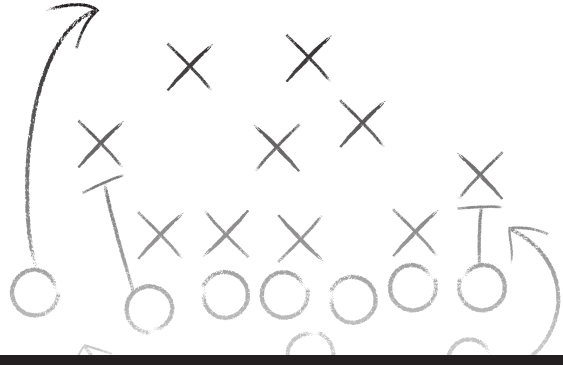
THE CYBER PLAYBOOK

A No-Nonsense Guide To Cybersecurity And Compliance For Business Owners

DAN STEWART

Featuring Cybersecurity Experts From Around The World

THE CYBER PLAYBOOK



A No-Nonsense Guide To Cybersecurity And Compliance For Business Owners

Featuring Cybersecurity Experts From Around The World

BigRedMedia
a TMT company

Nashville, Tennessee

Chapter 12:
The Risks Of Overloading Your Internal IT Department With Compliance

Dan Stewart
CEO & Founder, Stewart Technology Group, LLC

If you are running a business today that isn't subject to regulations, you're lucky – and in the minority. The majority of companies in the U.S., regardless of size or industry, are subject to some form of compliance requirements from the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) that protects sensitive unclassified information, to consumer data protection regulations like the Payment Card Industry Data Security Standard (PCI DSS), to industry-specific standards like the Health Insurance Portability and Accountability Act (HIPAA). And it's typically not just one layer of regulations but several.

For example, if you are a health care provider, you have to be HIPAA compliant but also PCI compliant if you are processing credit cards (and what business isn't?). But wait, there's more. There are different levels of PCI compliance, depending on the volume of card transactions, and each card brand has its own compliance levels. Not only that but there are also individual state guidelines for protecting consumer data. To date, 12 states have passed their own data privacy laws.[xxxiii] With all

these compliance nuances, how can your internal IT department keep up with them all? The startling answer is they can't.

No man or woman is an island. You can't expect your internal IT team to be an expert at managing your technology and operations and the ever-changing world of regulatory compliance. They're already neck-deep in network maintenance, software updates, troubleshooting user issues, and implementing new technologies to support your business's operations and keeping people productive. Adding the complexities of compliance management to these existing duties is —well—not sustainable for you or your team.

Here's the reality: Compliance is an encyclopedia – not a short story. It's too much for one person to handle on their own. And it's too important to not make sure it is done right. So, what are the risks of overloading your internal IT department with compliance, and what can you do to avoid it? I have a few things to say about that. First, let's talk about what compliance is and is *not*.

Compliance Is An Unavoidable Rabbit Hole

At its essence, compliance means just abiding by sets of rules for your business. What's so hard about that? Well, these rules are fluid from year to year, and they become more complex. The harder it gets, the harder it is to remain compliant. Can you really afford to take an ad hoc approach to compliance?

I spent years working in corporate IT. The attitude from the stakeholders toward compliance back then hasn't changed much from today: *"It's easy, just fill out the form."* Business owners, CEOs, CFOs, and even CIOs don't really realize that a) compliance is ongoing annually,

b) it is always subject to change, and c) just because you fill out the form doesn't make you compliant – and d) on some compliances an external audit is necessary.

I get it! It's been my experience that clients dislike dealing with compliance requirements. They think it adds unnecessary costs and burdens their staff, who spend time chasing rabbits down holes rather than working on productive, revenue-generating tasks. But Check-the-Box compliance no longer cuts it. Managing compliance requires a focus on the key risks. And that's not a job for your internal IT person because they will do *"just enough to get by."* After all, they don't have the time or the expertise, and their plate is full!

Now that you know the pathway to compliance isn't easy, let's talk about the six critical risks of overloading your internal IT department with the task.

#1. It Can Profoundly Impact Your Business

Compliance should not be a burden to your internal IT department but a positive opportunity that can enable your business's growth and performance. However, staying on top of compliance can be a full-time job. If your IT team has to research and understand the regulations, develop and implement compliance measures, document their processes, and respond to audits and inquiries – on top of everything else they do – I can assure you that something will fall through the cracks. And that could be a devastating hit to not just your bottom line but your entire business. For instance, if one of your IT employees makes a compliance misstep with PCI, you won't be able to conduct business as usual. If your credit card processor drops you because you checked the Yes box and got compromised, and it turns out you should

have checked the *No* box, your chance of getting denied by another processor is highly likely. Can you afford to go "cash only" in today's business environment?

#2. It Can Cost You Money!

The consequences of noncompliance can be harsh, including penalties, legal liabilities, and damage to your company's reputation.

Believe it or not, I've had clients who are supposed to be compliant but can't be bothered. They would matter-of-factly check No on the form that they weren't in compliance, pay the $40 or $50 a month penalty, and carry on. To them, it's like getting a $20 speeding ticket. If every time you get pulled over, the ticket is only $20, will that stop you from speeding? Some businesses, usually those with multiple locations, can get hit with thousands of dollars in monthly fees if they remain noncompliant.

Here's my tip. Sooner or later, that $20 ticket will go up, and then they'll take your car.

#3. It Can Lose You Contracts

If you do business with the DoD, you are already familiar with CMMC 2.0 compliance. This isn't for beginners. CMMC requires special skills to navigate channels and prepare clients for the audit and action plans necessary to complete the compliance process. Missing it, ignoring it, or simply faking it can cost you government contracts, both current and future. That means your competitor, who takes the CMMC process seriously, is cashing in while you are sitting on the sidelines.

CMMC is a deep, dark well, and it *goes way, way* down. Don't leave it to your internal IT team to find the bottom.

#4. It Can Cost You Customers

Consumers expect a company to protect their sensitive information. If your business is not on top of your compliance obligations and you experience a data breach, you can irrevocably damage that trust. In a recent McKinsey survey, 40% of all consumer respondents said they would no longer do business with a company after a data breach.[xxxiv]

#5. It Can Squash Innovation

If your internal IT team has to focus on compliance tasks, they aren't prioritizing work that supports your business's growth – or their passion for tech. A distracted focus means your company is late to the game when adapting to market changes. And it also leads to #6.

#6. It Can Cost You Employees

Here are some worrisome but important employee stats that should be top of mind for every technology-driven business leader:

- 13% is the job turnover rate in the IT industry – the highest rate of all sectors.[xxxv]
- 73% of tech employees leave due to burnout.[xxxvi]
- 57% of IT workers are burned out because of their heavy workloads.[xxxvii]

Here's a fact. Employee burnout can lead to horrible decision-making, which can undercut every aspect of your compliance program. IT professionals already feel pressure in an industry known for its competitiveness and changing skill demands. That is just one more reason not to put compliance management on their plates.

If Not Your Internal Team, Then Who?

So, now that you know why your internal IT team should *not* be burdened with compliance, who should be responsible?

The answer is a tricky question because, ultimately, *you* (the business) are still responsible. However, leaning on an outside managed services provider firm to help with some of the heavy lifting could mean the difference between staying compliant and impacting your company's competitiveness – even your livelihood.

I often hear something like this when I ask potential clients who manage their IT: "My cousin's neighbor over the fence." I'm exaggerating, of course (not by much), but you get the point. Anything dealing with compliance requires expertise.

An outside, experienced provider can help you navigate the wide-open field of compliance requirements by keeping the business up to date with changes in rules and standards, conducting internal audits to make sure there are no compliance gaps, implementing and managing tools that can help automate compliance processes, and offering training sessions to help educate your team on compliance requirements and best practices.

One of the most essential compliance tasks an outside provider can help you with is creating and implementing a POA&M, or a Plan of Action and Milestones. This is a checklist to help fix weaknesses identified during a compliance audit. While it's not bulletproof, think of it as a shield. If you get dinged for noncompliance, regulators often see it as a sign of progress. Here's a look at an 11-point sample POA&M:

1. **Introduction:** Provide an overview of the compliance audit findings.
2. **Deficiency Identification:** List each deficiency or noncompliance issue identified during the audit, including its severity level and associated risks.
3. **Action Items:** Outline specific measurable and achievable action items for each deficiency that needs to be addressed and provide a timeline to achieve compliance.
4. **Responsible Parties:** Assign responsibility for each action item to individuals or teams within the organization. Clearly define who is accountable for implementing each task.
5. **Resources Required:** Identify the resources – people, technology, and budget – needed to complete each action item successfully.
6. **Dependencies:** Identify and address any dependencies between action items or external factors that may impact the remediation process.
7. **Monitoring and Reporting:** Define the process for monitoring progress, documenting the completion of action items, and reporting status updates to stakeholders.
8. **Risk Management:** Assess and document any residual risks associated with the deficiencies and remediation efforts and develop strategies to mitigate these risks to ensure ongoing compliance.
9. **Completion Criteria:** Define criteria for determining when each deficiency has been fully remediated and achieved compliance.
10. **Approval and Sign-Off:** Obtain approval from relevant stakeholders, such as management or regulatory authorities, for the POA&M. Ensure that all parties involved agree to the proposed remediation plan and associated timelines.

11. **Revision and Review:** Establish a process for reviewing and updating the POA&M as needed, particularly if new deficiencies are identified, or changes occur in regulatory requirements.

We've talked about what a provider can do to help you keep from overloading your internal IT department; now, I want you to know one of the things they can't do.

The first thing I always tell my clients is this: ***"I cannot touch the compliance form."*** You can rely on me as an outside consultant to help you keep up with compliance, but the responsibility doesn't shift. Period

Conclusion

Long and short, your IT department should not be "doing" compliance. As requirements increase, so does a company's obligation to focus on data privacy. Your business depends on compliance being done right. As I stated earlier in the chapter, managing compliance can be a complex catacomb of rabbit holes that is repetitive, never-ending, and only expanding. What was last year's process is now last year, plus three more rules. And next year, there will be three new rules, if not more. Now is not the time to hand over the keys to your internal team, which does not have the skills, training, or bandwidth.

A strong leader can recognize a team's limitations and know when to call in external experts. Outsourcing your compliance to a managed services provider with the right capabilities can help identify gaps, streamline your audit efforts, and lighten the load on your internal IT team so they can focus on more strategic projects.

About Dan Stewart

Dan Stewart is CEO and founder of Stewart Technology Group (STG), a highly successful technology solutions firm headquartered in Columbia, Missouri, that serves clients across the Midwest. He has more than 30 years of experience in the IT industry as an expert in outsourced computer services, specializing in engineering, manufacturing, retail, and business services sectors. Dan and his team at STG have always been guided by the pivotal role that managed IT services play in navigating the complex landscape of compliance. Dan spent a large part of his career as an IT manager for WSP USA, formerly Parsons Brinckerhoff, one of the world's leading engineering firms, responsible for the data protection and regulation adherence of multimillion-dollar rail and transit projects.

With more than three decades of hands-on compliance expertise, Dan knows that IT providers must excel in personalizing technological solutions that align with a business's specific compliance requirements, with the understanding that there may be more than one set of regulations. That's what sets Stewart Technology Group apart from other MSPs. Dan's team is adept at staying on top of changes in regulatory requirements so they can help their clients adjust their IT infrastructure to meet the changing and sometimes challenging compliance requirements without compromising efficiency. Dan's success in IT comes from safeguarding his clients' long-term success.

Dan enjoys sharing his knowledge and expertise with the next generation of IT professionals. He taught server OS, workstation OS, and networking courses as an adjunct professor for 13 years at East Central College in Union, Missouri.

For more information, contact Dan Stewart at
Stewart Technology Group, LLC:
Phone: 573-673-6005
LinkedIn: linkedin.com/in/danstewart247
Email: dan@stewarttechgroup.com
Web: stewarttechgroup.com

THE CYBER PLAYBOOK

ABOUT DAN STEWART

Dan Stewart is CEO and founder of Stewart Technology Group (STG), a highly successful technology solutions firm headquartered in Columbia, Missouri, that serves clients across the Midwest. He has more than 30 years of experience in the IT industry as an expert in outsourced computer services, specializing in engineering, manufacturing, retail, and business services sectors. Dan and his team at STG have always been guided by the pivotal role that managed IT services play in navigating the complex landscape of compliance. Dan spent a large part of his career as an IT manager for WSP USA, formerly Parsons Brinckerhoff, one of the world's leading engineering firms, responsible for the data protection and regulation adherence of multimillion-dollar rail and transit projects.

With more than three decades of hands-on compliance expertise, Dan knows that IT providers must excel in personalizing technological solutions that align with a business's specific compliance requirements, with the understanding that there may be more than one set of regulations. That's what sets Stewart Technology Group apart from other MSPs. Dan's team is adept at staying on top of changes in regulatory requirements so they can help their clients adjust their IT infrastructure to meet the changing and sometimes challenging compliance requirements without compromising efficiency. Dan's success in IT comes from safeguarding his clients' long-term success.

Dan enjoys sharing his knowledge and expertise with the next generation of IT professionals. He taught server OS, workstation OS, and networking courses as an adjunct professor for 13 years at East Central College in Union, Missouri.

Designed and Produced by Big Red Media
Printed in the USA

BigRedMedia
a TMT company