Implementing and Auditing CIS Controls

SANS training:
SEC566: Implementing and Auditing CIS Controls
sans.org/sec566 giac.org/gccc

SANS
CYBERSECURITY LEADERSHIP

Version 8 of the CIS Critical Security Controls

AND

Implementing and Auditing CIS Controls

For Cyber Leaders of Today and Tomorrow

sans.org/cybersecurity-leadership

@secleadership SANS Security Leadership
sansurl.com/leadership-discord
sansurl.com/leadership-youtube

LDR_CIS-Controls-v8_v1.6_0124

Maturity Values

SANS

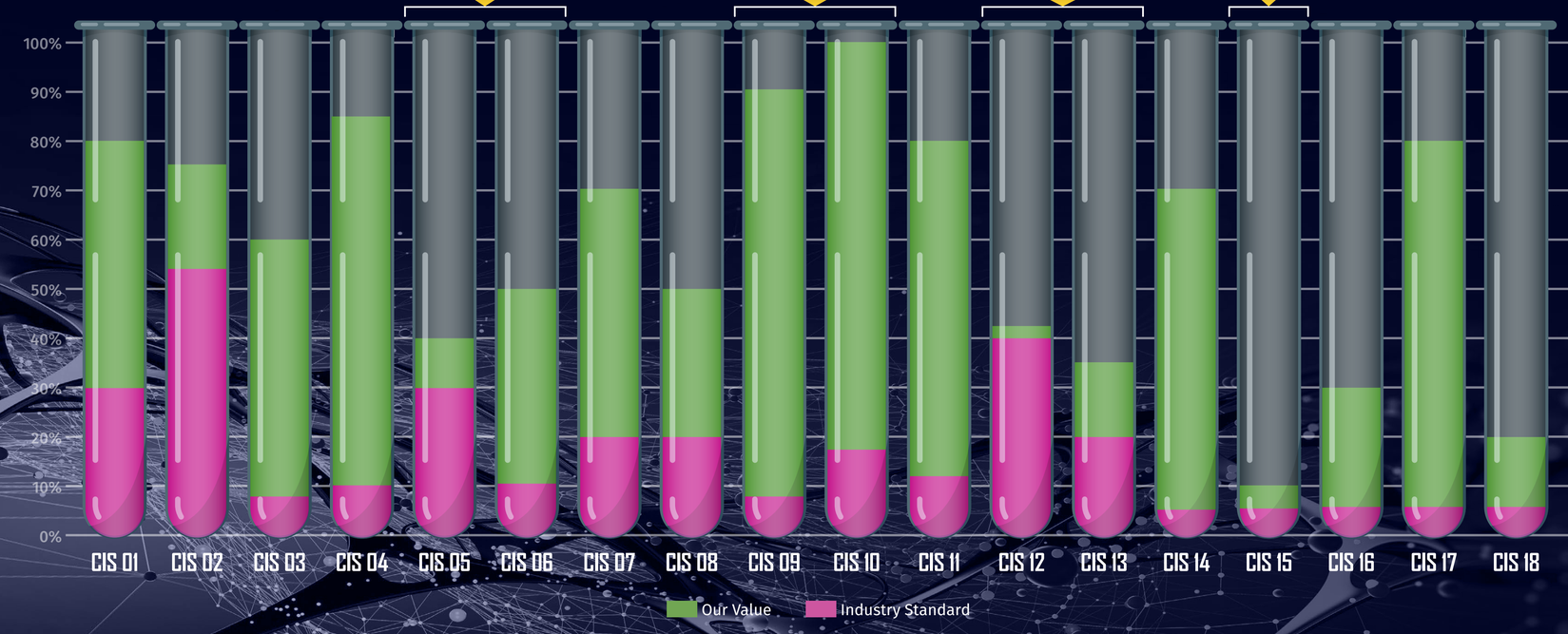
Measure and report: Show current progress against the industry.

Account management lower values indicate a need to focus on these two controls.

Data recovery and malware defense maturity is high reducing focus on these two controls.

Network hygiene maturity is low, segmentation, patching and configuration management is needed here.

Third-party management maturity is low, requiring focus.



The Big Picture

The CIS Controls are the bare minimum, low-water mark supporting and enabling advanced tools, controls and reporting.

Program Path

The CIS Critical Security Controls are designed to protect from the most likely and current attacks happening. To that end, there are some key milestones to ensure your program provides the best defenses and the business is informed.

IMPLEMENT
CIS Controls mitigate more than 90% of most common attacks.

MEASUREMENT
Identify successes and areas for improvement.

METRIC
Set goals to achieve and report to business leaders.

REPORTING TO BUSINESS
The CIS Critical Security Controls are designed to reduce cyber-related risk. The control measures and metrics provide the orgsnization with control-based risk, enabling business units to make responsible decisions.

AUTOMATION
To ensure consistency and efficiency of safeguards, automation of the controls is key.

CIS Controls

Welcome to Version 8 of the CIS Critical Security Controls

Creating Confidence in the Connected World.™

Critical Security Controls v8

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

153 TOTAL SAFEGUARDS

The number of Safeguards an enterprise is expected to implement increases based on which group the enterprise falls into.

IG1 — 56 SAFEGUARDS

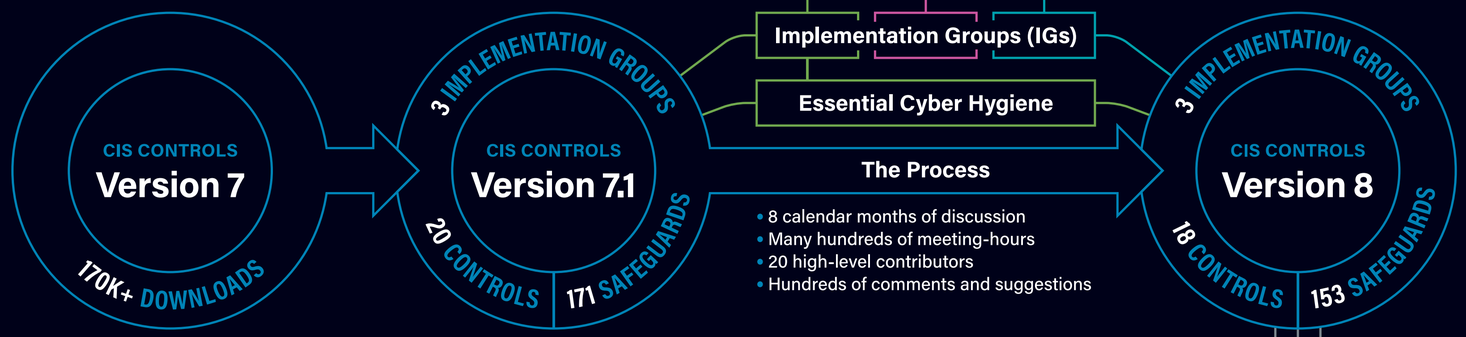
IG1 is the definition of essential cyber hygiene and represents a minimum standard of information security for all enterprises. IG1 assists enterprises with limited cybersecurity expertise thwart general, non-targeted attacks.

IG2 — 74 SAFEGUARDS

IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity.

IG3 — 23 SAFEGUARDS

IG3 assists enterprises with IT security experts to secure sensitive and confidential data. IG3 aims to prevent and/or lessen the impact of sophisticated attacks.



Guides Cloud • Mobile • Microsoft Windows 10 • Telework & Small Medium Businesses (SMB) • Community Defense Model (CDM)

Tools CIS Controls Assessment Specification • CIS Controls Self Assessment Tool (CSAT) • CIS Controls Navigator • CIS Risk Assessment Method (RAM)

Mappings NIST • CMMC • PCI • MITRE ATT&CK v6

CIS Center for Internet Security®

cisecurity.org

Thanks to our volunteer community, the CIS Critical Security Controls (CIS Controls) continue to grow in influence and impact across a world-wide community of adopters, vendors, and supporters.

Phyllis Lee

CIS Controls Tools

CIS CSAT Pro CONTROLS SELF ASSESSMENT TOOL
Helps teams track and document their progress in implementing the CIS Controls. Progress can be compared to industry averages.

CIS RAM RISK ASSESSMENT METHOD
A method and tool to let enterprises of varying security capabilities navigate the balance between implementing security controls, risks, and organizational needs.

CIS Controls Assessment Specification
Identifies specific tests for Safeguards that can be automated, and provides a specification for vendors to implement them.

CIS Controls Navigator
Online tool to compare CIS Safeguards with recommendations found in other security frameworks.

CIS WorkBench
CIS collaboration platform for volunteers and CIS staff to share ideas, develop content, and learn from each other.

CIS Community Defense Model
Identifies the security value of CIS Safeguards against specific attacks identified by open data sources, and described using the MITRE ATT&CK Framework.

Navigating an Ocean of Cyber Frameworks
Authoritative and vetted cross-mappings from our security best practices applied to well-known target frameworks or standards. For current versions and information on mappings, go to **www.cisecurity.org/controls/v8**