Center for Internet Security®

standards and frameworks and controls oh my!

Mike Garcia

Senior Advisor for Elections Best Practices

mike.garcia@cisecurity.org

The big three…in their own words

ISO 27000: family of standards to help organizations manage the security of assets such as financial information, intellectual property, employee details and [3rd party] information.

NIST CSF: prioritized, flexible, and cost-effective framework to manage cybersecurity-related risk. Helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

CIS Controls: a concise, prioritized set of cyber practices created to stop today's most pervasive and dangerous cyber attacks.

Questions?

Mike Garcia
Senior Advisor for Elections Best Practices
mike.garcia@cisecurity.org

More specifically…

ISO 27000: **family of standards** to help organizations manage the security of assets such as financial information, intellectual property, employee details and 3rd party information.

NIST CSF: prioritized, flexible, and cost-effective **framework** to manage cybersecurity-related risk. Helps to promote the protection and resilience of critical infrastructure and other sectors important to the economy and national security.

CIS Controls: a concise, prioritized set of **cyber practices** created to stop today's most pervasive and dangerous cyber attacks. The Controls are developed, refined, and validated by a community of leading experts from around the world.

More simply…

ISO 27000: **family of standards**

NIST CSF: **framework**

CIS Controls: **actions**

In one bullet…

ISO 27000: **family of standards**

- policy and process, less tactical

NIST CSF: **framework**

- puts the organize in your organization

CIS Controls: **cyber practices**

- the things you put in place to get results

What they have in common

All drive a standardized approach to security

- Standard here means repeatability and comparability; they turn amorphous cybersecurity blah blah into apples

All are developed with an open, consensus-based approach

- Experts gather, exfoliate brilliance, reach consensus

All work for all orgs regardless of size or substance

- The content is applicable to all; it's up to the org to place the goalpost

They get along but serve different purposes

ISO 27000

Pros

- About establishing appropriate conditions to do the right thing
- Something for everyone: a great deal of detail, including governance, privacy, supply chain
- High specificity, including sector-specific for different sectors such as energy, health, teleco, cloud

Cons

- Requires substantial expertise to understand and implement
- Can be costly to very small orgs
- Rather overwhelming to navigate

NIST Cybersecurity Framework

Pros

- (Mostly) understandable by non-technical readers
- Can be completed quickly or in great detail to suit the orgs needs
- Has a ‘self-contained’ maturity model—helps you understand what’s right for your org and track to it
- Highly flexible for different types of orgs

Cons

- Better suited for diagnostic, organizational, and planning than for executing
- Helps you focus; doesn’t tell you what to do or how to do it

CIS Controls

Pros

- Prioritized and concise
- Action oriented: provides technical implementation information
  - i.e., use a tool to do this, deploy controls to do that
- Relatively rapid updates

Cons

- Less tailored to discuss overall organizational posture at an executive level
- Partial maturity model (but v7.1 should fix this)

ISO 27000

Just a dip of the big toe…

- 27000: Overview and vocabulary
- 27001: Requirements
- 27002: Code of practices for information security controls
- 27003: Guidance
- 27004: Monitoring, measurement, analysis, and evaluation
- 27005: Information security risk management
- 27006: Requirements for bodies providing audit and certification of information security management systems
- 27007: Guidelines for information security management systems auditing
- 27008: Guidelines for auditors on information security controls

And the other big toe…

- 27009: Sector-specific application of ISO/IEC 27001 — Requirements
- 27010: Information security management for inter-sector and inter-organizational communications
- 27011: Code of practice for information security controls based on ISO/IEC 27002 for telecommunications organizations
- 27013: Guidance on the integrated implementation of ISO/IEC 27001 and ISO/IEC 20000-1
- 27014: Governance of information security
- 27016: Organizational economics
- 27017: Code of practice for information security controls based on ISO/IEC 27002 for cloud services
- 27018: Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors
- 27019: Information security controls for the energy utility industry
- 27021: Competence requirements for information security management systems professionals
- 27799: Information security management in health using ISO/IEC 27002

But ISO 27000 doesn't have to be scary…

27000 family focus on how to develop a system and making sure you use that system in a secure way

- Helps with the policies, procedures, people, assets that need to be managed and how to make them work in a system

Example:

- ISO 27002, 15.1 on supplier relationships
- Details how to develop a policy for supplier access to organizational information.

NIST Cybersecurity Framework

Truly a framework

Gives orgs “a common taxonomy and mechanism to:

1. Describe their current cybersecurity posture;
2. Describe their target state for cybersecurity;
3. Identify and prioritize opportunities for improvement within the context of a continuous and repeatable process;
4. Assess progress toward the target state;
5. Communicate among internal and external stakeholders about cybersecurity risk.”

5 **functions**, 23 **categories**, and 108 **subcategories**

Has implementation **tiers** for maturity and **profiles** to customize

Truly a framework

Example:

- Function: **Protect (PR)**
- Category: **Identity Management, Authentication and Access Control (PR.AC)**: Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.
- Subcat: **PR.AC-1**: Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes
- References include CIS Controls 1, 5, 15, 16

CIS Controls

A complete but not overwhelming model

Informed by 5 tenets:

- Offense informs defense
- Prioritization
- Measurements and Metrics
- Continuous diagnostics and mitigation
- Automation

20 controls encompassing a total of 171 sub-controls

Organized into 3 sets: basic, foundational, organizational

Starting in v7.1, sub-controls are organized into 3 implementation group to help implement a maturity model

CIS Controls Version 7

Basic

1. Inventory and Control of Hardware Assets
2. Inventory and Control of Software Assets
3. Continuous Vulnerability Management
4. Controlled Use of Administrative Privileges
5. Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations and Servers
6. Maintenance, Monitoring and Analysis of Audit Logs

Foundational

7. Email and Web Browser Protections
8. Malware Defenses
9. Limitation and Control of Network Ports, Protocols, and Services
10. Data Recovery Capabilities
11. Secure Configuration for Network Devices, such as Firewalls, Routers and Switches
12. Boundary Defense
13. Data Protection
14. Controlled Access Based on the Need to Know
15. Wireless Access Control
16. Account Monitoring and Control

Organizational

17. Implement a Security Awareness and Training Program
18. Application Software Security
19. Incident Response and Management
20. Penetration Tests and Red Team Exercises

A complete (but not overwhelming) model

Example:

- CIS Control 16: Account Monitoring and Control
- Includes 13 sub-controls
- Sub-controls related to NIST CSF PR-AC1 include:
  1. Maintain an Inventory of Authentication Systems
  2. Configure Centralized Point of Authentication
  3. Encrypt or Hash All Authentication Credentials
  4. Encrypt Transmittal of Username and Authentication Credentials
  5. Maintain an Inventory of Accounts
  6. Establish Process for Revoking Access
  7. Disable Any Unassociated Accounts
  8. Disable Dormant Accounts
  9. Ensure All Accounts Have An Expiration Date

Summarizing

Comparing NIST CSF to CIS Controls

NIST CSF PR.AC-1

– Identities and credentials are issued, managed, verified, revoked, and audited for authorized devices, users and processes

CIS Control: CIS Control 16, relevant sub-controls

1. Maintain an Inventory of Authentication Systems
2. Configure Centralized Point of Authentication
3. Encrypt or Hash All Authentication Credentials
4. Encrypt Transmittal of Username and Authentication Credentials
5. Maintain an Inventory of Accounts
6. Establish Process for Revoking Access
7. Disable Any Unassociated Accounts
8. Disable Dormant Accounts
9. Ensure All Accounts Have An Expiration Date

In summary

All widely accepted and don't compete with each other

ISO 27000 family
- Best for developing management systems
- Lots of detail on developing policies and procedures

NIST CSF
- Best as an executive diagnostic and communication tool
- Structured for setting organizational targets and objectives

CIS Controls
- Best for bridging the big picture and the details
- Faster rev rate, so better suited for evolving threats

Thank You

Mike Garcia
Senior Advisor for Elections Best Practices
mike.garcia@cisecurity.org