Compliance and Cyber-security

Navigating requirements, frameworks, and solutions

FIELD EFFECT

Table of contents

Introduction

There's something extremely satisfying about finishing a task and checking off a box on a to-do list. It's equal parts the satisfaction of a job well done and a feeling of progress. One done and on to the next one, after all.

Cybersecurity tasks aren't always so neat and tidy. Everything that is done should, ideally, ladder up to a larger effort to reduce the threat surface and secure an organization—but who determines what those efforts should be? What does "good" cybersecurity look like, and who checks on it? Who ensures that's it up to date and evolving as threats change?

The less-than-exciting answer is, often, "auditors." Auditors from various regulatory bodies, governments, or other institutions get the final say on whether an organization's cybersecurity efforts are compliant with best practices, laws, and regulations.

To that end, the cybersecurity to-do list becomes even more complex, incorporating concerns about technologies, policies, and practices to ensure compliance. Yet the elephant in the room is that compliance is hard. It's stressful, time-consuming, and often confusing—kind of like cybersecurity itself can be.

Compliance often gets treated as a check-the-box activity—but because it's taking something inherently subjective and trying to fit it into that neat check box, there's a lot of room for interpretation. That can lead to headaches and frustration, or worse, regulatory penalties and other major challenges.

The good news is that, by treating cybersecurity compliance as not only critical to business but a strategic element of normal operations, you can take proactive steps to improve both your protection and your regulatory standing to confidently check compliance tasks off your to-do list.

Understanding cybersecurity compliance

Like the cybersecurity industry itself, compliance can seem like a sea of acronyms and jargon. NIST, PCI DSS, HIPAA, GDPR, PIPEDA, ISO 27001... the list goes on. And those are just the frameworks themselves, let alone the many controls or requirements therein. As daunting as this can be, starting with one piece of information or one area of concern can help build the baseline needed to navigate compliance topics.

Before digging into specifics around established regulations or frameworks, we need to understand what compliance is, and why it matters.

What is compliance?

Compliance is a series of activities, policies, and processes organizations undertake to ensure they meet the various requirements established by government or regulatory authorities. Broadly, there are two types of compliance: regulatory compliance and what could best be described as *"best practices"* compliance.

Regulatory compliance refers to the specific laws, regulations, and frameworks established by governments or other regulatory bodies, usually for a specific industry. Regulatory compliance frameworks are often stringent with their requirements, generally involving periodic audits where in-scope organizations must demonstrate how they adhere to each control. The Health Insurance Portability and Accountability Act (HIPAA) is an example of regulatory compliance.

Failure to provide proof of adherence, or gaps uncovered during the auditing process, can result in fines, even more exacting audits in the future, and other serious penalties. Extreme cases of noncompliance can even result in an organization being unable to continue operations.

By comparison, best practices compliance refers to voluntary efforts to align with a widely used framework, not because of legal obligation, but because the organization has determined it's in their best interest. While some of these frameworks involve an auditing process, there is no legal or financial penalty for noncompliance, and organizations are often given a fair opportunity to address any gaps uncovered during an audit. The National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) is an example of best practice compliance.

Both forms of compliance have a bearing on the cybersecurity industry. Specific industries have specific requirements over how data and information technology are handled and managed; some requirements have legal obligations, while others are widely adopted standards that most organizations operate by.

Why is compliance important?

Compliance is a bit like the carrot and stick: regulatory authorities reward compliant organizations by recognizing their efforts and punish noncompliant organizations with fines or legal action. At its core, then, compliance matters because staying compliant ensures an organization can keep operating—for regulatory compliance frameworks—or is following the guidance of external experts to operate safely and protect intellectual property, employees and/or customers.

But in the context of cybersecurity, compliance is particularly important to:[1]

- Protect sensitive data
- Meet legal requirements
- Maintain customer trust
- Enhance an organization's overall security posture
- Access cyber insurance

If there's a common theme here, it's risk reduction. Cyber insurance and an improved security posture reduce risks for organizations, and the legal requirements and protections protect their customers. In fact, reducing risk and preventing harm are central concepts to most regulations and controls.

The consequences of noncompliance

Noncompliance leads to more than just increased risk, though. Organizations found to be noncompliant with regulatory compliance frameworks are subject to enforcement from various governing bodies, and may face fines, legal action, and in extreme cases may be shut down. In a more abstract sense, noncompliance can damage an organization's reputation, making it harder to attain or retain customers.

To put this in perspective, consider the European Union's General Data Protection Requirement (GDPR). While the GDPR may not have immediate cybersecurity implications, it's a great example of how information technology (IT) and the digital world collide with the real world.

The GDPR was created to protect fundamental rights and freedoms related to personal data, and authorities have numerous enforcement tools at their disposal.[2] The regulation grants authorities the ability to fine noncompliant organizations up to USD$21 million, or four percent of their annual worldwide revenue from the prior fiscal year, whichever is higher.[3] In May 2023, social media company Meta was fined a massive USD$3.1 billion for alleged breaches in privacy law.[4]

While these are some of the most severe enforcement actions, reserved for high-profile, large-scale cases, they serve as a reminder of how compliance can affect day-to-day business in big ways.

Key cybersecurity frameworks and regulations

Now that we have a baseline understanding of cybersecurity compliance, we can explore some of the key regulations, frameworks, and standards that may apply. The regulations and frameworks listed below are not exhaustive, but are some of the most referenced in the cybersecurity industry due to their IT and data management implications.

The Healthcare Insurance Portability and Accountability Act (HIPAA)

Established in 1996, HIPAA is a United States Act of Congress that modernized the flow of healthcare information. HIPAA stipulates how personally identifiable information (PII) maintained by the healthcare and health insurance industries should be protected from fraud and theft.[5] The act applies to most individuals and organizations that use and/or access the Protected Health Information (PHI) of patients treated inside the USA, regardless of citizenship.

HIPAA was originally applicable to physical records, but most healthcare clinics and organizations have digitized patient information into Electronic Protected Health Information (EPHI). EPHI has revolutionized how patient care is tracked and delivered, but it has also introduced sensitive data to a whole new range of threats. To combat these threats, it's important that in-scope organizations have policies, procedures, and technical safeguards in place to ensure the confidentiality, integrity, and availability of the EPHI under their control.

The Payment Card Industry Data Security Standard (PCI DSS)

First released in 2004, the Payment Card Industry Data Security Standard (PCI DSS) is a set of technical and operational requirements designed to protect credit card data from theft and misuse.[6] Prior to PCI DSS, each major credit card issuer (e.g., American Express, Visa, etc.) had its own security rules for vendors who stored, processed, or transmitted cardholder data. PCI DSS unified and strengthened these baselines to address increasingly sophisticated cyber threats while accounting for greater use of credit and debit cards.

The latest version of PCI DSS, v4.0, was released in March 2022. Vendors and companies that process cardholder data may continue to use v3.2.1 until March 2024, at which point the older versions will be retired.

The NIST Cybersecurity Framework (CSF)

NIST's Cybersecurity Framework (NIST CSF) is one of the most widely recognized cybersecurity frameworks, and often forms the basis for others. The framework is the result of collaboration between private industry and government security experts. It aims to provide organizations—regardless of size, risk exposure, or cybersecurity sophistication—with a set of best practices, standards, and guidelines for managing and reducing cybersecurity risks.[7]

NIST CSF is intended to be a living document that gets updated according to changing cyber threats. The framework is also a fitting example of best practice compliance, as adhering to the framework is entirely voluntary. Since then, the CSF has evolved to become a type of barometer for any organization to assess its cybersecurity maturity.

ISO 27001

The International Organization for Standardization (ISO) sets the international standard for information security through ISO 27001. ISO 27001 outlines and defines what an effective information security management system (ISMS) looks like. Originally published in 2005, with updates in 2013 and 2022, the standard has been referred to as "the world's best-known standard for information security management systems (ISMS)".[8]

ISO 27001 is a risk-based (as opposed to rule-based) standard designed to work for organizations of all sizes. To comply with risk-based standards, organizations must complete a thorough risk assessment and, in the case of ISO 27001, identify how the 93 controls in Annex A can help reduce the impact and frequency of those risks.

The Federal Risk and Authorization Management Program (FedRAMP)

Established in 2011, the Federal Risk and Authorization Management Program (FedRAMP) is a US government initiative to provide a standardized approach for monitoring, authorizing, and conducting security assessments on cloud products and services.[9] FedRAMP seeks to ensure that government departments and agencies have a framework to follow to better manage cloud computing risks through assessment and continuous monitoring.

Common compliance requirements

Chances are most organizations will face some unique mix of regulatory requirements at any given time. A healthcare organization operating in the United States may very well face requirements under both PCI DSS and HIPAA.

The good news? There is a lot of overlap between various frameworks, and they often share similar cybersecurity requirements or best practices. These commonalities can help with clarity and apply pressure on cybersecurity vendors to consider these when designing their solutions.

This overlap across frameworks and regulations is increasingly common as multiple nations and regions adopt common technical requirements, standards, and guidelines; for example, as mentioned earlier, the NIST CSF has served as a baseline for other standards and frameworks. Adherence to the CSF would thus mean some degree of compliance with these other models.

Here are some requirements commonly found in regulations and frameworks:

Information access controls

These requirements typically focus on demonstrating efforts to control user access. These controls can be addressed via policies as well as technologies that can monitor, identify, alert on, and even block unauthorized access.

Keeping information in the right hands is a central concept for cybersecurity and indeed one of the primary concerns of the field, so it makes sense that information access controls are a common thread in compliance. Without diving too deep into the topic, access control is often a primary function of security solutions—regardless of how they are marketed or presented.

A key consideration here, though, is that a solution must address the entirety of the modern threat surface—endpoint devices, networks, and cloud services. This is a critical component of preventing unauthorized access holistically. Layers of protection close gaps in traditional coverage, not to mention automatically detecting, isolating, and stopping identified threats.

Field Effect's holistic cybersecurity solution, Covalence, supports access control policies by monitoring for and detecting authentication attempts that fall outside normal patterns of use. Additionally, by monitoring for unauthorized disclosure and extraction of information, Covalence can lock cloud accounts and endpoint devices as a data leakage prevention measure if anomalies are detected.

Protection against malicious threats

Attackers are becoming more sophisticated in their tactics, partly to avoid traditional detection tools such as antivirus and endpoint detection and response (EDR) tools. Attackers may exploit open vulnerabilities, target unprotected attack surfaces, or deploy zero-day attacks those tools cannot yet detect.

This is why more frameworks and regulations are mandating that organizations not only look at what they can do to defend against known threats—that is, previously identified ones—but also what they can do to spot and defend against emerging or "unknown" threats.

Successfully doing this requires a combination of signature- and heuristic-based analytics, like those found in Covalence. This combination ensures that known threats are identified quickly and efficiently, while novel and emerging ones are flagged for further investigation by an analyst. Covalence also employs industry-standard indicators of compromise (IOCs) along with our own threat intelligence to protect against a wide array of threats, including malicious systems, domains, botnets, ransomware, and more.

Incident logging

Recording when an incident is detected, and retaining logs for future reference is a core component of many cybersecurity regulations and frameworks. For example, under HIPAA, if a log, note, or record relates to a HIPAA policy or procedure, then that item must be retained for six years from the date it was last used or was last effective.

On paper, that's a straightforward requirement. In practice, it represents a vast amount of information. Consider that, in 2022 alone, there were 707 breaches reported to the US Department of Health and Human Services (HHS); that averages out to 500 exposed records reported for every day of 2022.[10]

Under HIPAA, audit logs comprise records of network access, including when and at what time, and a list of the actions taken and/or data and documents viewed. These logs are a requirement for full compliance.

A SIEM (security information and event management) platform has been the fallback solution for compliance-driven logging needs. It centralizes all security events and logs to allow for granular visibility and stores information for future analysis. However, SIEMs are notoriously complex and noisy, and often too much for organizations without a well-staffed Security Operations Center (SOC) to manage them. They may capture the logs, but often don't provide the necessary cybersecurity alongside log retention.

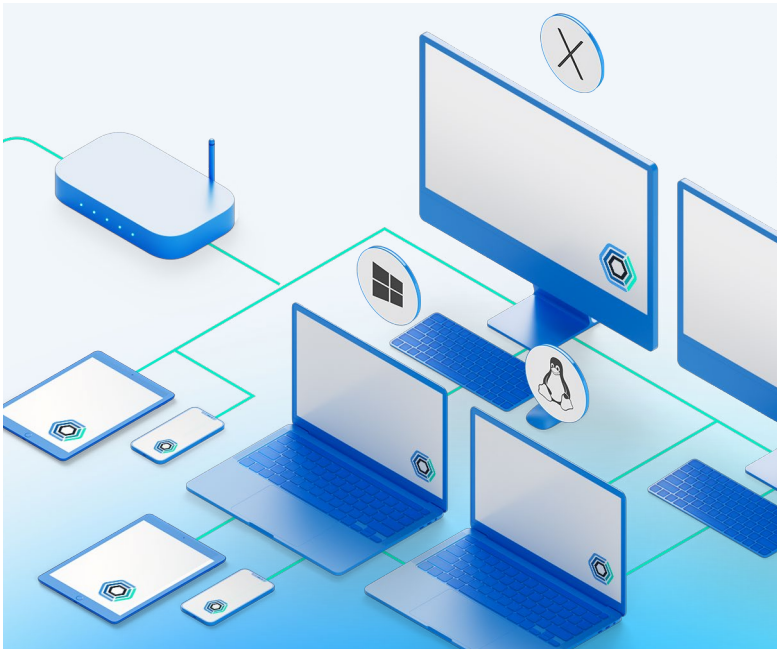
Covalence offers a central repository for logs and alerting, combined with long-term retention in a protected cloud server to help meet this requirement. It provides SIEM-like logging, storage, and retrieval—without the usual cost and complexity.

Network monitoring

The network is a critical component in cybersecurity, even as threat surfaces expand into the cloud, and as such being able to demonstrate that some degree of network monitoring is in place is a major consideration in multiple frameworks and regulations.

Without network protection, organizations lack the visibility and context needed to stop a range of attacks—including those that compromise the authenticity of communication sessions, such as man-in-the-middle attacks or session hijacking.

Using Covalence's network monitoring functionality as an example, the appliance acts as a network-based intrusion detection system (NIDS) capable of deep-packet inspection and alerting. It monitors event logs and system activities for anomalous behavior, abnormal traffic patterns, known attack characteristics, firewall configuration issues, and other unusual system behaviors—helping organizations meet this critical requirement.



Vulnerability monitoring

What steps are being taken to identify and address potential vulnerabilities? Closely related to protection against malicious threats, most compliance frameworks outline the specific need to spot and address security vulnerabilities. From a risk reduction perspective, it makes sense, as vulnerabilities make it easier for threat actors to achieve their goals. Organizations should be actively trying to identify and resolve security gaps—either through vulnerability monitoring or proactive threat hunting—before they can be exploited. Why deal with the fallout of the explosion when it could be avoided instead?

Covalence monitors endpoints, networks, and cloud applications to identify technical vulnerabilities, and provides detailed steps on how to address each one. Identifying vulnerable software and systems or insecure configuration of certain infrastructure in real-time makes it much easier to resolve these issues quickly.

Policies and physical controls

Clear policies, procedures, and controls are critical for many frameworks, particularly ISO 27001. These policies outline and inform the overall security functions and operations of an organization and may not even be directly related to information technology.

You may have heard the saying before: an organization's cybersecurity is only as strong as its physical security. It's true and often requires that organizations implement policies around things as straightforward as office visitors and device locking.

More practical cybersecurity-focused policies are often required, and it's important that staff remain informed about where to access these policies and what they entail. Beyond improving your general cybersecurity, policies even provide audit criteria so that external parties can ensure the organization is abiding by its own written rules and procedures.

But drafting and implementing policies isn't the easiest job. Field Effect compliance experts can work with you to help draft appropriate policies to ensure security and compliance, as well as simply answering any compliance-related questions, including those around physical controls.

HOW TO:

Simplify compliance while improving your overall security

The common thread between nearly every cybersecurity regulation and framework is that an effective solution can go a long way towards helping organizations improve their overall defense. Looking for solutions that already map to common requirements and frameworks helps ensure that boxes are checked off.

That said, not all cybersecurity solutions are created equal. There are several key elements to watch for when assessing potential solutions and their ability to support an organization as they navigate compliance complexities.

Comprehensive visibility and security

Cybersecurity regulations and frameworks don't focus on just endpoint, cloud, or network threats because threat actors don't just focus on a particular part of your threat surface either. The end goal of effective cybersecurity is to reduce risk across your entire IT environment to improve your defense.

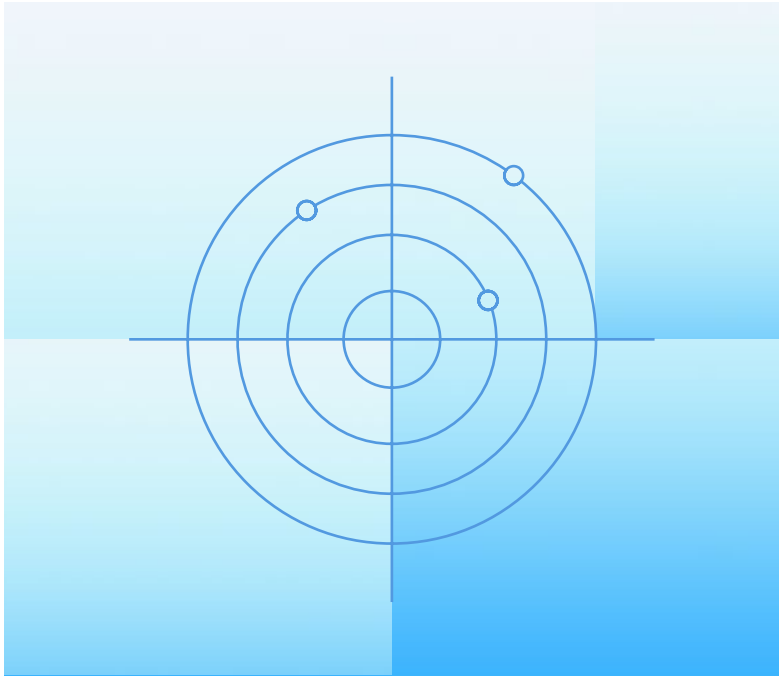
Many point solutions or narrowly focused tools lack the functionality, capability, or comprehensive visibility to tackle the wide range of controls required by various frameworks or regulations. As such, organizations should look to implement a more complete cybersecurity solution, mapping to more controls and/or requirements in one fell swoop and making it easier to track your compliance efforts.

A second key point to keep in mind is that the threat landscape is always evolving. So not only should the cybersecurity solution be holistic, but it should also be continually updated to reflect new and emerging tactics, techniques, and procedures used by threat actors.

Identifying and addressing noncompliance

It can sometimes feel like noncompliance is identified at the worst possible time, preventing organizations from earning new business by missing contract stipulations or otherwise impeding normal operations. Being able to identify areas of noncompliance requires careful mapping of specific security controls to solution functionality, a process usually only found on mature solutions or those backed by extensive cybersecurity expertise.

Put simply, compliance is hard, and the ideal cybersecurity solution will help make it easier by translating complex technical requirements into actionable tasks staff can tackle as part of their day-to-day.



Continued support and guidance

If it wasn't clear already, the real key to compliance success is working with those who have walked the path before and know how to navigate it, and who have proper cybersecurity experience to outline how a solution maps to requirements. No matter the situation, finding a cybersecurity solution that allows an organization to reach out to experts in the compliance space to answer their questions is crucial to continued success.

Working with trusted experts can help ensure that compliance programs succeed and continue to operate, supporting an organization's internal efforts to incorporate regulatory concerns as a strategic driver instead of a reactionary process.

The ideal cybersecurity solution, from a compliance perspective, must be able to confidently take a holistic approach to defense, ensuring a comprehensive overview of an organization's defenses while providing additional support, service, and insight.

Conclusion

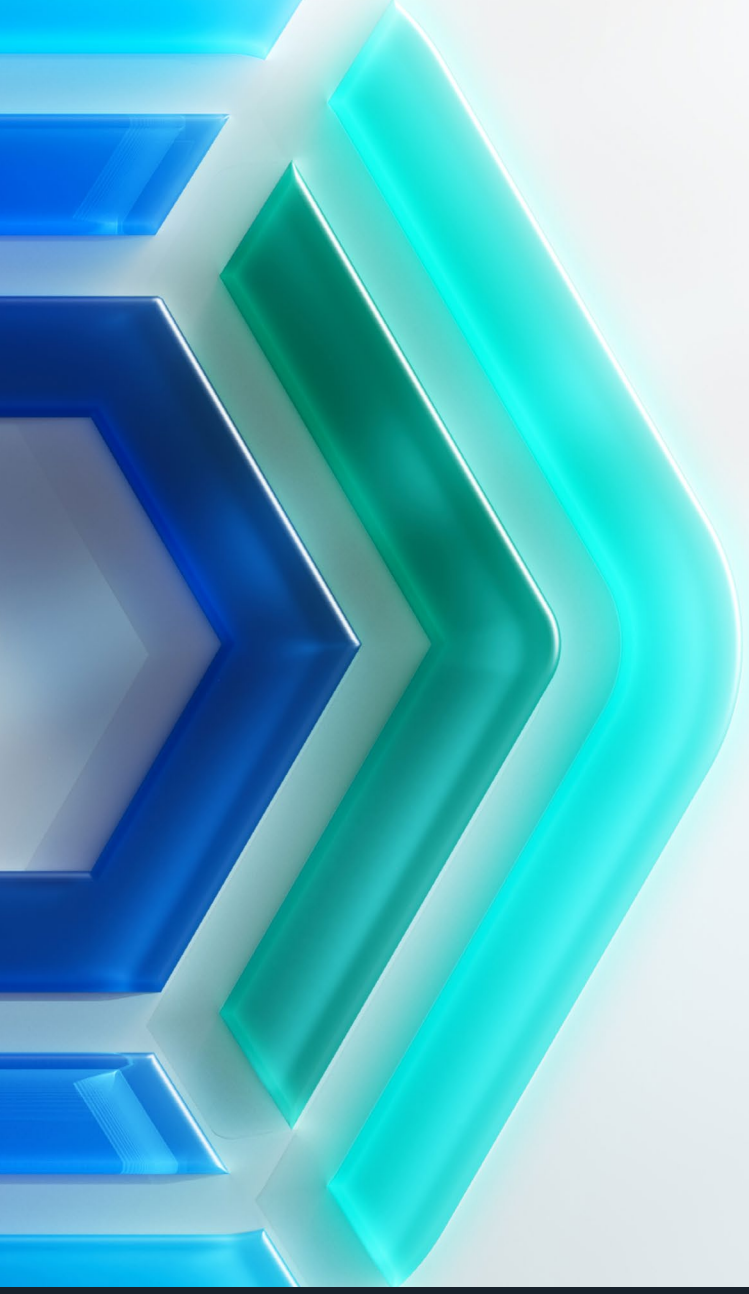
If you take one thing away from this white paper, let it be this: compliance is hard, but taking steps to address it now can help ensure the road ahead is clear and easy to follow.

The cybersecurity solution you choose can play a significant role in compliance success and allow you to achieve the protection the frameworks are trying to enforce. Organizations need an always-on solution that defends against cyber threats. You need actionable information that improves and enhances cybersecurity—without taking time out of your busy day. You need a continuous view of potential cyber risks and malicious activity, backed by expertise, to prevent cyber threats and eliminate security vulnerabilities easily.

While compliance will never quite be a simple to-do list you can check off in an afternoon, by rethinking your approach to these topics and incorporating them into your risk management strategy, you can access true peace of mind.

SOURCES

1. https://www.in.gov/cybersecurity/blog/posts/cyber-compliance-101-what-it-is-and-why-its-needed/
2. https://gdpr-info.eu/art-1-gdpr/
3. https://gdpr.eu/fines/
4. https://www.washingtonpost.com/technology/2023/05/22/meta-fined-eu-facebook-data-privacy/
5. https://aspe.hhs.gov/reports/health-insurance-portability-accountability-act-1996
6. https://docs-prv.pcisecuritystandards.org/PCI%20DSS/Standard/PCI-DSS-v4_0.pdf
7. https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf
8. https://www.iso.org/standard/27001
9. https://www.fedramp.gov/program-basics/
10. https://www.hipaajournal.com/healthcare-data-breach-statistics/



The most sophisticated cyber threat monitoring on the planet, made simple.

Covalence is an award-winning cybersecurity solution that provides transparent, holistic managed detection and response for your whole IT infrastructure in one platform, no matter where you are or where your endpoints are located. No add-ons, no modules, and no gaps in your security. Learn more about Covalence.

Covalence

About Us

Contact our team today.

Website:

Phone:

Email: