Building Your Security Foundations

Basics To Getting Started With Your Program

filament
INFORMATION SECURITY
filamentsecurity.org

What are Frameworks?

A cybersecurity framework is a set of structured best practices that help your organization understand your cyber risks, prioritize what to fix, and create a long-term plan to get there,

Think of it like building codes for your digital systems: you don't need to invent your own safety plan; you follow a tested model.

Why Do Schools and Nonprofits Use Frameworks?

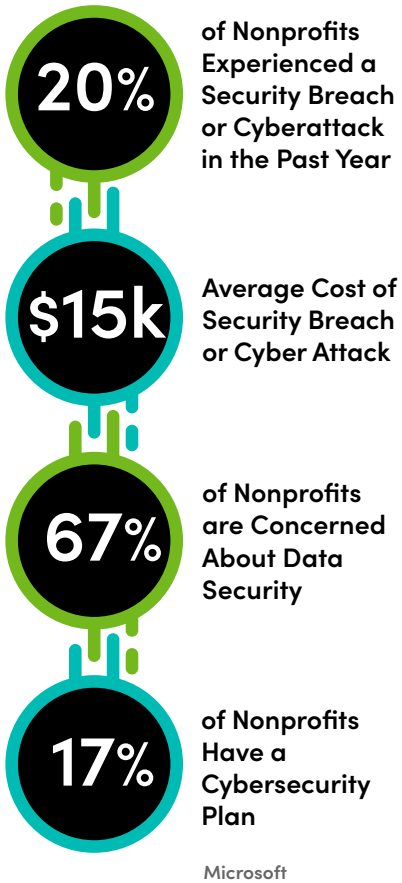
- **To prioritize work with limited resources:** Frameworks help small teams avoid "trying to do everything." They break security into manageable steps.
- **To communicate to funders and boards:** Loss of donations and grants due to decreased donor trust, as well as potential fines and penalties for non-compliance with data protection regulations.
- **To meet compliance and insurance needs:** Cyber insurance providers and grant funders increasingly task: "Which framework do you use?" Choosing one gives you a confident answer.
- **To prepare for incidents:** Frameworks help you document and improve how you prevent and responds to incidents — and prove it when something goes wrong.

I outsource my IT, do I still need a Framework?

Hiring a Managed Service Provider (MSP) or IT vendor can help implement and maintain many security controls. Your organization is still accountable. Whether it's a data breach, ransomware attack, or compliance audit, the organization remains liable for ensuring that proper protections were in place,and documented, regardless of who performed the work.

You can outsource the work, but not the responsibility!

- **You direct the vendor's work:** Ensure that all services provided by your MSP or IT contractor are explicitly mapped to the controls in your chosen frameworks.
- **You maintain the documentation:** Contracts should clearly define security responsibilities, deliverables, timelines, and breach response expectations.
- **You assign internal ownership:** Even if the work is outsourced, someone on your team (leadership, IT, operations) should be assigned to oversee the relationship. They should regularly review reports, ask questions, and ensure services meet the needs of your security program.



NIST CSF vs. CIS Critical Controls

There's no one-size-fits-all framework. But for small and mid-size organizations, two stand out for our sectors like schools and nonprofits.

Comparison Between CSF and CIS

Both NIST CSF and CIS Critical Controls achieve full-fledged security programs, and being compliant with either comes with similar benefits, but they have different strategies behind their controls.

NIST CSF	CIS Critical Controls
A strategic risk management framework built for critical infrastructure that had a more limited budget than federal systems.	A prioritized checklist of technical controls that was built by a nonprofit to make controls into actionable items.
Best for flexible long-term planning and board reporting where the goal being achieved is the primary deliverable.	Best for hands-on remediation and IT work where the implementation work is the primary deliverable.
Structured into 6 primary functions: Identify → Recover.	Structured into 18 controls, each with 3 tiers (low budget to large budget)
More flexible in how you can achieve controls, allowing for customized security programs.	Easier to "check off" and assign as the mechanisms for achieving the controls are defined.

Am I Locked Into My Framework?

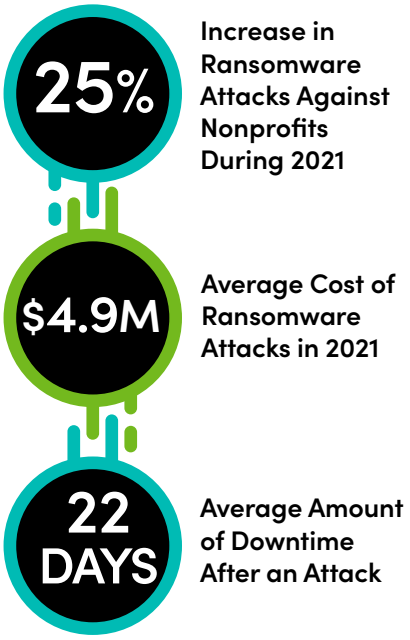
Many of our clients start with a framework that fits their current size and needs — like NIST CSF or CIS Controls — but find they need something different as they grow or face new requirements. That's totally normal. Frameworks aren't locked-in contracts; they're tools to guide your work.

You can map or "crosswalk" your progress from one framework to another. For example, if you start with CIS Controls and later need to adopt NIST 800-53 for federal compliance, you don't have to start over — many of your existing controls and documentation will carry over with just a few adjustments.

Think of it like switching from one curriculum to another: the topics are similar, but the structure changes. The key is tracking your work and being able to show how your security practices align with whichever framework you're using.

Understanding Security Assessments

Before you can improve cybersecurity, you need to understand where you stand. But there are different types of assessments, and they're not all the same. Its important to understand these differences at the start of your program launch and to know what tool is most appropriate for where you are today.



Cybersecurity Tech Accord | Accenture | Statista

Assessment Types

- **Gap Assessment:** A comparison of your current practices to a security framework (like NIST CSF or CIS Controls). Shows what's missing or incomplete.
- **Risk Assessment:** An analysis of which threats are most likely and which weaknesses matter most — often includes impact scoring.
- **Vulnerability Assessment:** A scan of your network or systems to identify known technical flaws (e.g., outdated software, missing patches).
- **Penetration Test:** A simulated cyberattack to see if vulnerabilities can be exploited — shows what an attacker could do in real life.

We Recommend Most Schools and Nonprofits Start with a Gap Assessment

We recommend most entities start with a gap assessment if you are just starting out. This is because it gives you a complete picture up front. You can't fix vulnerabilities or reduce risk if you don't know what controls you should have in place. A gap assessment gives you the big picture.

IBM 2020

Risk Assessments and Vulnerability Assessments are controls within the frameworks, with which you will have policies and routines for, within NIST CSF or CIS. Implementing a framework will achieve those results.

Penetration Testing comes later. If your organization already knows it does not have policies, response plans, or vulnerability patching schedules, a Penetration Test is an expensive way for someone to confirm what you already know about your security posture.

How to Get Started

Starting a cybersecurity program doesn't require a perfect plan — but it does require commitment. Whether you hire a third-party assessor or tackle it in-house, here's how to begin:

Step 1: Establish Your GRC Tracking Process

GRC stands for Governance, Risk, and Compliance. Even before choosing a framework, decide how you'll track and maintain progress.

- **Pick a System:** Use a simple spreadsheet, GRC tool or platform, or project tracker
- **Assign Roles:** Who owns policy? Who updates systems? Designate the duties in your organization.
- **Establish Routines:** Monthly check-ins, board reports, etc. What tasks are annual, quarterly etc.?

This is your operating system for cybersecurity. Without it, no framework or assessment will stick.

Step 2: Choose Your Framework

Choose one framework that fits your size, staffing, and reporting needs. You can always crosswalk your controls later if requirements change over time.

Step 3: Perform a Gap Assessment

Compare what you're currently doing against the framework. This shows you what's in place, what's missing, and what's next.

- **Internal Assessment:** Assign someone to run the assessment on your staff, if you have capacity and training to do so.
- **Hire Third-Party Assessors:** Bring in a trusted third party if you want support. Often times, an analyst can guide you through all the questions and requirements faster than doing it alone.

Start Simple. Stay Consistent.

You don't need a full-time security team or expensive software to build a strong cybersecurity foundation. You just need structure, a framework, and the commitment to keep going.

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!