FORTRA™

DATASHEET (TRIPWIRE)

Meeting Multiple Compliance Objectives Simultaneously with the CIS Controls

Meet Broad Compliance Requirements Leveraging the Center for Internet Security's Controls and Benchmarks

The CIS Controls are a set of recommendations comprised of controls and benchmarks. They are intended to serve as a cybersecurity "best practice" for preventing damaging attacks. The recommendations are meant to provide a holistic approach to cybersecurity and to be effective across all industries. Adhering to them serves as an effective foundation for any organization's security and compliance programs.

Not to be confused with regulations such as PCI and HIPAA or frameworks such as NIST, compliance with CIS controls is not enforced within audits. However, the CIS Controls are considered to be the building blocks to nearly all major compliance frameworks. They map to frameworks such as the NIST 800-53, ISO 27000 series and regulations such as PCI DSS, HIPAA, NERC CIP, and FISMA.

The Controls were first developed in 2008 by an international conglomerate of cybersecurity professionals representing a broad array of organizations, from small companies to government agencies. Since then, the Controls have been regularly updated to keep pace with the evolution of technology ecosystems and emerging threat vectors.

The CIS Benchmarks

The CIS Benchmarks are similar to the Controls, except the Benchmarks provide prescriptive guidelines for ensuring that operating systems, hardware, and devices are securely configured. There are more than 100 CIS Benchmarks, covering more than 25 vendor product families. CIS Benchmarks have been adopted by a number of industry frameworks, such as PCI DSS, FISMA, and FFIEC.

CIS Benchmarks exist for a variety of platforms, cloud providers, mobile devices, and more. Some examples include AWS, Google Cloud Computing, and Zoom. Adhering to these benchmarks is your best chance at ensuring that the data you relay to third parties is secure.

TRIPWIRE TIP

You can learn the specifics of how the CIS Controls map to various industry frameworks by visiting the CIS Controls Navigator and selecting your various compliance needs. The results will tell you exactly which requirements are met by which control(s).

How the CIS Controls Map to Other Policies

PCI DSS

PCI DSS (Payment Card Industry Data Security Standard) is the standard responsible for protecting the credit card industry from digital fraud. The standard ensures that cardholder's information remains in the right hands and limits the liability of card issuers and banks in the event that a merchant is breached.

The CIS Benchmarks and CIS Controls address a variety of aspects of PCI-DSS compliance, including:

- 1 – Firewall and Router Configurations
- 6.1 – Patch Management
- 6.4 – Change Control
- 7.1 – Access Control

NIST

NIST is the framework that guides federal information systems in the United States. The framework offers guidance on producing positive cybersecurity outcomes and on the protection of privacy and civil liberties in a cybersecurity context. The CIS Benchmarks and Controls address many different portions of NIST compliance, including:

- NIST SP 800-53 R4 Low Baseline
- NIST SP 800-171 r2

It is also important to note that the Federal Information Security Modernization Act (FISMA) regulatory standard, which serves as a portion of NIST, references CIS Controls and Benchmarks as acceptable compliance resources.

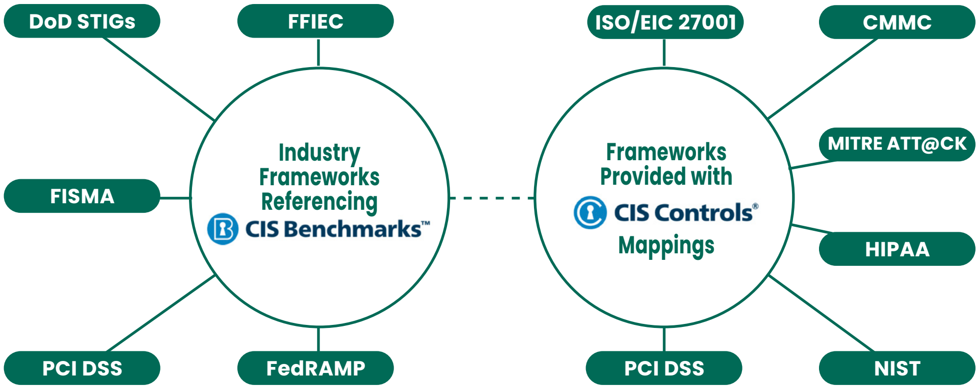
Other Standards and Frameworks

NIST and PCI DSS both use CIS Controls and Benchmarks as integral components of their compliance, but CIS coverage does not stop there—it extends into a multitude of other standards and frameworks, such as HIPAA, NERC CIP, and GDPR. Each of these recognizes the controls and benchmarks as excellent digital hygiene and endorses their effectiveness through the role they play in their respective compliance requirements.

Summary

No matter the industry you are in, the framework that you must adhere to, or even the size of your organization, adopting and upholding the CIS Controls and Benchmarks is an essential element to any compliance or network hardening program. These controls are by and for cybersecurity professionals of all roles and industries, making them the most well rounded path to defense and compliance imaginable. Heed the advice of the global cybersecurity community and fully embrace the CIS Controls.

The CIS Controls are "mapped" to other frameworks while the CIS Benchmarks are "referenced" as being acceptable standards. Additionally, CIS Benchmarks recommendations are mapped to the CIS Controls.



About Fortra

Fortra is a cybersecurity company like no other. We're creating a simpler, stronger future for our customers. Our trusted experts and portfolio of integrated, scalable solutions bring balance and control to organizations around the world. We're the positive changemakers and your relentless ally to provide peace of mind through every step of your cybersecurity journey. Learn more at fortra.com.

FORTRA™

Fortra.com