Security Assessments Aren't Accusations

Why Strong Tech Teams Still Benefit From External Help

filament
INFORMATION SECURITY
filamentsecurity.org

Assessments are not Audits

Security assessments often raise anxiety, not because they're risky, but because they're misunderstood. The idea of 'assessing' an internal team can feel like a vote of no confidence, especially when leadership has deep trust in their IT or Tech Director.

But here's the truth: a good assessment isn't about catching someone doing something wrong. It's about catching something **before** it causes harm. It's about validating the systems already in place, and identifying where gaps exist, not who's to blame for them. Most of our assessments confirm that 80–90% of your practices are sound. That's a good thing.

Cybersecurity is Not the Same as IT

Your IT Director is probably outstanding. But cybersecurity isn't just an extension of tech support — it's its own discipline. IT focuses on uptime, connectivity, infrastructure, and keeping operations running. Security focuses on risk, threats, controls, and governance. They overlap, but they're not the same.

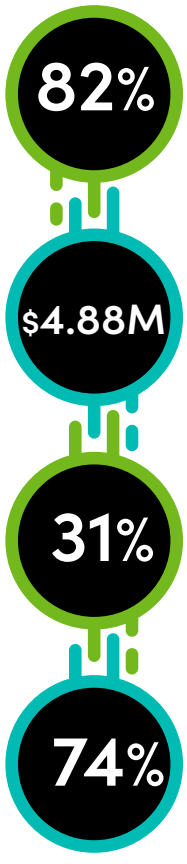
Think of HR vs. finance. They both report to the same leadership, but no one expects your payroll manager to run performance evaluations. The same applies here: expecting an IT leader to manage policy enforcement, risk acceptance, and governance documentation can be unrealistic — especially when those expectations grow year after year.

Threats Change Quickly

Cybersecurity is a rapidly evolving domain. New vulnerabilities come out daily. Threat actors shift tactics constantly. Regulations and frameworks change year over year.

Even the best IT professionals, the ones keeping your systems humming, aren't wired to spend hours a week reading threat reports, parsing federal guidelines, or mapping controls to audit checklists. That's a full-time discipline in itself.

Security professionals follow threat feeds, vendor disclosures, and CIS/NIST updates because that is their job. And it's exactly why external security assessments, framework alignment, and vCISO partnerships exist. To give your team the intel efficiently.



of 2023 breaches involved cloud misconfiguration according to the Wall Street Journal

is the average cost of a 2024 data breach according to Varonis

of nation-state attacks target nonprofits according to Microsoft

of breaches involve human error according to Varonis

How a Gap Assessment Supports Your IT Staff Member

When organizations hear "assessment," they often imagine an audit — a checklist, a rating, or worse: a finger-pointing report. That's not what one provides.

A gap assessment against a recognized cybersecurity framework (like NIST CSF or CIS Controls) is a collaborative process designed to support your internal team — especially your Tech Director — by putting structure around the things they already know, do, or worry about.

Here's what you'll actually walk away with:

Deliverable	Explanation
A clear, prioritized gap report mapped to a recognized framework (CSF, CIS)	A report that is translated into plain English for leadership. Includes what's working, what's missing, and what should be priority.
A Plan of Action & Milestones (POAM) that acts as a roadmap for next steps	A sequenced list of improvement actions, tailored to your size and capacity. Helps the Tech Director focus efforts and ask for resources with data.
Templates, Policies, and Tools	Sample policies and forms your team can adapt instead of writing from scratch.
Leadership-Facing Summaries	Executive summaries for boards or leadership. Clarifies responsibilities between IT and admin.
Knowledge Provided, not Tested	As assessment is not a test. You are not being audited. You can clarify the requirements of controls throughout without worrying you will fail.

An Assessment is Just Another Tool in Your IT Team's Pocket

A gap assessment is one of the most practical, respectful ways to support your IT Director while strengthening your organization's security posture. It translates security into language that leadership can act on, it helps your tech staff work smarter—not harder—and it ensures you're not waiting for a breach or compliance failure to start planning. You wouldn't skip an annual financial review—don't skip this one either. You'll come away with clarity, confidence, and a roadmap built to fit you.

The Gap Assessment Process

A gap assessments shouldn't be a surprise test. Analysts will bring your IT Director into the conversation from day one, ensuring they understand each control, its importance, and how to improve upon it. The best part is that the meeting cadences can be flexible, often only 2-4 hours a month, to avoid any disruptions to operations.

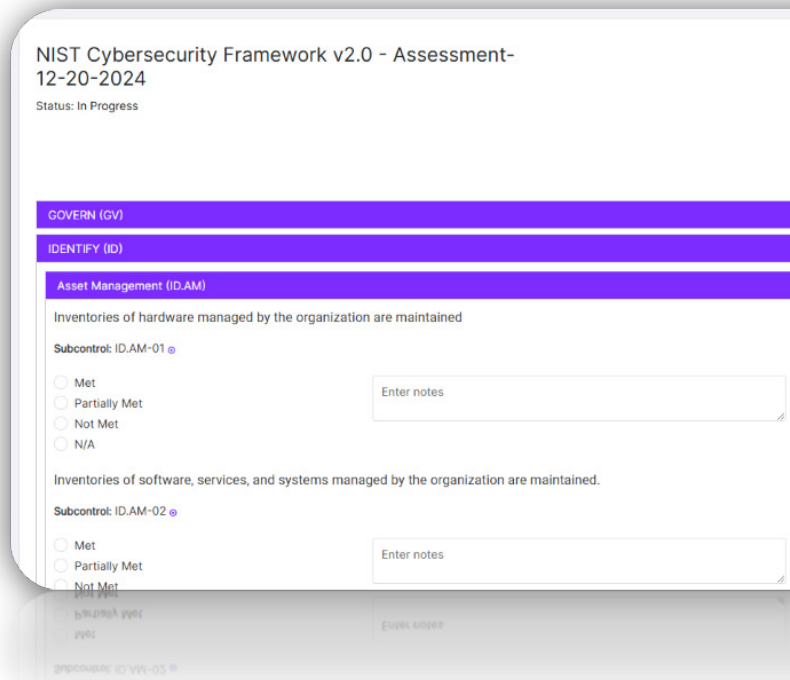
Step 1: Kickoff & Scoping

Assessments start with a short meeting to define your priorities, compliance concerns, and which frameworks matter to your organization (e.g., NIST CSF, CIS Controls).

Step 2: Interviews & Evidence

Analysts ask your IT Staff key questions, reviewing existing policies and procedures. This is a lightweight engagement but focused on facts, not opinions.

To the right, you will see a preview of the screen an assessor might share as they conduct the interview process.



Step 3: Findings & Roadmap

An analyst provides their findings at the end of the assessment with the gaps and risks discovered.

- **Findings Report:** A summary of strengths, gaps, and risks based on your current security posture, mapped to an industry framework and written in plain language for leadership.
- **POAM (Plan of Action & Milestones):** An optional follow-up document that outlines prioritized next steps, responsible parties, and realistic timelines to address each identified gap. Some organizations will want to take their Findings Report and do this themselves post assessment with their organization.

Step 4: Wrap-Up Presentation

Expect the delivery an executive summary of your findings and roadmap, tailored for leadership. This briefing focuses on key risks, priorities, and funding implications—giving decision-makers clarity without overwhelming them with technical detail.

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!