

WHY YOUR BUSINESS NEEDS AN INTEGRATED COMPLIANCE STRATEGY

AT A GLANCE:

Types of Compliance Standards and Regulations
How Integrated Compliance Strategy Works
Case Study: From Zero to Security and Compliance Hero
Conversations Over Questionnaires

The Compliance Landscape Today

Does it feel like the minute you wrap your brain around your organization's compliance requirements, someone goes and changes the rules? **Regulations can be not only difficult to implement and maintain**, but also produce a figurative mountain of data that's hard to decipher. Add to that the threat of fines or other punishment for not maintaining compliance, and it can lead to a real drain on both your human and financial resources.

A single compliance examination or audit can take as long as 10 to 12 weeks. And while it may seem like the path of least resistance to use multiple, specialized auditing service providers to complete all the necessary audits, the reality is, **it can be expensive, inefficient, and lead to conflicting recommendations.**

The good news is that you can save time, money, and sanity by **trading in your multiple vendors for one strong provider to oversee all your cybersecurity compliance assessments.** A solo audit service provider means one travel charge, one communication channel to ensure that important components aren't overlooked, and one team that sees your entire business across all frameworks.

Simply put? An integrated compliance solution makes life easier for everyone involved.

Part of a Stronger Cybersecurity Strategy

Protecting your company from cyber attacks is essential to ensuring the safety and privacy of sensitive data. Take these six steps to create a strong plan for your organization:

01 Identify the right compliance/regulatory framework for your organization by focusing in on business objectives, real needs, and smart solutions.

02 Assess the benefits of a quick, cheap fix now vs. a more expensive, long-term solution.

03 Hire an highly-trusted cybersecurity compliance firm to conduct risk assessments and penetration testing in order to uncover weaknesses in your security framework.

04 Develop and enable security protocols on several levels:

Physical: Laptop security, employee and guest identification controls, and other hardware protections.

Administrative: Implementation of compliance controls, policies, and procedures.

Technical: Software protection, including user access restrictions and wifi requirements.

05 Train employees on acceptable-use policies and security best practices, with regularly scheduled refresher courses.

06 Conduct routine monitoring and maintenance of your cybersecurity strategy to remain up-to-date.

At a Glance: Types of Compliance Standards and Regulations

The first step to compliance is understanding which sets of standards and regulations are applicable to your business. Here's a quick look at some of the most common types of regulations and their target industries:

SOC Examinations


- What It Is:** System and Organization Controls (SOC) reports establish credibility, trustworthiness, and commitment to governance over an organization's ethical and compliant operations.
- Who It's For:** Any third-party service provider that may touch, store, process, or impact their clients' financial or other sensitive data.



PCI DSS

- What It Is:** The Payment Card Industry Data Security Standard (PCI DSS) helps decrease internet payment card fraud. Becoming a PCI-compliant provider demonstrates that customers' credit card data is secure.
- Who It's For:** Any business that intends to accept card payments and store, process, or transmit cardholder data.

ISO 27001 Certification

- What It Is:** Standards for establishing, assessing and managing an organization's information security management system.
- Who It's For:** Any kind of organization that holds sensitive information, from IT companies with customer data to culinary institutes with secret recipes.
- 



GDPR Compliance

- What It Is:** General Data Protection Regulation (GDPR) sets guidelines for the collection and processing of personal information about citizens of the European Union.
- Who It's For:** Any company that stores sensitive information of an EU citizen, regardless of where the company is based.

HIPAA / HITECH

- What It Is:** Both the Health Insurance Portability and Accountability Act (HIPAA) and Health Information Technology for Economic and Clinical Health (HITECH) are federal regulations requiring how confidentiality, integrity, and availability of electronic, protected health information (ePHI) is addressed.
- Who It's For:** Any healthcare or healthcare Software-as-a-Service (SaaS) provider that carries out electronic patient transactions.



HITRUST

What It Is: The Health Information Trust Alliance (HITRUST) developed a common security framework (CSF) that provides a comprehensive approach to handling sensitive data. It combines elements of many separate but related standards, such as HIPAA, HITECH, ISO 27001 and others.

Who It's For: Healthcare organizations and their business partners who face a large number of regulatory requirements.

Microsoft SSPA

What It Is: The Microsoft Supplier Security and Privacy Assurance Program (SSPA) is designed to regulate how the company's suppliers handle sensitive Microsoft employee, customer, or vendor data.

Who It's For: Required for any supplier that wants to do business with Microsoft.

Experian EI3PA

What It Is: Experian Independent Third-Party Assessment (EI3PA) demonstrates that credit history information shared by its partners is kept secure. It follows the controls outlined by the PCI DSS.

Who It's For: Any organization that handles Experian credit information.

FISMA

What It Is: The Federal Information Security Management Act (FISMA) establishes specific documentation, policies and procedures, and defined processes for the storage, handling, and protection of federal data.

Who It's For: Federal agencies, vendors, or subcontractors that transmit or store federal data.

How Integrated Compliance Strategy Works

If you're used to working with multiple compliance vendors, how is an integrated solution different? Here are a few of the ways the process can change **when you partner with a single service provider.**

One Trusted Point of Contact

An integrated approach to compliance means having one partner to oversee and conduct all your required audits / assessments and other business regulatory requirements. **It's a singular approach to assuring data security, privacy, compliance, and processing integrity that's customized to your organization's needs.**

At the same time, an integrated approach means access to experienced seasoned professionals who've helped companies overcome challenges similar to yours, such as reducing the number of audits each year, expanding into regulated markets or industries, and obtaining valuable feedback throughout the process.

The result is a vendor relationship that evolves from one-time final report delivery to **long-term compliance strategy.**



Integrated Compliance is a Long-Term Plan

An Integrated Compliance Strategy is a more holistic approach that takes into account the diverse needs of your business, as well as industry trends and competitive forces. A compliance team will take time to thoroughly understand your business, your approach, and your goals to devise a strategy that meets the needs of today and plans for tomorrow.

Integrating Saves Time and Money

An integrated compliance solution means one planning phase, one execution phase, and one delivery phase. No more sifting through multiple reports, constructed in widely different formats, to try and find common threads or valuable nuggets of information. Instead, a single auditing team learns your business inside and out – once – and then gets to work on a timeline and strategy that reduces the time and workload required by you and your employees. The result is not just a process that's quicker and less stressful, but also significantly more efficient and valuable.

Putting one vendor in charge of multiple audits also helps eliminate communication breakdowns that can result in important pieces getting left behind (or left out completely). Missing a compliance requirement isn't an option when it comes to regulatory compliance and certification, and having to rework means extra time, money and pressure.

And, on the practical side of the cost equation, having only one vendor and an integrated audit means less travel and related expenses.

Better Protection For Your Clients' Data

Implementing an integrated solution allows your audit provider to see your entire data infrastructure, including potential weaknesses and opportunities to **streamline across areas where siloed vendors might not make the connection.**

Over time, a single cybersecurity and compliance auditor gains valuable insights to your overall business better than a single-service compliance auditor who has a very limited view. This long-term, deep relationship allows you to reap the benefits of recommendations tailored to your business making your risk assessments more effective with ways to incorporate scanning, penetration tests, and other proactive measures into your overall security and compliance strategy.

The result is a defensive stronghold built around the data you capture, process, or store for your clients.



From Zero to Security and Compliance Hero

Ontic Technologies, a leading provider of Protective Intelligence Security Software, delivers technology to empower security teams to protect assets, employees and customers. In today's world, you, your company, your employees, your students, or your physical assets may come under some kind of threat or attack. Investments in physical and other security systems have already been

made to protect these critical assets – **but are they working together, proactively, and preemptively?** Ontic provides proactive protection that leverages deep analytics and intelligence to discover signals, investigate risk, and initiate immediate, collaborative action. Ontic exists to make businesses safer by serving intelligence to those who protect.

Compliance Becomes Ontic's Advantage

As a new category of security software, Ontic needed a unique value proposition in order to instill confidence in the enterprise buyers of this market. Potential customers needed to know they could trust Ontic, so **compliance with standards and regulations impacting their customers would be the secret superpower that kept prospective relationships from stalling due to compliance concerns.**



Ontic needed a vendor that could work with their **fast-paced, fast-growing team** that was spread out across **multiple remote locations**.

Choosing the Right Vendor Makes All the Difference

Ontic knew they needed an examination of their controls supporting the security, availability, and confidentiality of their systems and how they handle customer data. They wanted a vendor that could work with their fast-paced, fast-growing team that was spread out across remote locations. **They needed a firm that had experience with startups and enterprise organizations;** a trusted counsel on what a large organization would expect from a new vendor.

Familiar with our reputation, Ontic CEO Lukas Quanstrom reached out for a consultation. **Our team dug in deep, gaining critical insight into Ontic's current data collection**

and management, as well as their short and long-term sales strategy and how these strategies could affect compliance options. After our comprehensive discovery process, we recommended an integrated compliance strategy, starting with a SOC 2 examination and HIPAA security assessment.

We developed and executed a structured, phased approach to complete the SOC 2 and HIPAA initiatives as part of a larger holistic approach to Ontic's overall organizational strategy. **This approach saved Ontic time and money** while providing two impressive compliance deliverables for the demanding prospects Ontic wanted to engage.

An Integrated Strategy Set the Stage for Big Wins

With the successful completion of the SOC 2 and HIPAA assessment, **Ontic now speaks to large enterprises confident that they meet the stringent requirements**

for vendor due diligence. While many vendors have taken an early exit on these opportunities, Ontic stepped up.



Conversations Over Questionnaires

What makes 360 Advanced different? **We prefer conversations over questionnaires.** We provide **year-round consultations with no hidden fees.** We tailor our services to each client, making sure we're always transparent with the delivery of our professional services.

- Relationship-focused auditors
- Actionable recommendations
- Flexible and thorough Q+A process
- Pre-assessment guidance
- Integrated services to save time and money
- Structured phases and review processes
- Collaborative approach with weekly status updates
- Quality reporting
- Fixed fees
- Year-round consultations

Let's chat to see if we're the right fit.

(866) 418-1708

INFO@360ADVANCED.COM

360ADVANCED

200 Central Avenue, Suite 2105, St. Petersburg, FL 33701