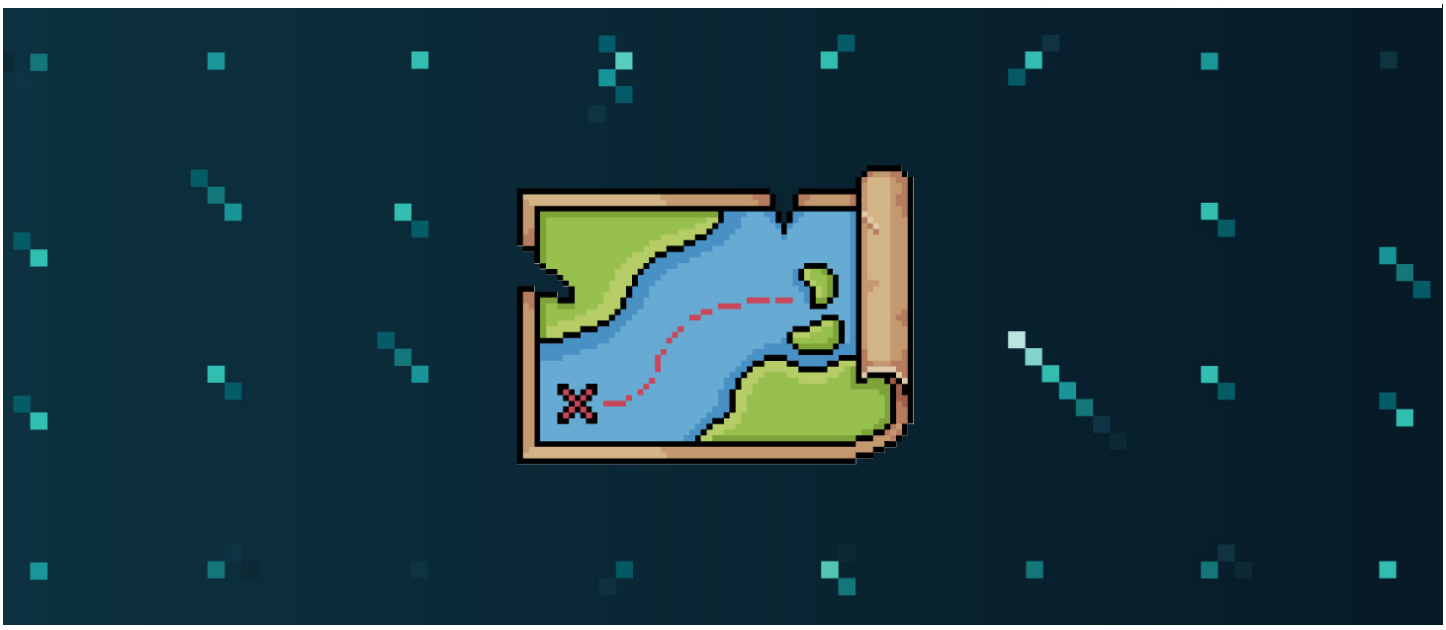


BACK TO BLOG

# Cybersecurity compliance: The Essential Guide for 2024

James Harrison

January 8, 2024

SOC 2, ISO, HIPAA, Cyber Essentials – all the security frameworks and certifications today are an acronym soup that can make even a compliance expert's head spin. If you're embarking on your cybersecurity compliance journey, read on to discover the differences between standards, which is best for your business, and how vulnerability management can aid compliance.

What we do How we do it Pricing Resources Company LOGIN TRY FOR FREE

Cybersecurity compliance means different things to different businesses in different industries and locations, but essentially it means you have met a set of agreed rules regarding the way you protect sensitive information and customer data. These rules can be set by law, regulatory authorities, trade associations or industry groups.

For example, the GDPR is set by the EU with a wide range of cybersecurity requirements that every organization within its scope must comply with, while ISO 27001 is a voluntary (but internationally recognized) set of best practices for information security management. While not mandatory, compliance may be necessary if you've signed a contract requiring it.

Agreements like these with customers and suppliers are increasingly driving compliance. Customers expect the assurance that compliance brings, because breaches and data disclosure will impact their operations, revenue and reputation too.

## Which cybersecurity compliance standard is right for you?

Every business in every industry is operationally different and has different cybersecurity needs. The safeguards used to keep hospital patient records confidential are not the same as the regulations for keeping customers' financial information secure.

For certain industries, compliance is the law. Industries that deal with sensitive personal information such as healthcare and finance are highly regulated. In some cases, cybersecurity regulations overlap across industries. For example, if you're a business in the EU that handles credit card payments, then you'll need to be compliant with both credit and banking card regulations (PCI DSS) and GDPR.

Security basics like risk assessments, encrypted data storage, vulnerability management and incident response plans are fairly common across standards, but what systems and operations must be secured, and how, are specific to each standard. The standards we explore below are far from exhaustive, but they are the most common compliance for

## GDPR

### What is GDPR compliance?

The General Data Protection Regulation (GDPR) is a far-reaching piece of legislation that governs how businesses – including those in the US – collect and store the private data of European Union citizens. Fines for non-compliance are high – up to €20,000,000 or 4% of global revenue – and the EU is not shy about enforcing them. Better security rarely comes free, and managing your vulnerabilities is no exception, but the expense of proper vulnerability management is extremely low compared to the costs of GDPR fines, not to mention damages caused by a breach itself.

### Who needs to comply with GDPR?

Buckle up because it's essentially anyone that collects or processes the personal data of anyone else in the EU, wherever they go or shop online. Personal information or "personal data" includes just about anything from the name and date of birth to geographic information, IP address, cookie identifiers, health data and payment information. So, if you do business with EU residents, you're required to comply with GDPR.

### How vulnerability scanning can aid compliance with GDPR

Your IT security policy for GDPR doesn't have to be a complicated document – it just needs to lay out, in easy-to-understand terms, the security protocols your business and employees should follow. You can also use free templates from SANS as models.

You can start taking simple steps right away. There are automated platforms that make it easier to work out which requirements you already meet, and which ones you need to correct. For example, you're required to "develop and implement appropriate safeguards to limit or contain the impact of a potential cybersecurity event" which vulnerability scanning using a tool like Intruder can help you achieve.

## SOC 2

SaaS and born-in-the-cloud businesses that provide digital services and systems will be most familiar with SOC 2 as it covers the storage, handling and transmission of digital data, although certification is becoming increasingly popular with all service providers.

SOC is managed by AICPA and based on achieving several specific criteria. There are two reports: Type 1 is a point-in-time assessment of your cyber security posture; Type 2 is an ongoing audit by an external assessor to check you're meeting these commitments, reviewed and renewed every 12 months.

Like ISO 27001, SOC 2 gives you some wiggle room on how to meet its criteria, whereas PCI DSS, HIPAA and most other security frameworks have very explicit requirements. You can find full details of the required criteria in this pdf document on the AICPA website or in our dedicated SOC 2 guide.

### Who needs SOC 2 compliance?

While SOC 2 isn't a legal requirement, it's the most sought-after security framework for growing SaaS providers. It's quicker and cheaper to achieve than most of the other standards in this list, while still demonstrating a concrete commitment to cyber security.

### How do you comply with SOC 2?

SOC 2 compliance requires you to put in place controls or safeguards on system monitoring, data alert breaches, audit procedures and digital forensics. The subsequent SOC 2 report is the auditor's opinion on how these controls fit the requirements of five 'trust principles': security, confidentiality, processing integrity, availability and privacy. You don't have to cover every category if they don't apply to your business operations, but one control you need for your SOC 2 report is vulnerability management using a scanner like Intruder – that's exactly what we did, using our own tool alongside Drata's compliance platform for our own report. Find out more in our handy guide to SOC 2 compliance and see how vulnerability management can get you there faster.

## ISO 27001

### What is ISO 27001 compliance?

The International Organization for Standardization, or ISO, produces a set of voluntary standards for a variety of industries – ISO 27001 is the standard for best practice in an ISMS (information security management system) to manage the security of financial information, intellectual property, personnel information, and other third-party information.

Unlike some standards, ISO 27001 is not a legal requirement by default, but many large enterprises or government agencies will only work with you if you are ISO certified.

It's recognized as one of the most rigorous compliance frameworks but it's notoriously difficult, expensive and time consuming to complete, even with a dedicated team or external consultants.

### Who needs it?

Like SOC 2, ISO 27001 is a good way to demonstrate publicly that your business is committed and diligent when it comes to information security, and that you've taken steps to keep the data you share with them secure. If you work in a highly regulated industry like finance, handle sensitive private data such as medical records, or if customers want an internationally recognized standard, then ISO 27001 may be

The ISO itself does not hand out certifications. Instead, third-party auditors validate that you've implemented all of the relevant best practices in accordance with the ISO standard.

There isn't a universal ISO 27001 compliance checklist that guarantees certification either. It's up to each organization to decide what's in scope and implement the framework, and auditors will use their discretion to evaluate each case.

Remember that ISO 27001 is largely about risk management. Risks are not static and evolve as new cyber threats emerge, so you should build automated vulnerability management with a tool like Intruder into your security controls to evaluate and analyze new risks as they emerge – you can find out more in our ISO 27001 compliance guide. Automated compliance platforms such as Drata can also help speed up the whole process too.

## PCI DSS

### What is PCI DSS compliance?

The PCI DSS (Data Security Standard) was developed by the PCI Security Standards Council and the major card brands (American Express, Mastercard and Visa) to regulate anyone that stores, processes, and/or transmits cardholder data.

Many payment card-using businesses, especially retailers and restaurants, don't know about PCI. After a hack, they may wish they did. When Target revealed that criminals got their hands on the credit card details of 40 million customers, it was using malware installed on their US point-of-sale (POS) network. It wasn't necessarily the work of a cybercriminal mastermind either; Forbes found they could hack into unsecured POS systems with equipment costing just $25. And while PCI is not technically a legal requirement, credit card companies and banks will expect it. Fail to comply, and they may stop you taking card payments or charge you more for doing so.

### Who needs it?

In theory, anyone that processes card payment transactions, but there are different rules depending on the number and type of payments you take. If you use a third-party card

### How to comply with PCI DSS

Unlike ISO 27001 and SOC 2, PCI DSS requires a strict vulnerability management program, but accreditation is complex. Third-party payment providers will usually populate the PCI form for you automatically, providing validation at the click of a button. For smaller businesses, this can save hundreds of hours of work; for larger ones, it can save thousands. If you're looking to implement cyber security best practices to help with PCI DSS, we can help.

## HIPAA

### What is HIPAA compliance?

HIPAA (the Health Insurance Portability and Accountability Act) regulates the transfer and storage of patient data in the US healthcare industry, where compliance is a legal requirement. And it makes sense too, because healthcare is a prime target for identity theft. Unlike credit card details, which at least change when cards expire, personal health information never changes and can be used for tax fraud, to take out false credit cards or loans, and open fraudulent bank accounts – which is why health records can go for 40 times as much on the black market as credit card numbers. HIPAA is designed to protect this sensitive information.

### Who needs it?

HIPAA compliance is mandatory for any business that handles patient information in the US, or anyone doing business in the US with companies that are also HIPAA compliant.

### How to comply with HIPAA

Although a part of life for anyone working in healthcare in the US, HIPAA can be difficult to navigate. The rules cover two categories: privacy and security, which requires a thorough assessment of the potential risks and vulnerabilities to the "confidentiality, integrity, and availability of electronic patient information that you create, receive, maintain, or transmit". It also requires a risk management plan with security measures sufficient to reduce risk to a reasonable and appropriate level. Although HIPAA doesn't specify the methodology,

## FedRAMP

### What is FedRAMP compliance?

The Federal Risk and Authorization Management Program is a US government-wide program designed to promote the adoption of secure cloud services by federal government agencies through a standardized approach to security and risk assessment.

### Who needs it?

Only federal agencies themselves need FedRAMP certification, but if you work directly with a government department in the US, you may be asked or hear about FedRAMP, so it's worth knowing what it entails. You can find out more on the FedRAMP website.

### How can vulnerability scanning aid compliance with FedRAMP?

While not necessary for non-governmental organizations, it's worth noting that it specifies operational visibility, managed change control, incident response, and continuous monitoring. So, if you work with a federal agency it may be worth proving or improving your security credentials and posture with a recognized standard such as SOC 2 or ISO 27001.

## NIST

### What is NIST compliance?

NIST, or the National Institute of Standards and Technology, creates cybersecurity standards, guidelines, best practices, and other resources to meet the needs of US industry, federal agencies and businesses in general. Its work ranges from producing specific information that you can put into practice immediately to long-term research that anticipates advances in technologies and future challenges.

### Who needs it?

Rather than specific certifications, NIST provides guidelines and best practices for contractors, universities and research institutions that receive federal grants, or anyone providing

benchmark for their own cybersecurity programs (including other certification bodies such as FedRAMP).

### How can vulnerability management aid compliance with NIST?

Continuous monitoring is integral to NIST's guidelines, where it defines Information Security Continuous Monitoring (ISCM) as the "ongoing awareness of information security, vulnerabilities, and threats to inform risk-based decision making" through continuous assessment and analysis of the effectiveness of all security controls, ongoing reporting of the security posture of IT systems, and risk management to reduce risk to acceptable levels.

## Cyber Essentials

### What is Cyber Essentials compliance?

Cyber Essentials is a UK government-backed scheme designed to check businesses are adequately protected against common cyberattacks. Similar to SOC 2, think of it as good cyber hygiene – like washing your hands or brushing your teeth. Designed for the smaller business without dedicated security expertise, it should be just the starting point of a more robust security program but it is widely recognized and demonstrates that you are trustworthy and take security seriously. What's more, if you're looking to win public sector contracts, Cyber Essentials may be necessary for any bid.

### Who needs Cyber Essentials compliance?

Any business bidding for a UK government or public sector contract which involves sensitive and personal information or providing certain technical products and services.

### How to comply with Cyber Essentials

The basic certificate is a self-assessment of five basic security controls: firewalls, secure configuration, user access control, malware protection and patch management. The self-assessments are available through a secure hosted platform. Cyber Essentials Plus provides a higher level of assurance through a technical audit of the systems that are in scope for Cyber Essentials. An assessor will test a sample of your user

## How to build a cybersecurity compliance program

With so many compliance framework, how can you build a cybersecurity compliance program that fits your needs and those of your chosen standard? With so many different standards, where do you start? While there's no one-size-fits-all approach – every standard or framework has its own requirements and criteria - there are steps you can take to streamline your compliance journey, whichever you decide to is best for your business...

### 1. Create a compliance team

Your IT team is the primary force for cybersecurity compliance. While IT teams typically handle most cybersecurity issues and processes, cybersecurity doesn't exist in a vacuum. In other words, everyone in your organization needs to work together to maintain good cybersecurity hygiene to reinforce your compliance measures.

### 2. Set up a risk analysis process

Although naming conventions will vary between frameworks, there are four basic steps in any risk analysis process:

- Identify: any systems, assets or networks that have access to data
- Assess: review the data, assess the risk level, and rate the risk where that data will pass through in its lifecycle
- Analyze: determine and prioritize the likely risk to your business: likelihood of breach x impact or cost
- Decide tolerance: agree what risks to fix, mitigate, transfer or accept

### 3. Mitigate or transfer risk

Set up security controls that mitigate or transfer risks to prevent, detect and mitigate cyberattacks and threats such

- Encryption and MFA
- Next generation firewalls
- Staff training
- Incident response
- Access control
- Patch management
- Vulnerability scanning

### 4. Monitoring and remediation

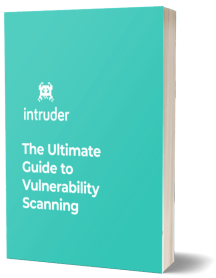
Continuously monitor systems and your attack surface as regulations evolve or are updated. The goal of a compliance program is to identify and manage risk and catch cyberthreats before they turn into a full-blown data breach. It's also critical to have business processes in place that allow you to remediate quickly when attacks do happen to avoid fines and damage to your reputation.

NIST provides a useful cyber security framework for managing risk that you can incorporate into your compliance program and tailor to meet your specific needs.

## Compliance doesn't need to be complex

Compliance can seem like a labor-intensive and expensive exercise, but it can pale in comparison to the cost of fixing a breach, paying settlements to customers, losing your reputation, or paying fines. You can also miss out on potential business if you don't have the certifications customers expect.

But cybersecurity compliance doesn't need to be difficult with today's automated tools. If you use Intruder's vulnerability management that already integrates with automated compliance platforms like Drata then auditing, reporting and documentation for compliance becomes a whole lot quicker and easier. Whether you're just starting your compliance journey or looking to improve your security, we can help you get there faster. ***Get started today with a free trial***




## Get Our Free "Ultimate Guide to Vulnerability Scanning"

Learn everything you need to get started with vulnerability scanning and how to get the most out of your chosen product with our free PDF guide.

DOWNLOAD OUR FREE PDF GUIDE

Written by James Harrison

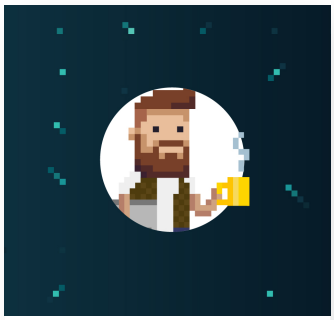
# Recommended articles


### Security compliance 101 with Intruder and Secureframe

Highlights of our latest webinar on how to achieve security compliance. Read for

### DevSecOps best practices: how to secure your pipeline

Many DevOps advantages actually create security



### What's new? Product updates from Intruder November 2023

out how easy it can be with the right tools.

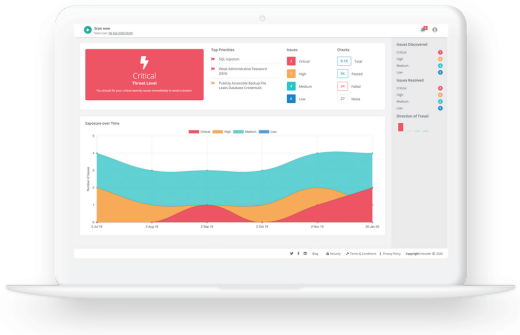
James Harrison — October 23, 2023

your dev pipeline with Intruder.

Christian Gonzalez — November 21, 2023

verifying that authenticated web apps have been setup correctly is now much easier, and a new compliance integration!

Andy Hornegold — November 14, 2023



## Ready to get started with your 14-day trial?

TRY FOR FREE

intruder

**SOLUTIONS**
Developers
Start-ups and scale-ups
Enterprise

**COMPARISONS**
Intruder vs

**USE CASES**
Automated Penetration Testing
Cloud Vulnerability Scanner
Network

**RESOURCES**
Developer Hub
Help Centre
Blog
Guides
Glossary
Success Stories
Research

**COMPANY**
About Us
Contact
Become a Partner
Careers (We're hiring!)