Texas Department of Family and Protective Services
Office of Information Security

DFPS External Partners and CIS Critical Security Controls Implementation Groups

CIS Controls (formerly called CIS Critical Security Controls) is a resource that the Center of Internet Security (CIS) publishes as a comprehensive best-practice guide for system and network security. The guide contains a checklist of 20 safeguards and actions that are high priority and have proven effective against the most pervasive and destructive cybersecurity threats on IT systems.

CIS Controls map to most of the major standards and regulatory frameworks, such as these:

- National Institute of Standards and Technology (NIST) Cybersecurity Framework
- NIST 800-53
- Health Insurance Portability and Accountability Act (HIPAA), Payment Card Industry Data Security Standard (PCI DSS), Federal Information Security Management Act (FISMA), and others in the ISO 27000 series of standards
- CIS Controls give you a starting point for following any of these compliance frameworks.

CIS Critical Security Controls Navigator

Use this page to learn more about the Controls and Safeguards and see how they map to other security standards

Implementation Groups (IGs) are the recommended guidance to prioritize implementation of the CIS Critical Security Controls (CIS Controls).

CIS Critical Security Controls Implementation Group 1

In most cases, an IG1 enterprise is typically small to medium-sized with limited IT and cybersecurity expertise to dedicate towards protecting IT assets and personnel. A common 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.

CIS Critical Security Controls Implementation Group 2

An IG2 enterprise employs individuals who are responsible for managing and protecting IT infrastructure. These enterprises typically 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 can withstand short interruptions of service. A major concern is loss of public confidence if a breach occurs.

IG2 is comprised 74 additional Safeguards and builds upon the 56 Safeguards identified in IG1.

The 74 Safeguards selected for IG2 can help security teams cope with increased operational complexity. Some Safeguards will depend on enterprise-grade technology and specialized expertise to properly install and configure.

CIS Critical Security Controls Implementation Group 3

An IG3 enterprise commonly 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**.**

IG3 is comprised of an additional 23 Safeguards. It builds upon the Safeguards identified in IG1 (56) and IG2 (74) totaling the 153 Safeguards in CIS Controls v8.

Where should I begin?

Begin by downloading and reading the 4-page summary of the CIS Implementation Groups. This document illustrates how CIS divides cybersecurity into various topics and provides an overview of all the safeguards in the context of the control they belong to.

Next, download the CIS Critical Security Controls® v8 Excel workbook. Reading the detailed descriptions of the many safeguards in the worksheet Controls V8 will give you a good understanding of the scope of the controls, how they are grouped and which are applicable to your business.

Then, to conduct the cybersecurity assessment of your organization, download the CIS Critical Security Control v8.0 Assessment Tool from the AuditScripts website. This assessment tool expands on the CIS Excel workbook by providing:

1. Dropdown lists of choices for assessment conclusions.
2. A dashboard that shows the results of your assessment graphically.
3. An assessment summary of results for each control.
4. More detailed instructions for conducting the cybersecurity assessment.

The effort required to conduct the cybersecurity assessment of your organization is typically one to two days.

The first cybersecurity assessment will form the baseline of the state of your cybersecurity defenses. By repeating the assessment every year, you can demonstrate continuous improvement.

Cybersecurity Risk Assessment by DFPS Office of Information Security

Cybersecurity risk assessments of new and existing contracts and partners are required by the Department of Information Resources and the DFPS Office of Information Security.

External Partners who interface with applications that are critical to DFPS are considered IG2 or IG3 are contractually required to conduct an audit such as System and Organization Control (SOC) 2 Type II, AICPA SSAE 18 review, or an IT General Controls or Application audit conducted by a certified auditor demonstrating that appropriate network and computing security safeguards and controls are in place.

Additionally, the external partners who fall under the aforementioned requirements must conduct a vulnerability assessment, such as a network penetration test, by an external, third-party on an annual basis to validate network and computing security controls are in place and functioning properly.

For more information on contractual cybersecurity requirements, please visit the DFPS Contractor Data and System Security Requirements.

Resources

CIS Controls

- v8 Resources and Tools
- Learn about Implementation Groups
- View All 18 CIS Controls