Managed Services

Compliance Guide

ENGLER IT

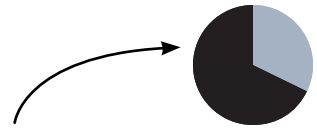
englerit.com

Rethinking Regulation.

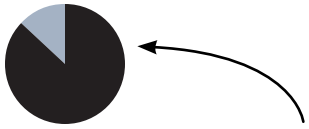
A closer look at the importance of **compliance** to growing your business.

▶▶▶ **Compliance can be a major headache for small and medium-sized business (SMB) owners.** Simply keeping track of — let alone complying with — the various rules and regulations that apply to your organization is a huge undertaking.

Without the same resources that larger firms can devote to compliance, your SMB can easily find itself getting crushed beneath the pressure of regulatory demands.



***68%** of small business owners feel that regulatory compliance puts a financial burden on their business*[1]



***87%** of compliance professionals report that their organizations have no additional capacity for compliance functions*[2]

The True Cost of Non-Compliance

When it comes to compliance, it can be tempting to cut corners to save your SMB time and resources — but it's never a good idea.

Ignorance does not exempt you from the harsh penalties and fines your business will face if it's found to be non-compliant.

The Cost of a Single Violation	
HIPAA	**$100–$50,000**
CCPA	**$7,500** per intentional violation; **$2,500** per unintentional violation
SOX	Up to **$5 million** and **20 years** in prison
PCI DSS	**$5,000–$100,000** per month

Compliance matters.

A Matter of Survival

Avoiding hefty fines is a good reason to stay on top of compliance, but preventing a cyberattack is an even better one. Cybercrime is at an all-time high, and a data breach can be devastating to your growing business.

Remaining in compliance with data privacy and protection regulations such as **HIPAA, NIST, SOC 2** and **PCI DSS** can go a long way toward keeping your digital kingdom safe.

Help is here.

Faced with a complex and ever-changing regulatory landscape, rampant cybercrime, and hybrid work environments, more and more companies are turning to third parties for help with compliance.

Partnering with a trusted managed service provider (MSP) can be a particularly effective way of dealing with compliance at your growing organization. The benefits of working with the right MSP are numerous:

Documentation & Automation
Compliance isn't just following the rules; it's being able to prove that you are. MSPs use documentation software and automation solutions to capture evidence of your organization's compliance, saving you time and money while setting you up for successful audits and the like.

Efficiency & Productivity
An MSP oversees your entire IT infrastructure and has detailed knowledge of how your business operates; the right MSP can make sure your compliance efforts work with — not against — core business functions.

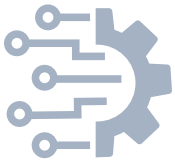
Security
Compliance is an important part of your security posture, but meeting regulatory requirements isn't always enough to keep your business safe from cyberattacks. An experienced MSP has cybersecurity pros who can make sure your compliance efforts are embedded in a broader security strategy that minimizes risk.

Proactive Support
The regulatory industry is evolving at breakneck speed. An MSP can look ahead and anticipate new regulations, allowing you to make timely adjustments and stay ahead of the compliance curve.

The number of ***"mature and advanced"*** compliance programs grew by ▲ **29%** in 2021, while ***"reactive and basic"*** ones declined by ▼ **35%.**[3]

Comprehensive Compliance Guidance

We have decades of experience in compliance, and can assist your organization with building out compliant systems and processes, whichever standard or regulatory framework you're facing.



NIST

Comprehensive cybersecurity framework to protect critical infrastructure

CMMC 2.0

Cybersecurity standards aimed at protecting the Defense Industrial Base

DFARS

The DoD's regulatory requirements for protecting Controlled Unclassified Information

PCI DSS

A set of requirements created to fight credit card fraud

HIPAA

Federal law governing the use and disclosure of individually identifiable health information

SOX

Federal law regulating financial record keeping and reporting

State-Specific Laws

Each state in the U.S. has its own regulatory landscape

SOC 2

Information security standards for US-based service organizations

Compliance is far too important — and noncompliance far too costly — for businesses to ignore.

How much does noncompliance actually cost your business?

The average revenue losses organizations experience on account of just one noncompliance event recently reached a staggering **$4 million**, up **45%** since 2011.[4] Following the rules isn't just good behavior; it's good business.

Noncompliance costs are ▲ 2.71x higher than the costs associated with maintaining compliance.[5]

But reaping the benefits of compliance takes a sophisticated strategy, and many SMBs simply lack the bandwidth to implement a mature and robust compliance management program on their own.

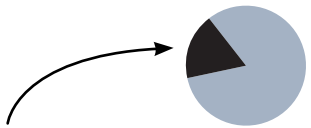
Does your company...

- Hold regular internal compliance audits?
- Monitor the regulatory landscape to keep up with changes?
- Thoroughly vet your vendors' data security and privacy practices?

If you answered "no" to any of these questions, you're likely undercutting your own compliance efforts. After all, an inadequate compliance strategy is almost as bad as a non-existent one, as it can drain your budget without securing the savings of a more mature compliance program.

Businesses are waking up to this fact, with many starting to invest in more proactive, modernized compliance solutions.

▶ **The trend is clear:** technology is quickly becoming an integral and indispensable part of compliance management. Many SMBs, however, continue to operate with obsolete methods and inefficient strategies.



*Despite its proven effectiveness, only **18%** of organizations enlist automation to help with IT risk data collection and reporting.*[6]

The right MSP can give your company IT tools and processes that streamline and automate compliance management, transforming it from a burden and a cost into a well-oiled machine that drives business forward.

We help build out compliant systems and processes...

The **NIST Cybersecurity Framework (NIST CSF)** was created by the National Institute of Standards and Technology for the purpose of helping organizations in the private sector minimize cyber risks and protect critical infrastructure.

NIST originated from an executive order made by President Obama in 2013, and remains a prominent part of the international security landscape.

▶ **Although NIST compliance is voluntary, many companies around the world adhere to NIST standards**, as they provide organizations with a flexible, performance-based framework for assessing current risk levels, and creating appropriate next steps to follow to achieve a more robust security posture.

Released by the Department of Defense (DoD) in 2021, the **Cybersecurity Maturity Model Certification (CMMC) 2.0** is an enhancement and refinement of its predecessor, CMMC 1.0. The program's requirements seek to protect the Defense Industrial Base (DIB) — and the sensitive national security information it handles — from increasingly complex and sophisticated cyberattacks.

A collaborative effort between the DoD and its contractors and subcontractors, CMMC 2.0 streamlines many of the requirements put in place by CMMC 1.0, thereby simplifying CMMC compliance for small and medium-sized businesses.

▶ **CMMC standards are tiered, requiring higher levels of compliance for more sensitive information.**

...whatever regulatory frameworks you're facing.

Published by the DoD in 2015, the **Defense Federal Acquisition Regulation Supplement (DFARS)** aims at safeguarding the confidentiality of Controlled Unclassified Information (CUI) for the sake of national security. DFARS compliance is achieved via self-certification (in contrast to the third-party assessments required for CMMC compliance), and must be met by all DoD contractors.

▶ **DFARS and CMMC largely overlap and share a common goal of protecting American interests through data security.** And, while the regulatory industry is shifting emphasis toward the CMMC and away from DFARS, CMMC isn't replacing DFARS, so DoD contractors need to maintain compliance with both sets of standards.

The **Payment Card Industry Data Security Standard (PCI DSS)** is a set of requirements that apply to any entity that handles credit card information.

The goal of PCI DSS is to fight credit card fraud and secure the entire payment card ecosystem. PCI DSS isn't a law, but a contractual obligation overseen by the PCI Security Standards Council (PCI SSC), an independent body formed by Visa, Mastercard, American Express, Discover, and JCB. That said, non-compliance with PCI DSS can result in harsh fines and severe reputational damage.

▶ **For this reason, many organizations work with a third party to manage the complex tasks associated with maintaining PCI DSS compliance.**

We help build out compliant systems and processes...

When people talk about "HIPAA compliance," they're usually referring to a specific aspect of the **Healthcare Insurance Portability and Accountability Act (HIPAA**), namely, Title II, which includes the HIPAA Privacy Rule and the HIPAA Security Rule. These rules set forth standards for the use and disclosure of individually identifiable health information by "covered entities" (healthcare providers and clearinghouses, health plans, and business associates).

▶ **Needless to say, HIPAA compliance can be complicated and time-consuming, which is why more and more covered entities are choosing to outsource their HIPAA compliance needs to a trusted third party such as an MSP.**

Passed by the U.S Congress in 2002 to combat corporate mismanagement and corruption, the **Sarbanes-Oxley Act (SOX)** lays out guidelines and regulations for accurate and secure financial record keeping and reporting. SOX only applies to publicly traded companies in the U.S., wholly-owned subsidiaries, and publicly traded foreign companies that do business with the U.S. However, other companies such as non-profits often choose to comply with SOX to get insurance, attract investors, and avoid lawsuits.

▶ **Working with an IT-savvy third party such as an MSP can help organizations of all sizes leverage tools such as documentation software and advanced security controls to streamline SOX compliance efforts.**

...whatever regulatory frameworks you're facing.

In the coming years, new state laws are expected to emerge around data privacy and protection. California, Virginia, and Colorado already have such laws in place, and the California Consumer Privacy Act (CCPA), in effect since 2020, is one of the most demanding and comprehensive privacy laws in the United States. Utah will soon join that list when the Utah Consumer Privacy Act takes effect at the end of 2023, and New York has a data privacy law under consideration, the New York Privacy Act.

▶ **Keeping up with state-specific compliance requirements can take a lot of work, and a large portion of that work is technical in nature.** Offloading these obligations onto an experienced MSP can save you considerable time and money.

Put forth by the AICPA, **System and Organization Controls (SOC) 2** is a voluntary information security framework that gives U.S.-based service organizations a way to demonstrate the effectiveness of their information security controls to stakeholders and clients. To achieve SOC 2 compliance, companies need to undergo an on-site audit performed by a CPA firm. A SOC 2 report evaluates how well your organization meets "Trust Services Criteria" (TSC) relevant to the services you provide.

▶ **Figuring out which TSC apply to your business, and how to best meet those criteria, can be confusing, which is why it's a great idea, when pursuing SOC 2 compliance, to seek guidance from a third party with SOC 2 expertise.**

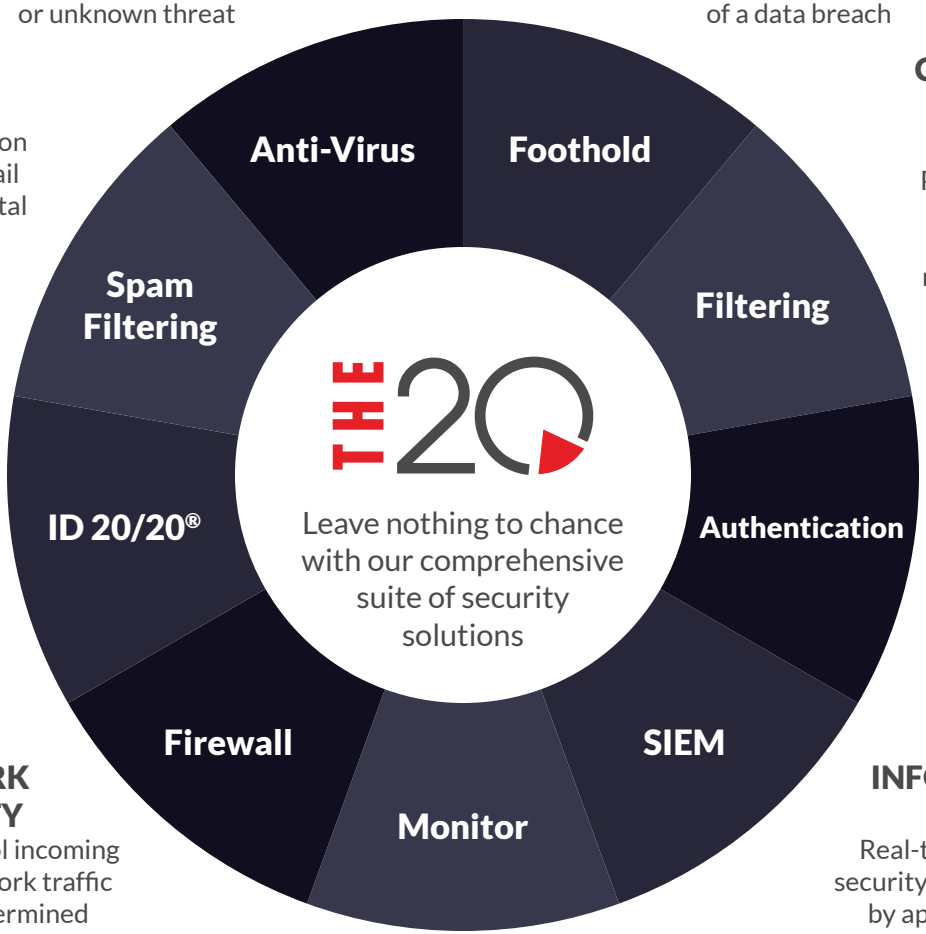
Multi-layer Cybersecurity is Key for Compliance

ZERO-TIME THREAT PREVENTION
Predictive threat prevention platform with multi-layer protection against any known or unknown threat

ADVANCED THREAT DETECTION
Threat detection and swift remediation techniques in the case of a data breach

EMAIL SECURITY
Unparalled protection from advanced email threats and accidental or malicious data leakage

CLOUD-BASED SECURITY PLATFORM
Protection against threats on the internet, such as malware, phishing and ransomware



USER VERIFICATION
Secure your clients from social engineering attacks

POWERFUL PASSWORD MGMT
Protecting passwords and personal data with multiple layers of security

NETWORK SECURITY
Monitor and control incoming and outgoing network traffic based on predetermined security rules

INFO & EVENT MGMT
Real-time analysis of security alerts generated by applications and network hardware

SECURITY MONITORING
The process of detecting cyberthreats and data breaches

Compliance Management for Every Industry

3 Compliance Success Stories

Crisis Averted

Miguel is the managing partner at an up-and-coming law firm.

Miguel and his team are in the thick of preparing for the biggest trial of their professional lives, when, over the weekend … the firm gets hacked!

Luckily, Miguel recently partnered with an MSP. The MSP's Security Operations Center quickly spots and contains the breach before it can do serious harm.

What could have been a catastrophe barely causes a ripple, and a week later, the firm celebrates a huge win in court.

A Healthy Recovery

Sydney runs a small community hospital.

It's been a tough year: declining revenue, one IT disaster after another, and to top it all off, a huge HIPAA fine.

Feeling overwhelmed — but determined to turn things around — Sydney reaches out to an experienced MSP.

One year later …

Sydney's no longer losing sleep — or money — over HIPAA. And, more importantly, her hospital's running more smoothly than ever, with modern IT tools that make it easier for Sydney and her staff to do their jobs.

Making IT Happen

Tom owns a small toy company.

Tom's father founded the business before Tom was born. Tom's dream is to continue growing what his father built. But to do that, things need to change.

Tom partners with an MSP to bring his IT infrastructure into the 21st-century — and in compliance with the dizzying number of regulations that manufacturers face.

The MSP takes care of all things IT, freeing up Tom to take care of his staff, his customers, and his dad's legacy.

We're happy to answer any questions you may have.
Contact us to schedule a FREE consultation!

Sources:
1. Funding Circle 2. Deloitte 3. NAVEX 4. Ponemon 5. Ponemon 6. KPMG

Compliance. Managed.

Keeping up with regulatory requirements can be difficult for growing businesses — but it doesn't have to be.

Say hello to comprehensive compliance management.

Get in touch today!

englerit.com | **(443) 390-2575**

Corporate HQ

1910 Towne Centre Blvd, Suite 250
Annapolis, MD 21401

Operations Center

6600 Chase Oaks Blvd, Suite 100
Plano, TX 75023

ENGLER IT

THE 20