Selecting Your Security Framework

The Differences Between NIST CSF and CIS Critical Controls

filament
INFORMATION SECURITY
filamentsecurity.org

Importance of Frameworks

Public institutions like schools and local governments face increasing cyber threats but often lack the resources of large enterprises. Two widely used security frameworks—NIST Cybersecurity Framework (CSF) and the CIS Critical Security Controls (CIS Controls)—offer different paths to building resilience. This guide explains the basics, differences, and how to choose the right fit for your organization.

Reasons for Standardization

Cybersecurity isn't just about tools—it's about following a structured, recognized standard. While some vendors, regional groups, or consultants create their own "custom" frameworks, these can cause problems:

- **Regulations and Funding:** State and federal laws (such as Ohio HB96) often name specific frameworks like NIST CSF or CIS Controls. Custom frameworks may not meet the bar.
- **Cyber Insurance:** Many insurers now require proof of alignment with recognized standards. Using an "off-brand" approach could leave you uncovered.
- **Interoperability:** Recognized frameworks allow benchmarking, easier audits, and shared language with partners and regulators.
- **Longevity:** Nationally recognized frameworks evolve with the threat landscape. Custom models may be abandoned, leaving your team stuck with outdated practices.

Bottom line: Schools and local governments should avoid reinventing the wheel. Adopt a standard framework like NIST CSF or CIS Controls to ensure your efforts are defensible, fundable, and sustainable.

Understanding Your Options

Schools and local governments are often presented with the option to adopt either NIST CSF or CIS Critical Controls. Both are nationally recognized, both are acceptable to regulators and insurers, and either can serve as a foundation for building a cybersecurity program.

The key difference is that they represent two distinct methodologies: NIST CSF offers a strategic, governance-focused roadmap, while CIS Controls provides a tactical, operations-focused playbook. The following sections of this guide outline each approach in more detail so you can decide which best fits your needs—or how to use both in tandem.

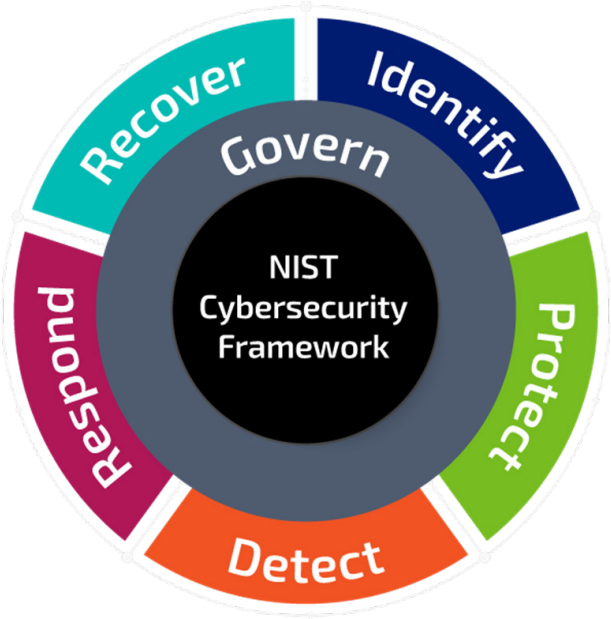
NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) is one of the most widely adopted cybersecurity standards in the United States. It was originally developed by the National Institute of Standards and Technology (NIST) to help organizations of all sizes reduce risk and improve resilience. Unlike many technical checklists, NIST CSF is designed to be flexible, scalable, and risk-based, making it especially valuable for schools and local governments that have to balance security needs with limited staff and budgets.

Structure of the Framework

NIST CSF organizes cybersecurity outcomes into six core functions:

- **Govern** – Establish and monitor your organization's cybersecurity risk management strategy, roles, policies, and oversight (including third-party/supply-chain expectations).
- **Identify** – Understand assets, systems, data, and risk context.
- **Protect** – Implement safeguards to limit impact.
- **Detect** – Develop activities to discover events quickly.
- **Respond** – Contain and mitigate incidents.
- **Recover** – Restore services and improve resilience post-incident.



Why It Matters for Schools & Local Governments

For schools and local governments, the appeal of NIST CSF is its role as a strategic roadmap. Unlike more tactical playbooks such as the CIS Critical Controls, NIST CSF provides a broad structure that connects technology risks to organizational mission, compliance, and funding. It is increasingly referenced in legislation, regulatory guidance, and cyber insurance requirements, making it a defensible choice. Key notes may include:

- **Board-Level Visibility:** Makes cybersecurity understandable for superintendents, councils, and boards.
- **Risk-Driven Prioritization:** Focuses limited resources on the areas of greatest impact.
- **Flexible & Scalable:** Works for both small rural schools and large city governments.
- **Outcome-Oriented:** Defines what to achieve, but leaves the how to prescriptive guides like CIS Controls.
- **Leadership Accountability:** The new Govern function emphasizes that cybersecurity is an organizational responsibility, not just IT's job.

CIS Critical Controls

The CIS Critical Security Controls are a set of 18 prioritized best practices that serve as a practical playbook for defending against the most common attacks. Unlike NIST CSF, which is more strategic and governance-focused, CIS Controls provide step-by-step technical guidance that small IT teams can act on right away. They are organized into three Implementation Groups (IG1–IG3) so schools and local governments can start with the basics and add more advanced protections over time. Below is a graphic outlining all 18 Controls produced by CIS, and how many sub-controls are required per Implementation Group.

For resource-constrained environments, CIS Controls offer a clear to-do list: inventory devices, manage accounts, harden systems, monitor activity, and prepare defenses against ransomware and phishing. They are widely recognized by insurers and regulators as a practical baseline. They strengthen day-to-day defenses if implemented as prescribed by CIS and their recommendations.

Summarizing the Differences

Both NIST CSF and the CIS Critical Controls are accepted standards, but they take different approaches. CSF is about setting direction and managing cybersecurity as an organizational risk, while CIS focuses on specific actions IT staff can take to reduce threats.

NIST CSF	CIS Critical Controls
Focused on risk management and governance	Focused on technical safeguards against common attacks and tactics
Audience is tailored for leadership, boards, and compliance officers	Audience is tailored for IT staff and system administrators
Guidance defines *what* outcomes to achieve	Guidance specifies *what* practices to implement
Approach is descriptive of outcomes	Approach is prescriptive of activities
Broad, long-term, and supports program maturity over time.	Narrow, tactical, and enables quicker implementation in scale

Awareness and Training as an Example

Take user awareness and training as an example. In NIST CSF, the Protect function includes the outcome "personnel are provided cybersecurity awareness education and are trained to perform their information security-related duties and responsibilities." This is descriptive—it tells leadership that staff training is essential, but it doesn't prescribe how to design or deliver that training.

In contrast, the CIS Controls get prescriptive. Control 14 requires organizations to "establish and maintain a security awareness program," and it goes further by specifying elements such as conducting role-based training, simulating phishing attacks, updating training content regularly, and tracking participation. NIST highlights the what (staff need training), while CIS outlines the how (the exact practices that make the program effective).

Nonprofit Security Programs Based in the Midwest

Filament Information Security is a divisional program under the Foundation of Educational Services (FES). This program was founded to help schools and mission-drive organizations build lasting cybersecurity programs sustainably.

Most security vendors are coastal, expensive, and built for large enterprises. Our programs offer affordable, rightsized solutions for Midwest organizations through both contract-based work and mentoring engagements. Our goal is to empower internal teams to confidently manage their own security posture, even without a full-time security department.

Meet the Team

Art Provost, VP of Security Services

Art, with 30 years of experience in Information Security across diverse roles, joined Filament in 2011 and holds multiple certifications, including CISSP, GSEC, GPEN, GWAPT, CISM, and GSTRT.

Tyler Malcom, Security and Compliance Analyst

Tyler, who joined Filament in 2022, has a strong background in cyber defense and offensive operations from his time in the US Navy and holds CISSP and GSEC certifications.

Keri Kunkle, Security and Compliance Analyst

Keri, who joined Filament in 2023, is a seasoned cybersecurity professional with experience in the US Marine Corps and Department of Defense, holding multiple certifications and advanced degrees in cybersecurity.

filament
INFORMATION SECURITY
filamentsecurity.org

Brendan Conway
Solutions Manager
402.479.6991 - Direct
800.850.8397 ext. 6991
BrendanC@filamentservices.org

Schedule a Discovery Call Today!