# Managing Security With Outsourced IT

## Your Third-Party Providers Are Not Your Security Program

filament
INFORMATION SECURITY
filamentsecurity.org

# The Appeal (and Limits) of Outsourced IT

Outsourcing IT through Managed Service Providers (MSPs) and relying on cloud platforms has become the norm for cost-conscious and capacity-limited organizations. These solutions promise efficient help desk support, system uptime, and basic cybersecurity hygiene.

But there's a catch. Many organizations mistakenly assume these vendors take full responsibility for their cybersecurity and compliance obligations. In reality, your MSP supports your infrastructure but **you** still own the risk.

Think of it this way: your contractor builds what's on the blueprint, but they don't design the building, approve the zoning, or decide how it fits into the neighborhood. Likewise, your IT vendor executes on systems, but the security program still needs to be designed, governed, and maintained by you.

## The Scope of Work for Your MSP

MSPs are essential, but they are not compliance consultants or governance experts. Here's what they typically do not handle:

- Writing, maintaining, or enforcing your internal cybersecurity policies
- Conducting risk assessments aligned to NIST, CIS, or state mandates
- Creating or maintaining a formal incident response plan
- Monitoring the configuration of third-party tools outside their control

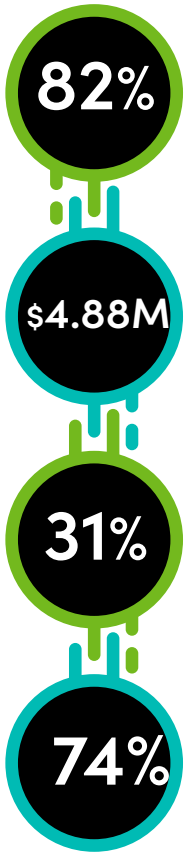
An MSP ensures functionality. But cybersecurity requires intentional governance, frameworks, policy, ownership, and strategy. Only your organization can establish those.

## Cloud Does Not Mean Compliance

Cloud platforms like Microsoft 365, Google Workspace, or your Student Information System (SIS) offer excellent security capabilities, but they don't configure themselves. If you haven't

- Enabled and enforced MFA for all users
- Defined data sensitivity levels and access rights
- Reviewed what third-party apps are connected to your accounts
- Logged and reviewed administrator actions regularly

Then you're not compliant, even if your vendor is SOC2 certified. Compliance is about **your implementation**, not just your vendor's.



# Auditors and Insurance Requirements

A common mistake among mission-driven organizations is assuming that vendor dashboards, licensing agreements, or "we've never had a breach" claims will satisfy external reviewers. They won't.

Auditors, grantors, and cyber insurance underwriters aren't looking for tools — they're looking for governance. Specifically, they want evidence that your organization has a formalized, intentional cybersecurity program that is owned internally — even if much of the technical execution is handled by outside partners.

These questions can include the following to discover if your organization is managing their own program.

| Question | Explanation |
|---|---|
| Do you have a formal cybersecurity policy that's been approved by leadership? | Not just a list of rules from your IT provider — but a written policy that reflects your own data priorities, signed off at the board or executive level. |
| Have you conducted a gap assessment against a recognized framework? | Frameworks like NIST CSF or CIS Controls are the common language of auditors. Even if your MSP is compliant, it does not mean you are. |
| Who is formally accountable for cybersecurity decisions? | Insurance carriers in particular want to know who's responsible for risk acceptance. |
| Do you maintain basic artifacts of a mature security program? | A list of vendors and what data they access, change logs, past incident reports, tabletop results |

## So What Does This Mean?

Having security tools in place is expected — but it's not enough. Even if your MSP is technically competent, highly responsive, and installing every recommended product, your organization can still fail an audit if you haven't fulfilled your governance responsibilities.

Auditors look beyond execution — they're looking for ownership. They want to see that you, the organization, have formally adopted policies, identified who is accountable for risk, performed internal assessments, and documented decisions around security posture. If those elements are missing, no amount of patching or ticketing from your vendor will satisfy compliance requirements.

Cyber insurance carriers are no different. They don't just underwrite based on your toolset — they evaluate whether your organization is proactively managing risk. If governance is outsourced in name only, you may appear high-risk and ineligible for preferred coverage, even with an excellent MSP.

# How a vCISO and Assessment Improves Your MSP

Bringing in a virtual Chief Information Security Officer (vCISO) or conducting a framework-based assessment isn't about replacing your IT provider — it's about strengthening your program, formalizing your governance, and making your MSP even more effective.

While your MSP handles the day-to-day technical operations, a vCISO or independent security consultant helps guide the why behind the what. That includes aligning your security efforts to business goals, identifying long-term risks, and ensuring your investments actually reduce exposure.

## What Does This Look Like In Practice?

- **Define priorities, timelines, and acceptable risk:** Not every risk is urgent, but you do need to triage. A vCISO or assessment helps you rank vulnerabilities, align them with funding cycles, and create a roadmap that your MSP can help implement without chaos.
- **Establish governance your vendors can follow:** MSPs thrive when expectations are clear. With a framework-based approach (like NIST CSF or CIS Controls), your organization defines what "secure" looks like, not just what's running. This helps vendors focus on execution instead of guessing.
- **Give your internal IT team context and backup:** Many IT directors wear multiple hats: help desk, systems admin, tech trainer, and now they're also expected to be the security expert. A vCISO gives them strategic air cover: policies, documentation, leadership engagement, and a neutral voice that can say, "We need to slow down and fix this."
- **Support executive leadership in policy, investment, and oversight:** Board members and executive directors are often uncomfortable making decisions about cybersecurity, and rightly so. An outside advisor translates tech into plain language, helping them fund wisely and govern responsibly.

At the end of the day, cybersecurity isn't a tool or a technician — it's a program. That program lives in the space between what's working and what's at risk. We help you bridge that gap, with your MSP at the table, not in the hot seat.

# 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!