CIS Controls Self Assessment Tool Document Library

About the CIS Controls™

The CIS Controls™ are a prioritized set of actions that collectively form a defense-in-depth set of best practices that mitigate the most common attacks against systems and networks. The CIS Controls are developed by a community of 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.

We are at a fascinating point in the evolution of what we now call cyber defense. Massive data losses, theft of intellectual property, credit card breaches, identity theft, threats to our privacy, denial of service -- these have become a way of life for all of us in cyberspace.

As defenders we have access to an extraordinary array of security tools and technology, security standards, training and classes, certifications, vulnerability databases, guidance, best practices, catalogs of security controls, and countless security checklists, benchmarks, and recommendations. To help us understand the threat, we have seen the emergence of threat information feeds, reports, tools, alert services, standards, and threat sharing frameworks. To top it all off, we are surrounded by security requirements, risk management frameworks, compliance regimes, regulatory mandates, and so forth. There is no shortage of information available to security practitioners on what they should do to secure their infrastructure.

But all of this technology, information, and oversight has become a veritable "Fog of More" -- competing options, priorities, opinions, and claims that can paralyze or distract an enterprise from vital action. Business complexity is growing, dependencies are expanding, users are becoming more mobile, and the threats are evolving. New technology brings us great benefits, but it also means that our data and applications are now distributed across multiple locations, many of which are not within our organization's infrastructure. In this complex, interconnected world, no enterprise can think of its security as a standalone problem.

So how can we as a community -- the community-at-large, as well as within industries, sectors, partnerships, and coalitions -- band together to establish priority of action, support each other, and keep our knowledge and technology current in the face of a rapidly evolving problem and an apparently infinite number of possible solutions? What are the most critical areas we need to address and how should an enterprise take the first step to mature their risk management program? Rather than chase every new exceptional threat and neglect the fundamentals, how can we get on track with a roadmap of fundamentals, and guidance to measure and improve? Which defensive steps have the greatest value?

These are the kinds of issues that led to and now drive the CIS Controls. They started as a grassroots activity to cut through the "Fog of More" and focus on the most fundamental and valuable actions that every enterprise should take. And **value** here is determined by knowledge and data -- the ability to prevent, alert, and respond to the attacks that are plaguing enterprises today.

Led by CIS®, the CIS Controls have been matured by an international community of individuals and institutions that:

- Share insight into attacks and attackers, identify root causes, and translate that into classes of defensive action;

- Document stories of adoption and share tools to solve problems;
- Track the evolution of threats, the capabilities of adversaries, and current vectors of intrusions;
- Map the CIS Controls to regulatory and compliance frameworks and bring collective priority and focus to them;
- Share tools, working aids, and translations; and
- Identify common problems (like initial assessment and implementation roadmaps) and solve them as a community.

These activities ensure that the CIS Controls are not just another list of good things to do, but a prioritized, highly focused set of actions that have a community support network to make them implementable, usable, scalable, and compliant with all industry or government security requirements.

Why the CIS Controls Work: Methodology and Contributors

The CIS Controls are informed by actual attacks and effective defenses and reflect the combined knowledge of experts from every part of the ecosystem (companies, governments, individuals); with every role (threat responders and analysts, technologists, vulnerability-finders, tool makers, solution providers, defenders, users, policy-makers, auditors, etc.); and within many sectors (government, power, defense, finance, transportation, academia, consulting, security, IT) who have banded together to create, adopt, and support the Controls. Top experts from organizations pooled their extensive first-hand knowledge from defending against actual cyber-attacks to evolve the consensus list of Controls, representing the best defensive techniques to prevent or track them. This ensures that the CIS Controls are the most effective and specific set of technical measures available to detect, prevent, respond, and mitigate damage from the most common to the most advanced of those attacks.

The CIS Controls are not limited to blocking the initial compromise of systems, but also address detecting already-compromised machines and preventing or disrupting attackers' follow-on actions. The defenses identified through these Controls deal with reducing the initial attack surface by hardening device configurations, identifying compromised machines to address long-term threats inside an organization's network, disrupting attackers' command-and-control of implanted malicious code, and establishing an adaptive, continuous defense, and response capability that can be maintained and improved.

The five critical tenets of an effective cyber defense system as reflected in the CIS Controls are:

Offense informs defense: Use knowledge of actual attacks that have compromised systems to provide the foundation to continually learn from these events to build effective, practical defenses. Include only those controls that can be shown to stop known real-world attacks.

Prioritization: Invest first in controls that will provide the greatest risk reduction and protection against the most dangerous threat actors and that can be feasibly implemented in your computing environment. The CIS Implementation Groups are a great place for organizations to start identifying relevant Safeguards.

Measurements and Metrics: Establish common metrics to provide a shared language for executives, IT specialists, auditors, and security officials to measure the effectiveness of security measures within an organization so that required adjustments can be identified and implemented quickly.

Continuous diagnostics and mitigation: Carry out continuous measurement to test and validate the effectiveness of current security measures and to help drive the priority of next steps.

Automation: Automate defenses so that organizations can achieve reliable, scalable, and continuous measurements of their adherence to the Controls and related metrics.

Getting Started

The CIS Controls are a relatively small number of prioritized, well-vetted, and supported security actions that organizations can take to assess and improve their current security state. They also change the discussion from "What should my enterprise do?" to "What should we ALL be doing?" to improve security across a broad scale.

But this is not a one-size-fits-all solution, in either content or priority. You must still understand what is critical to your business, data, systems, networks, and infrastructures, and you must consider the adversarial actions that could impact your ability to be successful in the business or operation. Even a relatively small number of controls cannot be executed all at once, so you will need to develop a plan for assessment, implementation, and process management.