MS-ISAC®
government technology
ISAC Annual Summit
Stronger Starts Here
June 21-24
Orlando, FL
2026

Visualizing Security Posture

by Mapping Frameworks and Tools to the CIS Controls Framework

Valecia Stocchetti, *Senior Cybersecurity Controls Engineer, CIS*

Andy Boell, *Co-Founder and Developer, Viosoph and Midwest Cyber*

Your Presenters

Valencia Stocchetti
Center for Internet Security

Andy Boell
Midwest Cyber / Viosoph

Agenda

- The CIS Critical Security Controls Intro
- Implementation Groups (IGs)
- CIS Controls Mappings (to Frameworks)
- The Cost of Cyber Defense: IG1
- A Practitioner’s Approach to Implementation

CIS Controls Intro

Best Practice Guidance	• Prioritized set of defensive actions • Allows you to build and improve your cybersecurity program
Developed by Cybersecurity Experts	• We use a consensus-based process for soliciting feedback and using it for future versions of the Controls.
Globally Recognized	• Over 500,000 downloads since CIS took the reins
Internationally Adopted	• Adopted by ETSI • 60%+ International adoption

Earlier Controls History

NSA/DoD Project

CSIS The Consensus Audit Guidelines (CSIS)

SANS "The SANS Top 20" (the SANS Institute)

CIS Critical Security Controls The Critical Security Controls (CCS/CIS)

CIS Controls

CIS Controls v8.1

18 Top-Level Controls and 153 Safeguards

Implementation Groups (IGs)

Implementation Groups (IGs)

- IGs are based on the risk profile and resources an enterprise has available to them to implement the CIS Controls
- Every enterprise should start with IG1

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

153 TOTAL SAFEGUARDS

IG3 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. **23** SAFEGUARDS

IG2 IG2 assists enterprises managing IT infrastructure of multiple departments with differing risk profiles. IG2 aims to help enterprises cope with increased operational complexity. **74** SAFEGUARDS

IG1 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. **56** SAFEGUARDS

IG1 Backed by Data

What is the Security Value?

"The benefit"

The benefit a CIS Safeguard provides in defending against an individual attack, or group of attacks.

Takeaway

CIS Safeguards can defend against 90% or more of ATT&CK (sub-)techniques in each attack type.

IG1 CIS Safeguards can defend against 77% or more of ATT&CK (sub-)techniques in attack type.

Top 5 Attacks	IG1 CIS Safeguards IG1 can defend against XX% of ATT&CK (Sub-)Techniques	All CIS Safeguards CIS Safeguards can defend against XX% of ATT&CK (Sub-)Techniques
Malware	77%	94%
Ransomware	78%	92%
Web Application Hacking	86%	98%
Insider Privilege and Misuse	86%	90%
Targeted Intrusions	83%	95%

All percentages are based on ATT&CK (sub-)techniques assigned to an ATT&CK mitigation.

Mappings

Security and Compliance

Assisting enterprises who are working with other frameworks

Mappings

- CIS is committed to interoperability with other industry frameworks
- CIS maps to a variety of security standards and frameworks
- Join the CIS Controls Mapping Community on CIS WorkBench

Frameworks Provided with CIS Controls Mapping

Australian Signals Directorate Essential Eight	FFIEC-CAT	NERC-CIP	SOC 2
Azure Security Benchmark v3	GSMA FS 31 Baseline Security Controls	New Zealand Information Security Manual v3.5	TSA Security Defense Directive Pipeline
CISA Cybersecurity Performance Goals (CPGs)	HIPAA	NYS Department of Financial Services 23 NYCRR Part 500	UK Cyber Essentials
CMMC	ISACA COBIT 19	NIST CSF	UK National Cyber Security Centre (NCSC) Cyber Assessment v3.1
Criminal Justice Information Services (CJIS)	ISO 27001:2022	NIST SP 800-53 R5	
CSA Cloud Controls Matrix v4	ISO/IEC 27002:2022	NIST SP 800-171	
Cyber Risk Institute (CRI) Profile v1.2	MITRE ATT&CK v8.2	PCI DSS	

Industry Frameworks Referencing CIS Benchmarks

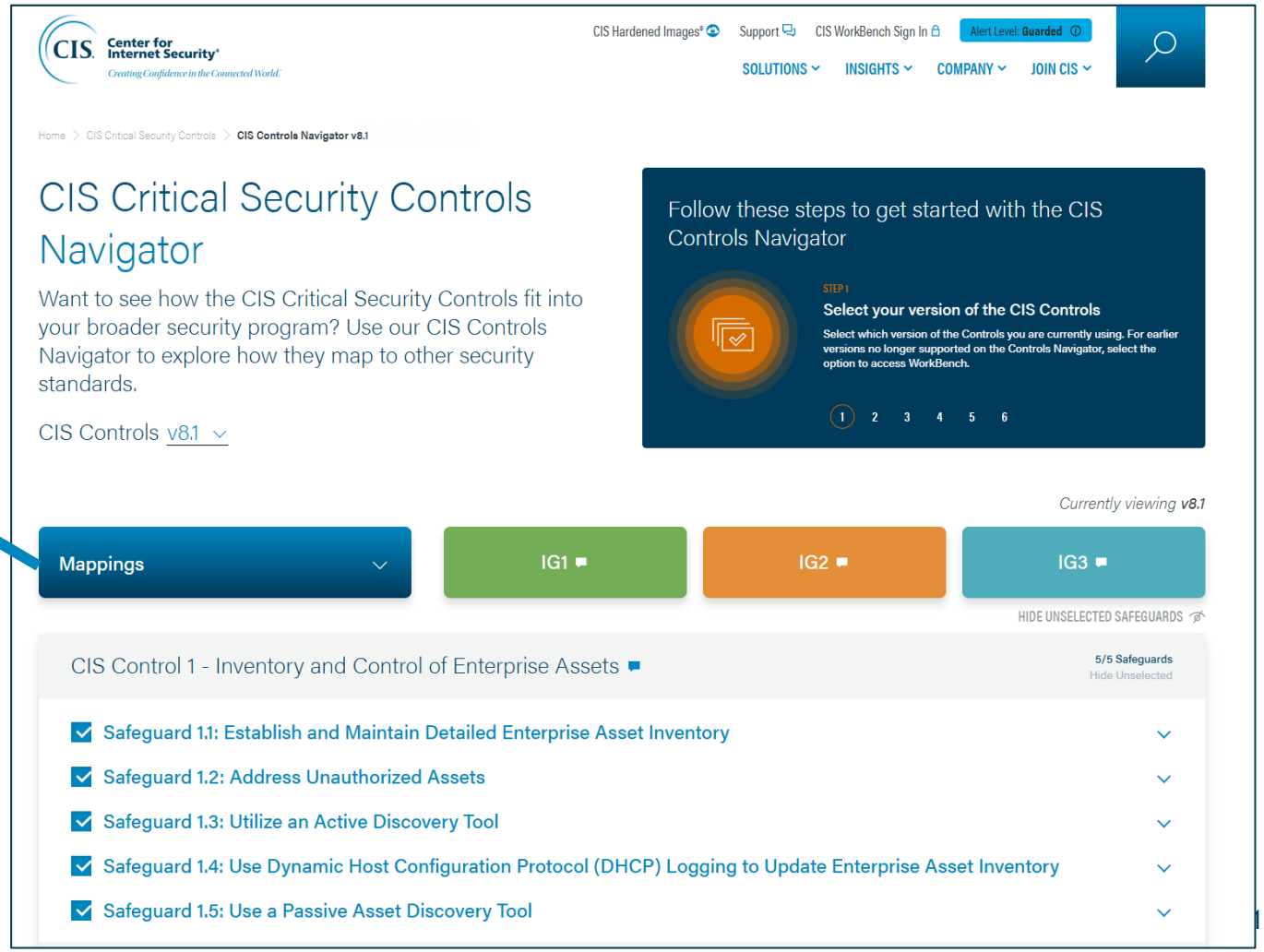
DISA STIGs	FISMA
FedRAMP	PCI DSS
FFIEC	

For mappings, please visit https://www.cisecurity.org/controls/cis-controls-navigator/

For our mappings community, please visit https://workbench.cisecurity.org/communities/94

CIS Controls Navigator

Assisting enterprises who are working with other frameworks



Cost of Cyber Defense: Implementation Group 1 (IG1)

The Cost of Cyber Defense Dilemma

Have You Ever Asked These Questions?

01

Which Safeguards to Start With?

Identify the right Safeguards for your organization

02

Which Tools Will Be Needed?

Tools required to implement each protection

03

How Much Will It Cost?

Get a clear picture of implementation investment

THE SOLUTION

Cost of Cyber Defense for IG1

WHY PUT A COST ON CYBER DEFENSE?

Strategic Planning

Data-driven resource for security roadmap planning

Leadership Buy-In

Evidence to secure executive and board support

Proactive vs. Reactive

Shift from emergency spending to proactive investment

Budget Forecasting

Plan and allocate resources with confidence and clarity

WHAT THE COST OF CYBER DEFENSE GUIDE OFFERS

Which Protections to Start With

CIS Controls IG1 safeguards prioritized for your organization

Tools to Implement Protections

Specific technologies mapped to each safeguard

Approximate Implementation Cost

Data-backed cost estimates for planning and budgeting

Data-Driven Answers

Answers the critical questions leadership needs to act

Breaking It Down By Tool

- 56 Safeguards
- 16 tools
- 10 policies
- Defends against over 70% of techniques used in the top five attack types

Category	Tool	Safeguards						
Asset Management	Enterprise Asset Management Policy/Process	1.1						
	Enterprise and Software Asset Management Tool	1.1	1.2	2.1	2.2	2.3	9.1	12.1
	Software Asset Management Policy/Process	2.1						
	Service Provider Management Tool	15.1						
Data Management	Data Management Policy/Process	3.1						
	Data Management Tool	3.2						
	Data Disposal Tool	3.5						
	Encryption Tool	3.6						
Secure Configurations	Secure Configuration Policy/Process	4.1	4.2					
	Configuration Management Tool	4.1	4.2	4.3	4.6	4.7	5.4	10.3
	Firewall	4.4	4.5					
Account and Access Control Management	Account and Credential Management Policy/Process	6.1	6.2					
	Identity and Access Management Tool	3.3	3.4	5.1	5.3	5.4		
	Password Management Tool	5.2						
	Multi-Factor Authentication Tool	6.3	6.4	6.5				
Vulnerability Management	Vulnerability/Patch Management Policy/Process	7.1						
	Vulnerability/Patch Management Tool	7.2	7.3	7.4				
Log Management	Log Management Policy/Process	8.1						
	Log Management Tool	8.2	8.3					
Malware Defense	Anti-Malware Software	10.1	10.2					
	DNS Service/Server	9.2						
Data Recovery	Data Recovery Policy/Process	11.1						
	Data Backup and Recovery Tool	11.2	11.3	11.4				
Security Training	Security Training and Awareness Policy/Process	14.1						
	Security Training and Awareness Tool(s)	14.2	14.3	14.4	14.5	14.6	14.7	14.8
Incident Response	Incident Response Planning	17.1	17.2	17.3				

How to Calculate Cost

Tooling

- **Majority of tools are priced one of five ways**
  - Number of Employees
  - Number of Users
  - Number of Workstations
  - Number of IT Administrators
  - Size of Log Data
- **Types of Tools**
  - Commercially-supported
  - Open-source
  - No-cost (free)

How to Calculate Cost

IG1 Enterprise Profiles

- **Create Model Tiers (IG1 Enterprise Profiles)**
  - No two enterprises will be the same!
  - Guidance, but not absolute calculations
  - Cyber/Information Technology budgets will vary
  - Can estimate per person ($5,000 pp)

Company Size	Employee Count	Number of IT Staff	Number of Servers	Number of Workstations	Number of Total Systems	Size of Logs[4]	Annual Revenue	Annual IT Budget (5%)	Annual Cyber-security Budget (20% of IT Budget)
Tier 1	1 to 10	1[5]	1 to 2	1 to 12	1 to 14	0–100 GB/ Month	$0–$5,000,000	$0–$250,000	$0–$50,000
Tier 2	10 to 100	1 to 2	2 to 5	12 to 115	14 to 120	100–300 GB/Month	$5,000,001–$50,000,000	$250,001–$2,500,000	$50,001–$500,000
Tier 3	100 to 999	2 to 10	5 to 50	115 to 1,149	120 to 1,199	Up to 1,500 GB/Month	$50,000,001–$500,000,000	$2,500,001–$25,000,000	$500,001–$5,000,000

How to Calculate Cost

Things to Keep in Mind

- Every tool has its pros/cons
- Open source does not equal free
- No-cost tools still come with a cost
- Each enterprise is different
- Sometimes, a tool can be multi-purpose (e.g., A tool used in IT, also used by the Security Office)
- Tool is the *enabler*, not the *decider* on whether or not to implement a Safeguard

How to Calculate Cost

The Results

IG1 can be implemented for a relatively low cost and small number of tools

Category	Cost Range Tier 1			Cost Range Tier 2			Cost Range Tier 3		
	Max Cyber Budget: $50,000			Max Cyber Budget: $500,000			Max Cyber Budget: $5,000,000		
	No-Cost	Low	High	No-Cost	Low	High	No-Cost	Low	High
Asset Management	$0	$556	$2,044	$0	$690	$3,896	$0	$790	$18,414
Data Management	$0	$1,148	$14,566	$0	$11,192	$41,918	$0	$87,027	$387,867
Secure Configurations	$0	$968	$9,008	$0	$4,710	$47,494	$0	$18,138	$269,263
Account and Access Control Mgmt.	$0	$1,579	$4,025	$0	$7,063	$39,240	$0	$29,412	$388,728
Vulnerability Management	$0	$345	$1,969	$0	$845	$7,200	$0	$5,285	$64,746
Log Management	$0	$88	$2,520	$0	$632	$10,866	$0	$3,543	$54,000
Malware Defense	$0	$452	$1,399	$0	$5,591	$10,799	$0	$44,870	$107,898
Data Recovery	$0	$650	$2,143	$0	$2,925	$11,888	$0	$28,275	$118,701
Security Training	$0	$120	$450	$0	$1,440	$3,660	$0	$3,420	$36,570
Incident Response	$0	$0	$0	$0	$0	$0	$0	$0	$0
TOTAL	**$0**	**$5,906**	**$38,124**	**$0**	**$35,088**	**$176,961**	**$0**	**$220,760**	**$1,446,187**

The Cost Broken Down By Tool

Tool	Cost Range Tier 1			Cost Range Tier 2			Cost Range Tier 3		
	No-Cost	Low	High	No-Cost	Low	High	No-Cost	Low	High
Enterprise Asset Management Policy/ Process	$0	$0	$0	$0	$0	$0	$0	$0	$0
Enterprise and Software Asset Management Tool	$0	$400	$1,549	$0	$195	$2,600	$0	$295	$15,474
Software Asset Management Policy/ Process	$0	$0	$0	$0	$0	$0	$0	$0	$0
Service Provider Management Tool	$0	$156	$495	$0	$495	$1,296	$0	$495	$2,940
SUBTOTAL	**$0**	**$556**	**$2,044**	**$0**	**$690**	**$3,896**	**$0**	**$790**	**$18,414**

Mappings to Tools/Resources

For CIS and MS- and EI-ISAC Offerings

Category	Tool	Safeguards	CIS, MS/EI-ISAC Tools
Asset Management	Enterprise Asset Management Policy/Process	1.1	• CIS Controls Enterprise Asset Management Policy Template
	Enterprise and Software Asset Management Tool	1.1, 1.2, 2.1, 2.2, 2.3, 9.1, 12.1	• CIS Controls Asset Tracking Spreadsheet
	Software Asset Management Policy/Process	2.1	• CIS Controls Software Asset Management Policy Template
	Service Provider Management Tool	15.1	
Data Management	Data Management Policy/ Process	3.1	• CIS Controls Data Management Policy Template
	Data Management Tool	3.2	• CIS Controls Asset Tracking Spreadsheet
	Data Disposal Tool	3.5	
	Encryption Tool	3.6	
Secure Configurations	Secure Configuration Policy/ Process	4.1, 4.2	• CIS Controls Secure Configuration Management Policy Template
	Configuration Management Tool	4.1, 4.2, 4.3, 4.6, 4.7, 5.4, 10.3	• CIS Benchmarks™ (PDF versions) – Best Practice Guidance • CIS-CAT®14 Lite – Tool for implementing Best Practice Guidance • CIS SecureSuite® Membership (Includes CIS-CAT® Pro, CIS Build Kits, and CIS Benchmarks™ in Word, Excel, XML versions) – No-Cost to SLTTs15 • CIS Hardened Images®
	Firewall	4.4, 4.5	• CIS Benchmarks™ (PDF versions) – Best Practice Guidance • CIS-CAT® Lite – Tool for implementing Best Practice Guidance • CIS SecureSuite® Membership (Includes CIS-CAT® Pro, CIS Build Kits, and CIS Benchmarks™ in Word, Excel, XML versions) – No-Cost to SLTTs - Best Practice Guidance • CIS Hardened Images®
Account and Access Control Management	Account and Credential Management Policy/Process	6.1, 6.2	• CIS Controls Account and Credential Management Policy Template
	Identity and Access Management Tool	3.3, 3.4, 5.1, 5.3, 5.4	
	Password Management Tool	5.2	• CIS Controls Password Policy Guidance
	Multi-Factor Authentication Tool	6.3, 6.4, 6.5	

Category	Tool	Safeguards	CIS, MS/EI-ISAC Tools
Vulnerability Management	Vulnerability/Patch Management Policy/Process	7.1	• CIS Controls Vulnerability Management Policy Template
	Vulnerability/Patch Management Tool	7.2, 7.3, 7.4	
Log Management	Log Management Policy/ Process	8.1	• CIS Controls Audit Log Management Policy Template
	Log Management Tool	8.2, 8.3	• CIS Benchmarks™ (PDF versions) – Best Practice Guidance • CIS-CAT® Lite – Tool for implementing Best Practice Guidance • CIS SecureSuite® Membership (Includes CIS-CAT® Pro, CIS Build Kits, and CIS Benchmarks™ in Word, Excel, XML versions) – No-Cost to SLTTs • CIS Hardened Images®
Malware Defense	Anti-Malware Software	10.1, 10.2	• CIS Endpoint Security Services (ESS) - SLTTs only
	DNS Service/Server	9.2	• MS-ISAC® and EI-ISAC® Service: Malicious Domain Blocking and Reporting (MDBR) service – MS-/EI-ISAC Members only
Data Recovery	Data Recovery Policy/Process	11.1	• CIS Controls Data Recovery Policy Template
	Data Backup and Recovery Tool	11.2, 11.3, 11.4	
Security Training	Security Training and Awareness Policy/Process	14.1	• CIS Controls Security Awareness Skills Training Policy Template
	Security Training and Awareness Tool(s)	14.2, 14.3, 14.4, 14.5, 14.6, 14.7, 14.8	• MS-ISAC® Advisories/Newsletter Subscription – Available to everyone • MS-ISAC® Cybersecurity Awareness Toolkit – SLTTs only
Incident Response	Incident Response Planning	17.1, 17.2, 17.3	• MS-ISAC® and EI-ISAC® Service: Cyber Incident Response Team (CIRT) - SLTTs only

CSP and MSP Considerations

Environmental Shift

- Strictly on-premise environments are a thing of the past
- Hybrid environments are now the norm

Shared Responsibility Model

- "Who is responsible for what and when?"
- Especially critical to define before an incident occurs
- Best way is through contracts/agreements

Service Offerings

- One tool or service can cover multiple Safeguards
- Some services offered (e.g., Threat Intelligence) may fall outside the scope of Controls
- Policy templates generally not outsourced
- Not all services will be fully covered by a CSP and/or MSP

Cost is Highly Variable

- Dependent on number of end-users, endpoints, applications, and scope of services
- Cost calculations are complex
  - Dependent on volume of data accessed, stored, or transmitted to a service provider

Crossover of Budgets

- Budget structures vary with MSPs and CSPs
- Some tools may reside with IT but be used by Security, and vice versa
  - Shared budget line items are also common
- Can be beneficial for organizations with smaller cybersecurity budgets
  - IT can purchase more expensive tooling that is also leveraged by the security team

Cost of Cyber Defense v1.1 Highlights

- Accounts for hybrid and multi-tenant environments
  - Includes mapping to major cloud providers: AWS, GCP, and Azure
  - Designed to reflect today's complex enterprise environments
- 100% of Safeguards can be outsourced to an MSP
- 80% of Safeguards can be outsourced to a CSP

Key Takeaways

- The data provided within the report gives end users a guide for budget forecasting as it pertains to the tools available
- The tool itself is the enabler, not the decider on whether to implement a Safeguard
- IG1 can be implemented for a relatively low cost and small number of tools

A Practitioner's Approach to Implementation

The Practice Gap

Good guidance exists. Implementing it is another story.

The organizations under the most pressure — school districts, local governments, small businesses, nonprofits — face the same threats as the enterprise with a fraction of the staff, budget, and expertise.

No dedicated staff

Security is one more hat worn by an IT generalist — or no one at all.

No slack in the budget

Every tool and every hour competes with the mission they actually exist to serve.

No room for error

A single misstep can mean a breach, a failed audit, or lost funding.

One Organization, Many Rulebooks

The same control, re-documented in a different dialect for every framework

Almost no one answers to the CIS Controls alone. A typical organization is simultaneously accountable to:

- **CIS Controls v8.1**
- **NIST CSF 2.0**
- **NIST 800-171 / CMMC**
- **HIPAA Security Rule**
- **PCI DSS**
- **State & Sector Mandates**
- **Cyber Insurance Forms**

The hidden cost: The underlying controls of these frameworks share significant common ground, yet keeping that alignment current across frameworks remains a largely manual process, one that requires ongoing attention as frameworks evolve.

From Safeguard to Tool

Knowing a Safeguard exists is not the same as knowing what satisfies it

What the guidance gives you

- 56 IG1 Safeguards to implement
- ~16 categories of tooling
- 10 supporting policies
- A mapping of Safeguards to tool types

What you still have to answer

- Which specific product satisfies which Safeguard?
- Where does one tool cover several at once?
- Where am I paying twice for the same coverage?
- Where is a Safeguard quietly going unmet?

The result: teams buy overlapping tools, carry redundant spend, and still leave real coverage gaps — because the tool inventory is never reconciled against the safeguards.

Where Do You Even Start?

Even IG1 is a long list when there is no security team behind it

56

IG1 Safeguards — all essential

You cannot do all 56 on day one. So which first?

Sound prioritization should follow risk:

- what attackers are actively exploiting today
- the techniques behind the top attack types
- the realities of your own environment

Without that lens, scarce dollars get spent easiest-first or vendor-led — not where they reduce the most risk.

Can You Trust the Tool Itself?

A Safeguard satisfied by a risky product just trades one risk for another

AUTHORIZED	Is the vendor formally authorized — FedRAMP, or StateRAMP / GovRAMP for SLTT?
VALIDATED	Is the cryptography independently validated — FIPS 140-2 / 140-3?
EXPLOITED	Does it carry a vulnerability on CISA's Known Exploited Vulnerabilities (KEV) catalog?
SECTOR FIT	Does it meet sector bars — HECVAT for education, HITRUST for healthcare?
ATTESTED	Is data handling independently attested — SOC 2, CSA STAR?

Links and Resources

Other Resources

- CIS Controls v8.1
- CIS Policy Templates
- CIS Companion Guides/Resources
- CIS Controls Navigator (Mappings)
- CIS Controls Assessment Specification
- CIS Risk Assessment Method (RAM)
- CIS-Hosted CSAT
- CIS Benchmarks
- CIS Hardened Images
- CIS Build Kits
- CIS CIS-CAT Pro
- CIS WorkBench
- CIS SecureSuite Membership
- CIS SecureSuite Platform

Contact Us

- **Website:** www.cisecurity.org
- **Email:** ControlsInfo@cisecurity.org
- **Twitter:** @CISecurity
- **Facebook:** Center for Internet Security
- **LinkedIn:** Center for Internet Security
  CIS Critical Security Controls

BEFORE YOU GO

FrameworkMapper

by Viosoph • The Way of Wisdom

Built on the CIS Controls — the same mapping approach we walked through today.

Learn more: frameworkmapper.com

Let’s connect after the session

Thank You