

INTRODUCTION

[The Essential Guide to Election Security](#)

MATURITY

[Maturities](#)

[Determining Your Maturity Level](#)

[Prioritizing Best Practices for the Level 1 maturity](#)

[Prioritizing Best Practices for the Level 2 and Level 3 maturities](#)

BEST PRACTICES

[Index of Best Practices](#)

[Addressing Physical Threats](#)

[Join the EI-ISAC](#)

[Asset Management](#)

[Encrypt Data at Rest](#)

[Encrypt Data in Transit](#)

[Managing Infrastructure with Secure Configurations](#)

[User Management](#)

[Backups](#)


[Incident Response Planning](#)

[Building and Managing Staff](#)

[Patching and Vulnerability Management](#)

[Remediate Penetration Test Findings](#)

[Perform Internal Penetration Test](#)

v: latest

# Implementing the CIS Controls

The CIS [Critical Security 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. They are developed by a consensus-based community of cybersecurity experts and are globally accepted security best practices.

Within each of the 18 CIS Controls is a set of safeguards focused on a specific security function. There are a total of 153 safeguards. Experience has shown that organizations of every size and complexity need help to get started with the CIS Controls, and to focus their attention and resources.

CONTROL 01 Inventory and Control of Enterprise Assets	CONTROL 02 Inventory and Control of Software Assets	CONTROL 03 Data Protection
CONTROL 04 Secure Configuration of Enterprise Assets and Software	CONTROL 05 Account Management	CONTROL 06 Access Control Management
CONTROL 07 Continuous Vulnerability Management	CONTROL 08 Audit Log Management	CONTROL 09 Email and Web Browser Protection
CONTROL 10 Malware Defenses	CONTROL 11 Data Recovery	CONTROL 12 Network Infrastructure
CONTROL 13 Network Monitoring and Defense	CONTROL 14 Security Awareness and Skills Training	CONTROL 15 Service Provider Management
CONTROL 16 Applications Software Security	CONTROL 17 Incident Response Management	CONTROL 18 Penetration Testing

The CIS Implementation Groups ([IGs](#)) were created to address this need. These IGs provide a simple and accessible way to help organizations of different classes focus their scarce security resources, and still leverage the value of the CIS Controls program, community, and complementary tools and working aids.

The CIS Controls are organized into IGs, each with its own unique list of Safeguards. The IGs are defined according to three attributes:

1. Data sensitivity and criticality of services offered by the organization
2. Expected level of technical expertise exhibited by staff or on contract
3. Resources and expertise available and dedicated toward cybersecurity activities

This results in three IGs, and the maturities in this Guide are loosely based on those IG classifications:

- **IG1: Basic.** Contains controls that help an organization assess its current security and take simple steps to improve it. Roughly equivalent to the Level 1 maturity.
- **IG2: Foundational.** Contains more advanced guidance to improve an organization's security. Roughly equivalent to the Level 2 maturity.
- **IG3: Organizational.** Contains controls that make changes to an organization's policies to improve and maintain their cybersecurity. Roughly equivalent to the Level 3 maturity.

## Goals

1. Implement the appropriate IGs for your organization (Level 1 maturity)

## Actions

For Implementing the CIS Controls, the necessary actions vary by maturity as detailed below.

### Level 1 Maturity

1. Implement the IG1 controls.
  - The easiest way to do this is through the Level 1 [Priorities](#). This will help you complete all of the actions for the Level 1 maturity, including IG1.
  - You can also use the [CIS Controls Navigator](#) to get to export a convenient list of the IG1 controls.

### Level 2 Maturity

Organizations operating at a Level 2 maturity should take additional actions, including:

1. Implement the IG2 controls. Use the [CIS Controls Navigator](#) to get this done.

### Level 3 Maturity

Organizations operating at a Level 3 maturity should take additional actions, including:

1. Implement all of the CIS Controls that are applicable for your environment. Use the [CIS Controls Navigator](#) to get this done.

## Cost-Effective Tools

- [CIS Controls Navigator](#): A simple tool to allow export of customized sets of safeguards from the CIS Controls.
- [CIS Controls version 8](#): 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.

## Mapping to CIS Controls and Safeguards

- All!

## Mapping to CIS Handbook Best Practices

- There are no relevant Handbook best practices



ON THIS PAGE

Goals

Actions

Level 1 Maturity

Level 2 Maturity

Level 3 Maturity

Cost-Effective Tools

Mapping to CIS Controls and Safeguards

Mapping to CIS Handbook Best Practices

