Center for Internet Security®

Guide to the

First 5 CIS Controls™ (v6.1)

CIS Controls

Understanding the CIS Controls™

In 2008, the CIS Controls – formerly known as the Critical Security Controls – were created in collaboration with representatives from the U.S. government and private sector security research organizations. A set of practical defenses targeted toward stopping cyber attacks, the CIS Controls are technical in nature and define specific, practical steps an organization can take to stop the most common cyber threats from compromising their systems.

Put simply, the CIS Controls were developed to answer the frequent question:

"Where should I start when I want to improve my cyber defenses?"

CIS Controls

Why Use The CIS Controls?

Many organizations facing the current cybersecurity environment are overwhelmed by what we call the "Fog of More"—a constant stream of new information and problems. They are challenged by competing expert opinions, a noisy and fast-changing marketplace of potential solutions, and unclear or overwhelming regulatory and compliance requirements.

The CIS Controls are developed by a global expert community based on their first-hand experience of the threat environment to identify the most high-value practices to secure networks. Their in-depth understanding of the current threat landscape drives the priority order and focus of the CIS Controls. Further, CIS routinely incorporates feedback from the user community and ensures the best practices are vendor-neutral.

Relationship to Compliance Frameworks

The CIS Controls align with top compliance frameworks such as NIST, PCI, ISO, HIPAA, COBIT and others. Downloaded more than 65,000 times across the globe, most CIS Controls adopters use more than one framework to improve their security. CIS does not compete with any other framework; rather, we strive to offer users tools and work aids to simplify their security journey. In fact, many CIS adopters tell us they use the CIS Controls as the implementation guide to the NIST Cybersecurity Framework (CSF).

Getting Started

A number of studies show that implementation of the First 5 CIS Controls provides an effective defense against the most common cyber attacks (~85% of attacks). In an effort to help organizations implement the First 5 CIS Controls, the objective of each is described next.

1

CIS Control 1
Inventory of Authorized & Unauthorized Devices

This CIS Control helps organizations define a baseline of what must be defended. Without an understanding of what devices and data are connected, they cannot be defended. The inventory process should be as comprehensive as possible, and scanners (both active and passive) that can detect devices are the place to start.

After an organization has accurately inventoried their systems, the next step is to prevent unauthorized devices from joining a network—this is where implementation of network level authentication excels. The initial goal of CIS Control 1 is not to prevent attackers from joining the network, as much as it is to understand what is on the network so it can be defended.

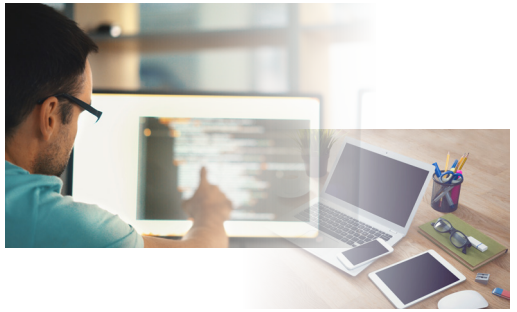
2

CIS Control 2
Inventory of Authorized & Unauthorized Software

The purpose of this CIS Control is to ensure that only authorized software is allowed to run on an organization's systems. While an inventory of software is important, application whitelisting is a crucial part of this process, as it limits the ability to run applications to only those which are explicitly approved. While not a silver bullet for defense, this CIS Control is often considered one of the most effective at preventing and detecting cyberattacks.

Implementing CIS Control 2 often requires organizations to reconsider their policies and culture—no longer will users be able to install software whenever and wherever they like. But this CIS Control, already successfully implemented by numerous organizations, will likely provide immediate returns to an organization attempting to prevent and detect cyber attacks.

3



CIS Control 3
Secure Configurations for Hardware & Software on Mobile Devices, Laptops, Workstations, & Servers

By default, most systems are configured for ease-of-use and not necessarily security. In order to meet CIS Control 3, organizations need to reconfigure systems to a secure standard.

Many organizations already have the technology necessary to securely configure systems at scale, such as Microsoft® Active Directory Group Policy Objects and Unix Puppet or Chef. By utilizing configuration standards such as the CIS Benchmarks, most organizations can successfully implement this CIS Control. The consensus-driven CIS Benchmarks are freely available for most operating systems, middleware and software applications, and network devices.

CIS Benchmarks

4

CIS Control 4
Continuous Vulnerability Assessment & Remediation

The goal of this CIS Control is to understand and remove technical weaknesses that exist in an organization's information systems. Successful organizations implement patch management systems that cover both operating system and third-party application vulnerabilities. This allows for the automatic, ongoing, and proactive installation of updates to address software vulnerabilities.

In addition to patch management systems, organizations must implement a commercial vulnerability management system to give themselves the ability to detect and remediate exploitable software weaknesses.

5

CIS Control 5
Controlled Use of Administrative Privileges

This CIS Control ensures that workforce members have only the system rights, privileges, and permissions that they need in order to do their job—no more and no less than necessary. Unfortunately, for the sake of speed and convenience, many organizations allow staff to have local system or even domain administrator rights which are too generous and open the door for abuse, accidental or otherwise.

The simple answer for CIS Control 5 is to remove unnecessary system rights or permissions. For larger organizations struggling with this task at scale, privilege management vendors can provide endpoint solutions to help lessen the administrative burden.

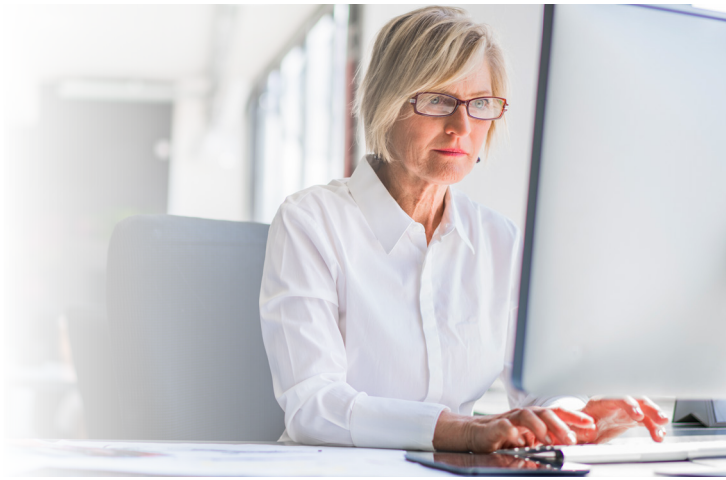
Guidance for Implementing the Controls

Perhaps the best tip for implementing the CIS Controls is to create a plan. Some organizations may establish a "Governance, Risk, and Compliance" (GRC) program. Other successful tactics include assigning program managers to coordinate tasks involved with server administrators, workstation specialists, network engineers, software developers, and even professionals outside of Information Technology such as human resource specialists, trainers, and compliance officers.

Many organizations have found success by implementing the CIS Controls in a phased approach, tackling some early and implementing others later as part of a long-term strategy coordinated and approved by senior management. Organizations rarely implement every sub-control described in the CIS Controls (Version 6.0, for example, has 149 sub-controls).

Most sub-controls are foundational to effective cyber defense, while others provide advice on advanced techniques (Version 6.1 was created to add categories for "foundational" and "advanced" controls).

A phased implementation approach also helps ensure that organizations receive the most significant benefits by implementing the highest priority controls first. In fact, implementation of asset inventory (CIS Controls 1 & 2) and standard configurations (CIS Control 3) often results in cost savings as fewer resources are required to manage the organization's cyber environment. There are a few practical considerations to make when embarking on this journey.



Keeping these suggestions in mind and building them into the program's plan will help to ensure its success.

Specifically, an organization should:

- Make a formal, conscious, top-level decision to make the CIS Controls part of the organization's standard for cybersecurity. Senior management and the Board of Directors should be on board for support and accountability.
- Assign a program manager who will be empowered and responsible for the implementation of the CIS Controls.
- Decide who will be responsible for the long-term sustainability of maintaining cyber defenses.
- Start with a gap analysis, assessment, or audit of the current organization's state against the CIS Controls and develop an implementation plan scheduled with priority focus on the First 5 CIS Controls.
- Document the long-term plan (3-5 years) for implementing cyber defenses that are not already a part of the entity's defensive strategy.
- Embed the definitions or goals of the CIS Controls into the organization's security policies to streamline their implementation.
- Ensure that internal and external auditors use the CIS Controls as a part of their benchmark for assessing the organization's security stance.
- Educate workforce members on the organization's security goals and enlist their help as a part of the long-term defense of the organization's data.

While there may be other steps that help improve an organization's chances of success, these considerations are a good starting point for structuring a program to implement the CIS Controls.

Ensuring Success

With hard work and dedication, an effective cyber defense **is** achievable. As we know, rarely do worthy rewards and accolades come easily. Organizations must assume that implementing and then maintaining these technical defenses will be an ongoing program, not a short-term project with a defined end date. As with any program, appropriate resources such as time, budgets, and people must be dedicated to the effort to ensure its success.

About Us

CIS is a forward-thinking, nonprofit entity that harnesses the power of a global IT community to safeguard private and public organizations against cyber threats.

Our CIS Controls and CIS Benchmarks are the global standard and recognized best practices for securing IT systems and data against the most pervasive attacks. These proven guidelines are continually refined and verified by a volunteer, global community of experienced IT professionals.

CIS is home to the Multi-State Information Sharing and Analysis Center (MS-ISAC®), the go-to resource for cyber threat prevention, protection, response, and recovery for state, local, tribal and territorial government entities.

The entire CIS Controls v6.1 can be found at
www.learn.cisecurity.org/20-controls-download

Questions? Contact us at
controlsinfo@cisecurity.org

CIS Controls **CIS Benchmarks** **MS-ISAC**