 15
Service Provider Management
7 Safeguards: IG1 1/7 IG2 4/7 IG3 7/7

CONTROL 16
Application Software Security
14 Safeguards: IG1 0/14 IG2 11/14 IG3 14/14

CONTROL 17
Incident Response Management
9 Safeguards: IG1 3/9 IG2 8/9 IG3 9/9

CONTROL 18
Penetration Testing
5 Safeguards: IG1 0/5 IG2 3/5 IG3 5/5

To help with prioritization, the Safeguards are divided into three Implementation Groups (IGs): IG1, IG2, and IG3. IG1 is essential cyber hygiene and represents the minimum standard of information security for all enterprises. These are the actions that every enterprise should take first, regardless of size. It also lays the foundation for implementing Safeguards in IG2 and IG3 .

**Figure 2** | **Implementation Groups (IGs) of the CIS Controls**

**The number of Safeguards an enterprise is expected to implement increases based on which group the enterprise falls into.**

**153** TOTAL SAFEGUARDS

**IG3** IG3 assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.

**23** SAFEGUARDS

**IG2** IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

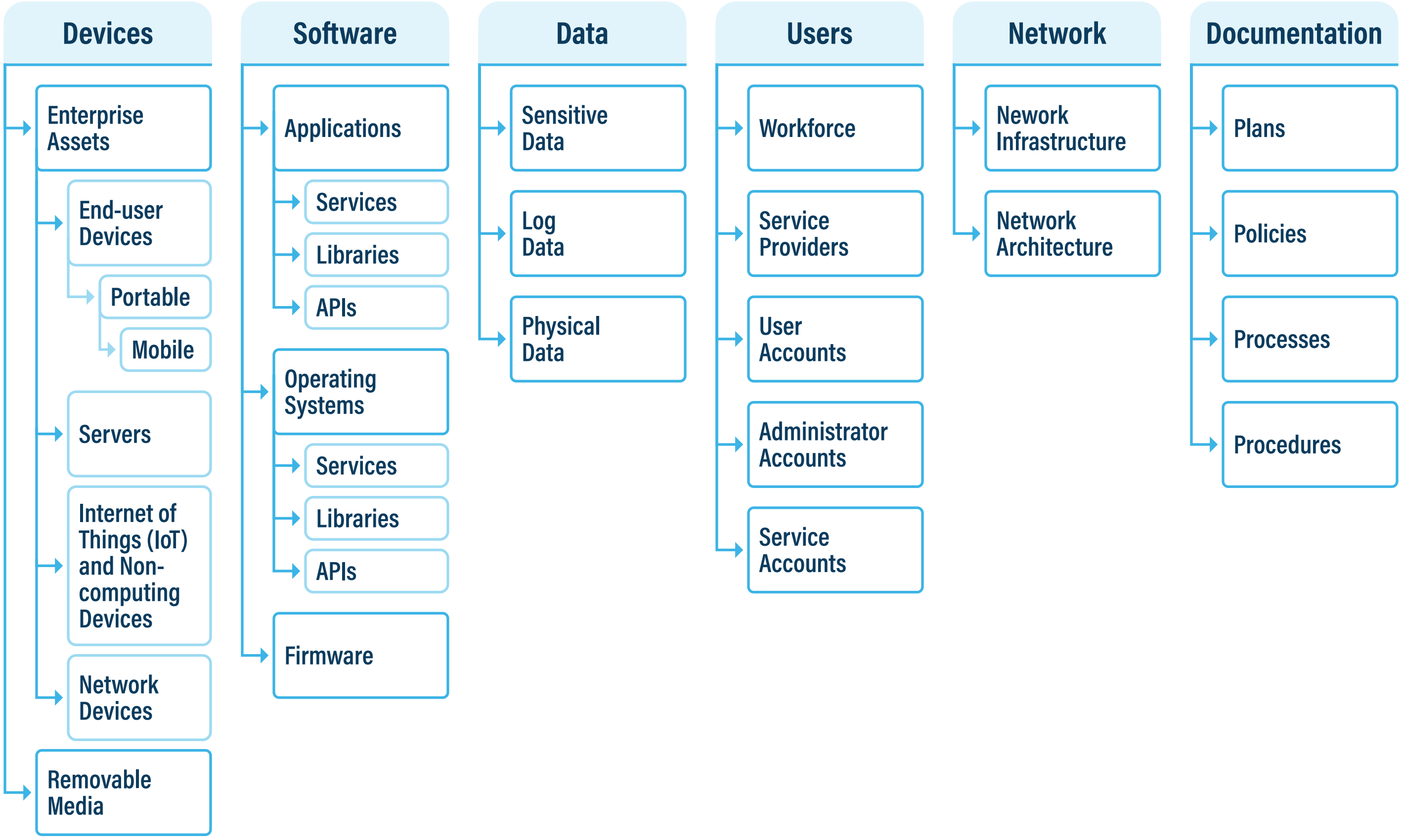
**74** SAFEGUARDS

**IG1** IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

**56** SAFEGUARDS

Each Safeguard is also assigned an Asset Class, defined as a group of information assets that are evaluated as one set based on their similarity. In v8.1, Asset Classes are categorized into *Devices*, *Software*, *Data*, *Users*, *Network*, and *Documentation*. Within each Asset Class, there are a number of sub-categories that align to language used throughout the CIS Controls. More information on Asset Classes can be found here.

Figure 3 | Asset Classes of the CIS Controls



Beyond the main documentation associated with the CIS Controls, various tools, guides, and other resources are available to users. These are broken down into six categories – *Assess and Measure*, *Implementation Tools/Resources*, *Minimization of Threats*, *External Frameworks*, *Collaboration*, and *Training and Speaking Engagements*.

## Assess and Measure

Beyond our Implementation Groups (IGs), enterprises often want to know where to start first and how to prioritize Safeguards. Is it by cost? risk? threat? tool? One of the first steps in implementing any security framework is to conduct a baseline assessment.

**CIS Controls Self Assessment Tool (CSAT)** | One of the first steps in implementing any security framework is to conduct a baseline assessment. CIS offers a selection of tools that can help with this. To start, our CIS Controls Self Assessment Tool (CSAT) enables enterprises to assess and track their implementation of the CIS Controls. This powerful tool can improve an enterprise's cyber defense program regardless of size or resources. CIS CSAT can help enterprises identify where CIS Safeguards are already well-implemented and where there are opportunities for improvement. This can be useful information as enterprises decide where to devote their limited cybersecurity resources. CSAT can also allow an enterprise to anonymously compare their results to the average of their industry or other peer groups to help drive the direction of their security program. There are two different versions of CSAT: CIS-Hosted CSAT (no-cost) and CSAT Pro (paid).

**CIS Business Impact Analysis Tool** | Enterprises may want or need to conduct a risk-based assessment and analysis. As a compliment to CIS-Hosted CSAT, the CIS Business Impact Analysis tool provides a cyber risk analysis by identifying specific Safeguards and cross-referencing them to an enterprise's CIS CSAT assessment. This helps to identify unique enterprise assets and estimate the potential costs incurred with a successful ransomware attack against those assets. The tool provides enterprises with the insight they need, now and over time, to communicate cyber risk to a variety of audiences, identify potential weak points in an enterprise's cybersecurity policy, and prioritize cyber threat abatement activities.

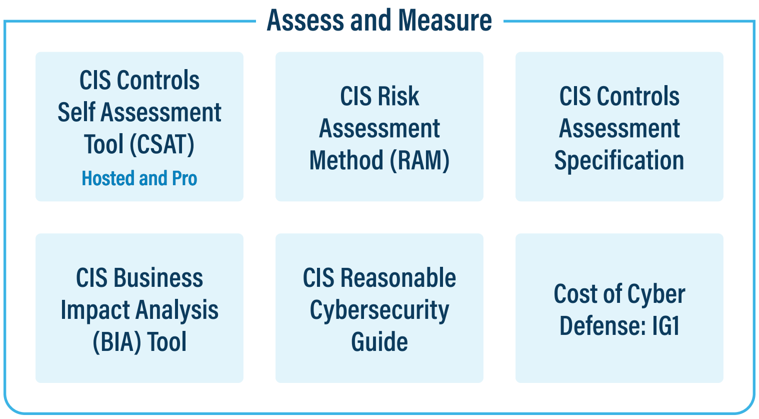
**CIS Risk Assessment Method (RAM)** | CIS has also published the CIS Risk Assessment Method (RAM), which is an information security risk assessment method that helps enterprises implement and assess their security posture against the CIS Controls. While CIS RAM is not a replacement for other risk assessment standards, it conforms to and supplements established information security risk assessment standards and methods, such as ISO 27005, NIST SP 800-30, and Risk Information Technology. CIS RAM also helps enterprises justify investments for reasonable implementation of the CIS Controls. Guides for CIS RAM are available for IG1, IG2, and IG3.

**A Guide to Defining Reasonable Cybersecurity** | To assess whether reasonable cybersecurity measures were implemented, CIS released A Guide to Defining Reasonable Cybersecurity to help with this. Several prominent data breaches, court cases, and state data privacy laws have placed the concept of "reasonable" cybersecurity in the public discourse, but there has been no real definition of what "reasonable" cybersecurity is. This guide provides practical and specific guidance to enterprises seeking to develop a cybersecurity program that satisfies the general standard of "reasonable cybersecurity."

**The Cost of Cyber Defense: Implementation Group 1 (IG1)** | As with any business decision, budget may play a role in the prioritization and assessment of where to allocate resources first when it comes to the CIS Controls. CIS has published The Cost of Cyber Defense: Implementation Group 1 (IG1), to help answer the questions as to which protections to start with, which tools will be needed to implement those protections, and how much an implementation will cost. 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). In turn, this information will help enterprises make informed and prioritized decisions when it comes to cyber defense.

**CIS Controls Assessment Specification** | During implementation, enterprises may also be wondering how to measure the implementation of a Safeguard. The purpose of the CIS Controls Assessment Specification is to provide a common understanding of what should be measured in order to verify that CIS Safeguards are properly implemented. The Controls Assessment Specification provides the inputs, operations, measures, and metrics that are needed during implementation of the Controls.

Below is a summary of the various products available when assessing and measuring the CIS Controls.



Assess and Measure

CIS Controls Self Assessment Tool (CSAT)
Hosted and Pro

CIS Risk Assessment Method (RAM)

CIS Controls Assessment Specification

CIS Business Impact Analysis (BIA) Tool

CIS Reasonable Cybersecurity Guide

Cost of Cyber Defense: IG1

## Implementation Resources/Tools

Once an enterprise begins to assess which Safeguards to select, implementation begins. CIS offers several resources that can be used during implementation of the CIS Controls.

**Environment-Specific Guidance** | Learn how to implement the CIS Controls in different environments such as cloud, mobile, Industrial Control System (ICS) environments, and Internet of Things (IoT). CIS also offers guides on privacy, small- to medium-sized enterprises (SMEs), managed service providers (MSPs), Windows 10, and teleworking.

**Establishing Essential Cyber Hygiene** | When tasked to implement a cybersecurity program, many enterprises ask, "How do we get started?" In response, CIS sorted the Safeguards into three IGs based on an enterprise's risk profile and the resources available to them. Establishing Essential Cyber Hygiene is a resource to assist with IG1 (*"essential cyber hygiene"*), providing specific tools and resources that can be used during implementation.

**CIS Policy Templates** | CIS has created several policy templates to function as a "jumping off point" for when enterprises are drafting their own policies. Using these policy templates, you can work to meet your cybersecurity goals around establishing essential cyber hygiene at a faster pace than if you were working alone.

**OSCAL** | The Open Security Controls Assessment Language (OSCAL) framework contains OSCAL serializations of the CIS Controls. OSCAL assists with the automation of mappings and improves an end-user's transition from one framework version to the next.

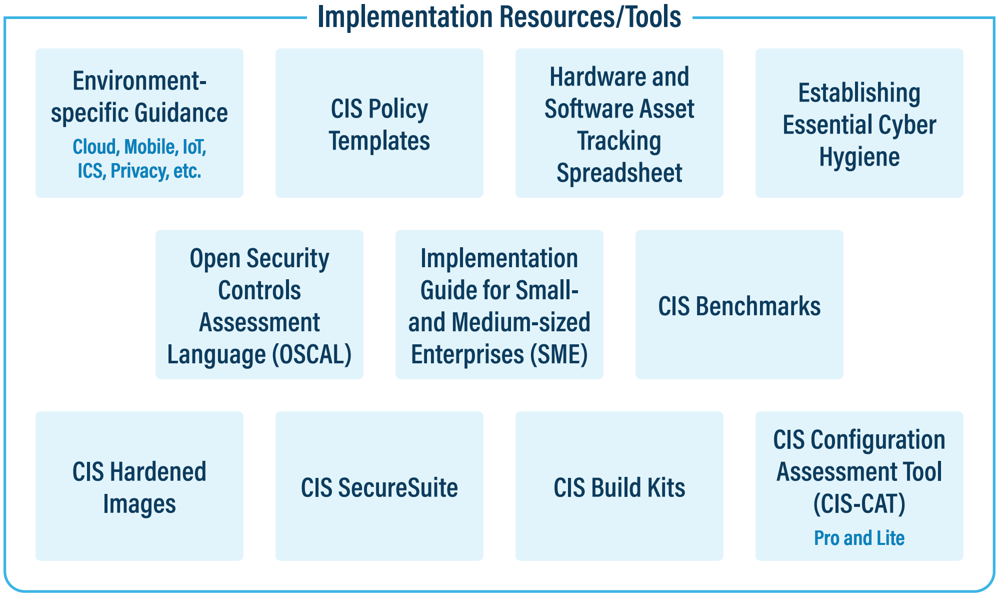
**Implementation Guide for Small and Medium-Sized Enterprises (SME)** | A guide to help SMEs protect their enterprises with a limited number of high-priority actions based on the CIS Controls. It works as a ladder to help SMEs rapidly adopt IG1 – *essential cyber hygiene*. The SME Guide contains several helpful resources such as spreadsheets for tracking various different items and a guide that provides a step-by-step walk-through of what actions to take.

**Hardware and Software Asset Tracking Spreadsheet** | A simple, easy-to-use spreadsheet for tracking an enterprise's assets and software.

**CIS Benchmarks™** | Many of the Safeguards in the CIS Controls require the configuration of certain technologies. CIS Benchmarks are prescriptive secure configuration recommendations for hardening specific technologies in an enterprise environment, available for over 25 vendor product families.

- **CIS Hardened Images** | Virtual machine (VM) images are pre-hardened to the CIS Benchmarks. Available on major cloud service platforms like AWS, Azure, Google Cloud Platform, and Oracle Cloud.

- **CIS Build Kits** | CIS offers Build Kits for certain technologies to assist in the automation of hardening systems. The Build Kit is designed to cover the majority of the Benchmark settings.
- **CIS-Configuration Assessment Tool (CIS-CAT)** | A powerful tool for automating CIS Benchmark assessment and reporting. CIS-CAT has two types: CIS-CAT Pro (paid with a SecureSuite Membership) and CIS-CAT Lite (no-cost).
- **CIS SecureSuite** | A Membership that provides scalable, customizable tools and resources to suit an enterprise's needs. CIS SecureSuite includes access to CIS-CAT Pro, CIS CSAT Pro, CIS Build Kits, CIS WorkBench, and more.



Implementation Resources/Tools

Environment-specific Guidance
Cloud, Mobile, IoT, ICS, Privacy, etc.

CIS Policy Templates

Hardware and Software Asset Tracking Spreadsheet

Establishing Essential Cyber Hygiene

Open Security Controls Assessment Language (OSCAL)

Implementation Guide for Small- and Medium-sized Enterprises (SME)

CIS Benchmarks

CIS Hardened Images

CIS SecureSuite

CIS Build Kits

CIS Configuration Assessment Tool (CIS-CAT)
Pro and Lite

## Minimization of Threats

Every enterprise is faced with at least one threat and often more than one. Whether it be ransomware, malware, web application attacks, or a wide variety of other threats, CIS has developed some key resources that will assist in minimizing the threats that impact the majority of enterprises.

**CIS Community Defense Model (CDM)** | CIS Community Defense Model (CDM) v2.0 can be used to design, prioritize, implement, and improve an enterprise's cybersecurity program. Enterprises naturally want to know "How effective are the CIS Controls against the most prevalent types of attacks?" The CDM was created to help answer that and other questions about the value of the Controls based on currently available threat data from industry reports.

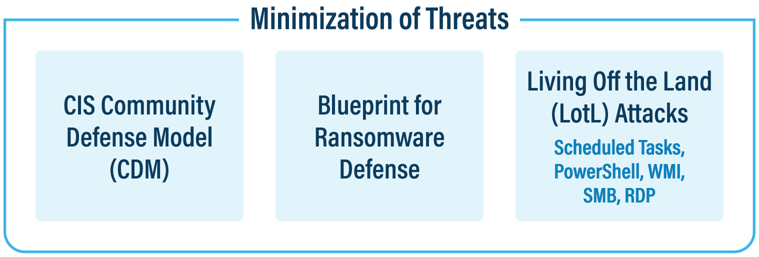
CDM v2.0 leverages industry threat data to determine the top five attack types (*Ransomware*, *Malware*, *Web Application Hacking*, *Insider and Privilege Misuse*, and *Targeted Intrusions*) and create comprehensive attack patterns (the set of attacker techniques that are required to execute an attack). Version 2.0 of the CDM builds on the original version, by mapping the Safeguards to the MITRE

Enterprise ATT&CK® v8.2 framework. This methodology allows CIS to measure which Safeguards are most effective overall for defense across attack types. As an example, CDM v2.0 asserts that, independent of any specific attack type, implementing IG1 Safeguards defends against 74% of ATT&CK (sub-)techniques in the MITRE ATT&CK framework.

**Blueprint for Ransomware Defense** | In response to Action 3.1.1 of the Ransomware Task Force (RTF) report, which calls for the cybersecurity community to "develop a clear, actionable framework for ransomware mitigation, response, and recovery," the Blueprint for Ransomware Defense Working Group developed a blueprint. In partnership with the Ransomware Task Force (RTF), which consists of more than 60 members (including CIS) spanning several sectors, the Blueprint for Ransomware Defense provides a set of 40 Foundational and Actionable Safeguards from IG1 of the CIS Controls that assist with ransomware defense while considering those SMEs that have limited cybersecurity expertise.

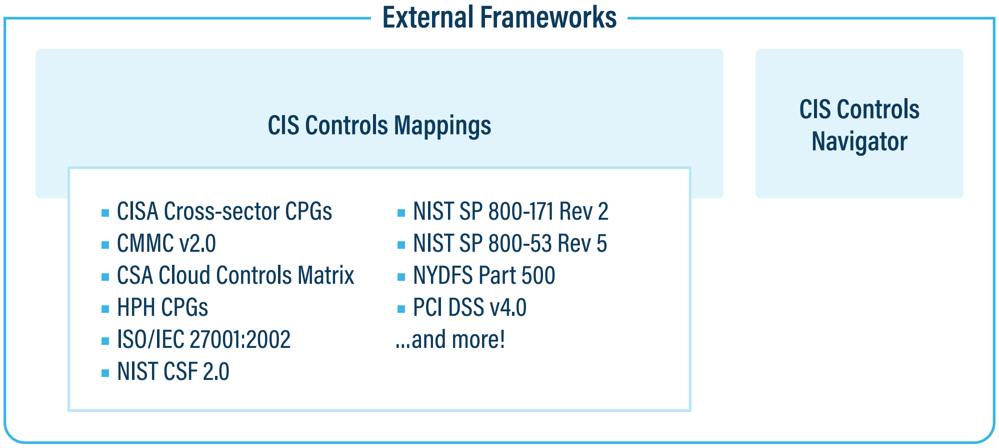
**Living off the Land (LotL) Attacks** | Attacks using exploited protocols and other LotL attack techniques have been, and continue to be, on the rise. CIS has published several guides that address the most commonly exploited LotL techniques including:

- Scheduled Tasks
- PowerShell
- Windows Management Instrumentation (WMI)
- Server Message Block (SMB)
- Remote Desktop Protocol (RDP)


Minimization of Threats
CIS Community Defense Model (CDM)
Blueprint for Ransomware Defense
Living Off the Land (LotL) Attacks
Scheduled Tasks, PowerShell, WMI, SMB, RDP

## External Frameworks

Many enterprises are required to comply with multiple other industry regulations or frameworks. By implementing the CIS Controls, enterprises create an on-ramp to comply with PCI DSS, HIPAA, GDPR, and more. The CIS Controls are mapped to over 25 industry frameworks for ease of implementation. These mappings are offered in two forms: Microsoft® Excel® spreadsheet and through our CIS Controls Navigator (available for v8.1, v8, and v7.1 of the CIS Controls).



External Frameworks

CIS Controls Mappings

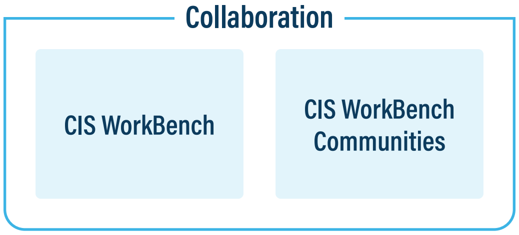
- CISA Cross-sector CPGs
- CMMC v2.0
- CSA Cloud Controls Matrix
- HPH CPGs
- ISO/IEC 27001:2002
- NIST CSF 2.0
- NIST SP 800-171 Rev 2
- NIST SP 800-53 Rev 5
- NYDFS Part 500
- PCI DSS v4.0

...and more!

CIS Controls Navigator

## Collaboration

CIS is proud to offer a platform where users can collaborate with other professionals in the industry around the world. CIS WorkBench brings together adopters of the CIS Controls and CIS Benchmarks by providing communities of common interests. Discussions range from the most detailed technical configuration settings to broader cybersecurity policies. Integrating these groups on the same platform provides enterprises with greater insight into key initiatives.



Collaboration

CIS WorkBench

CIS WorkBench Communities

## Training and Speaking Engagements

CIS participates in a variety of webinars, podcasts, conferences (virtual and in-person), and more.

Additionally, training on various CIS Controls topics are available through a few different platforms including:

- SANS SEC366: CIS Controls IG1
- SANS SEC566: Implementing and Auditing CIS Controls
- Salesforce Trailhead:
  - Trailhead Controls Introductory Course
  - Trailhead CIS RAM Course
  - Trailhead The Value of Security Controls

CIS also offers a CIS Controls Accreditation for CIS SecureSuite Members. This initiative gives the ability to provide CIS Controls implementation, auditing, and/or assessment with the assurance that they have met the consistent and rigorous standards of CREST certification. It also offers service providers a "stamp of approval" at the organization level, assuring that their customers can feel confident that they are doing business with a reputable and reliable CIS Controls assessment organization.

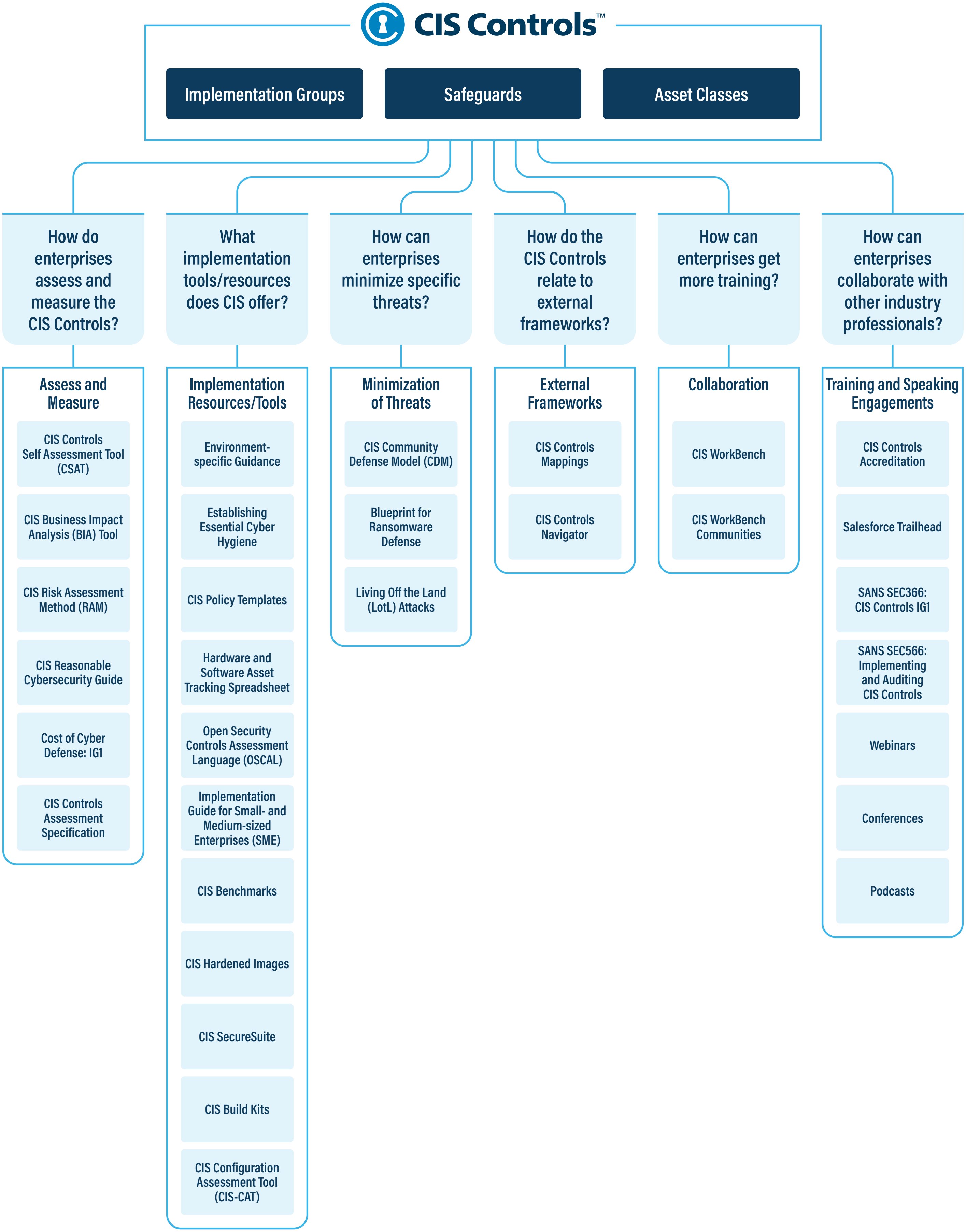
Training and Speaking Engagements
CIS Controls Accreditation
Salesforce Trailhead
SANS SEC366: CIS Controls IG1
SANS SEC566: Implementing and Auditing CIS Controls
Webinars
Conferences
Podcasts

# Putting It All Together

Whether you use the CIS Controls, and/or another way to guide your security improvement program, you should recognize that "it's not about the list." You can get a credible list of security recommendations from many sources—it is best to think of the list as a starting point. It is important to look for the ecosystem that grows up around the list. Questions that are at the forefront of many enterprises' minds include:

- Where can I get training, complementary information, explanations?
- How have others implemented and used these recommendations?
- Is there a marketplace of vendor tools and services to choose from?
- How will I measure progress or maturity?
- How does this align with the myriad regulatory and compliance frameworks that apply to me?

The true power of the CIS Controls is not about creating the best list, it is about harnessing the experience of a community of individuals and enterprises to actually make security improvements through the sharing of ideas, tools, lessons, and collective action.



CIS Controls™

Implementation Groups

Safeguards

Asset Classes

How do enterprises assess and measure the CIS Controls?

Assess and Measure

- CIS Controls Self Assessment Tool (CSAT)
- CIS Business Impact Analysis (BIA) Tool
- CIS Risk Assessment Method (RAM)
- CIS Reasonable Cybersecurity Guide
- Cost of Cyber Defense: IG1
- CIS Controls Assessment Specification

What implementation tools/resources does CIS offer?

Implementation Resources/Tools

- Environment-specific Guidance
- Establishing Essential Cyber Hygiene
- CIS Policy Templates
- Hardware and Software Asset Tracking Spreadsheet
- Open Security Controls Assessment Language (OSCAL)
- Implementation Guide for Small- and Medium-sized Enterprises (SME)
- CIS Benchmarks
- CIS Hardened Images
- CIS SecureSuite
- CIS Build Kits
- CIS Configuration Assessment Tool (CIS-CAT)

How can enterprises minimize specific threats?

Minimization of Threats

- CIS Community Defense Model (CDM)
- Blueprint for Ransomware Defense
- Living Off the Land (LotL) Attacks

How do the CIS Controls relate to external frameworks?

External Frameworks

- CIS Controls Mappings
- CIS Controls Navigator

How can enterprises get more training?

Collaboration

- CIS WorkBench
- CIS WorkBench Communities

How can enterprises collaborate with other industry professionals?

Training and Speaking Engagements

- CIS Controls Accreditation
- Salesforce Trailhead
- SANS SEC366: CIS Controls IG1
- SANS SEC566: Implementing and Auditing CIS Controls
- Webinars
- Conferences
- Podcasts

## Appendix A

# Acronyms and Abbreviations

| | |
|---|---|
| **AWS** | Amazon Web Services |
| **CIS BIA Tool** | CIS Business Impact Analysis Tool |
| **CIS CAT** | CIS Configuration Assessment Tool |
| **CIS CDM** | CIS Community Defense Model |
| **CIS CSAT** | CIS Controls Self Assessment Tool |
| **CIS HIs** | CIS Hardened Images |
| **CIS RAM** | CIS Risk Assessment Method |
| **CISA** | Cybersecurity and Infrastructure Security Agency |
| **CMMC** | Cybersecurity Maturity Model Certification |
| **CSA** | Cloud Security Alliance |
| **GDPR** | General Data Protection Regulation |
| **HIPAA** | Health Insurance Portability and Accountability Act |
| **HPH CPGs** | Healthcare and Public Health (HPH) Cybersecurity Performance Goals |
| **ICS** | Industrial Control Systems |
| **IG** | Implementation Group |
| **IoT** | Internet of Things |
| **ISO/IEC** | International Organization for Standardization/International Electrotechnical Commission |
| **IT** | Information Technology |
| **LotL** | Living off the Land |
| **MITRE ATT&CK** | MITRE Adversarial Tactics, Techniques, and Common Knowledge |
| **MSP** | Managed Service Provider |
| **NIST CSF** | National Institute of Standards and Technology Cybersecurity Framework |
| **NIST SP** | National Institute of Standards and Technology Special Publication |
| **NY DFS** | New York State Department of Financial Services |
| **OSCAL** | Open Security Controls Assessment Language |
| **PCI DSS** | Payment Card Industry Data Security Standard |
| **RDP** | Remote Desktop Protocol |
| **RTF** | Ransomware Task Force |
| **SMB** | Server Message Block |
| **SME** | Small and medium-sized enterprises |
| **VM** | Virtual Machine |
| **WMI** | Windows Management Instrumentation |

The Center for Internet Security, Inc. (CIS®) makes the connected world a safer place for people, businesses, and governments through our core competencies of collaboration and innovation.

We are a community-driven nonprofit, responsible for the CIS Controls® and CIS Benchmarks™, globally recognized best practices for securing IT systems and data. We lead a global community of IT professionals to continuously evolve these standards and provide products and services to proactively safeguard against emerging threats. Our CIS Hardened Images® provide secure, on-demand, scalable computing environments in the cloud.

CIS is home to the Multi-State Information Sharing and Analysis Center® (MS-ISAC®), the trusted resource for cyber threat prevention, protection, response, and recovery for U.S. State, Local, Tribal, and Territorial government entities, and the Elections Infrastructure Information Sharing and Analysis Center® (EI-ISAC®), which supports the rapidly changing cybersecurity needs of U.S. elections offices.

CIS® Center for Internet Security®

www.cisecurity.org
info@cisecurity.org
☎ 518-266-3460
Center for Internet Security

CenterforIntSec
@CISecurity
TheCISecurity
cisecurity