hyperproof

GUIDE

How to Prioritize Implementing New Compliance Frameworks



hyperproof.io // info@hyperproof.io

Table of Contents

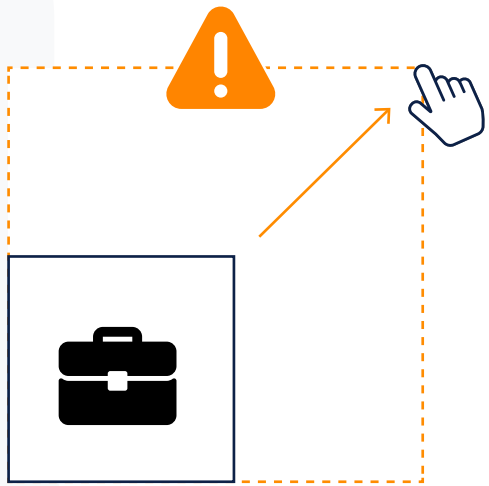
Introduction **3**

The 7 dimensions of risk management and compliance **5**

1. Regulatory compliance and governance 6
2. Cybersecurity requirements 7
3. Operational risks 8
4. Risk management processes 9
5. Workforce compliance 10
6. Legal and intellectual property protections 10
7. Financial and tax compliance 10

Adopting new compliance frameworks is necessary for market expansion **11**

Common compliance frameworks companies have adopted 13
How to budget for new compliance frameworks 22
How to prioritize and decide which compliance framework(s) to implement next 32
Reduce your compliance burden and manage multiple frameworks efficiently with Hyperproof 34



Introduction

Expanding and scaling a company requires careful risk management and compliance planning, especially as you grow into new markets and increase operational complexity.

As your product lines and customer base grow, so will the number regulations you need to adhere to. At this stage in your growth, you'll run into the inevitable: having to identify one or more compliance frameworks to implement to enable business expansion, unlock new markets, and grow your business.

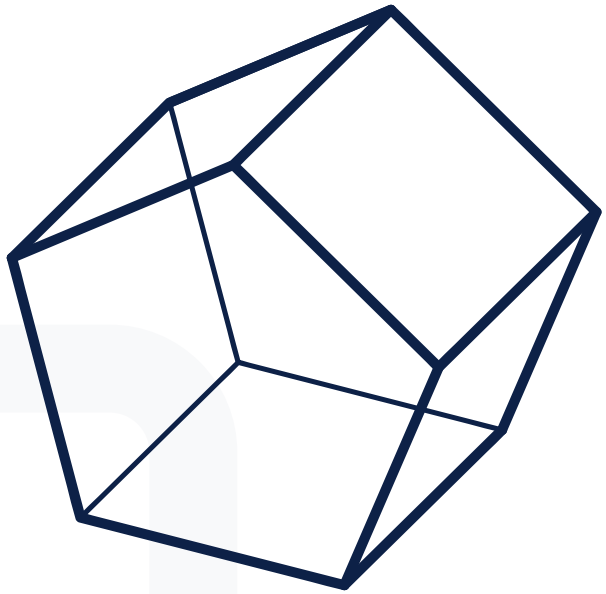
Compliance frameworks provide structured approaches to managing and securing data, protecting a company's IP, and maintaining user privacy in accordance with regulatory requirements. These frameworks help establish processes for data protection, risk assessment, and incident response.

In this comprehensive guide, we'll cover:

- A broad set of risk management and compliance considerations for growing businesses
- Common and newer compliance frameworks companies adopt based on their stage, data handling, customers, and industry
- Practical questions to help you make the best decision for your organization

This guide will help you holistically consider risk management and compliance and identify the next framework(s) your organization should implement, balancing risk and growth for your company's expected trajectory.





The 7 dimensions of risk management and compliance

Growing and scaling a business requires strategic planning around managing risks and ensuring compliance. The following section outlines a structured approach to tackle these challenges from a compliance and cybersecurity viewpoint.

1. Regulatory compliance and governance

Data privacy regulations

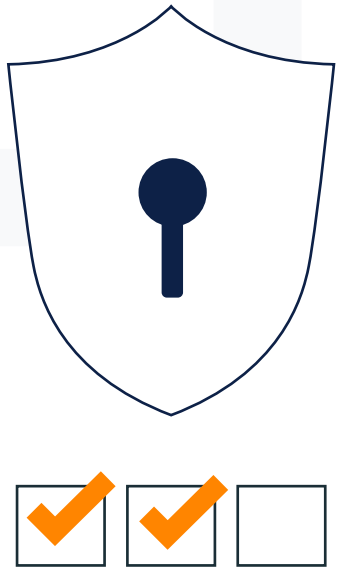


As your business expands, you'll likely deal with more personal data from customers or employees. Your growth makes compliance with data protection laws like the General Data Protection Regulation (GDPR) in the EU or the California Consumer Privacy Act (CCPA) crucial. Non-compliance can lead to significant fines and reputational damage. Growing companies need to:

- Conduct regular privacy impact assessments
- Implement data encryption and anonymization
- Establish procedures for responding to data breaches within required timeframes

Additionally, depending on your industry, you may need to comply with specific regulations like HIPAA for the healthcare industry, PCI-DSS for the payment card industry, or Sarbanes-Oxley (SOX) for financial reporting. Understanding the regulatory landscape in your target markets and building systems to monitor compliance is critical.

As you scale internationally, it's crucial to understand local laws regarding data storage, intellectual property, and digital communications. Countries like the US, Canada, Australia, China, the United Kingdom, and Brazil all have laws governing how businesses must handle and secure resident's data. Laws like DORA and NIS2 affect infrastructure providers operating in certain EU vertical markets. This may require expanding your compliance team or hiring regional experts.



2. Cybersecurity requirements

As you grow, you become a more attractive target for cybercriminals. A proactive cybersecurity approach includes:

Access control and authentication: Implement multi-factor authentication (MFA) for sensitive systems. Apply the principle of least privilege, regularly audit user access and promptly remove inactive or terminated users.

Regular audits and penetration testing: Conduct vulnerability assessments to identify system weaknesses, particularly after significant system changes.

Incident response plan: Develop a clear incident response plan to handle data breaches or cyberattacks, including legal obligations, communication strategies, and recovery procedures.

Cloud security: Ensure cloud providers meet robust security standards like ISO 27001 or SOC 2®. Verify their data handling and disaster recovery processes meet your business's needs.

3. Operational risks



As you scale and rely on more third-party vendors, you need a robust vendor risk management program that includes:

Vendor due diligence: Assess vendors' security policies, financial stability, and compliance posture before engagement.

Ongoing monitoring: Conduct regular reviews of vendor performance and risks through audits and reporting.

Contractual safeguards: Ensure contracts with vendors contain clear data protection clauses, particularly around breach notification and data-handling standards.

Scaling up can increase operational complexity, so a business continuity plan (BCP) is essential to ensure your company can continue operations during a crisis. A solid BCP includes:

- Regular backups of key data and systems with redundancy built into IT infrastructure
- Disaster recovery testing, where you simulations to test your ability to recover from critical failures like cyberattacks, server failures, or natural disasters



4. Risk management processes

Once an organization has been operating for a few years and has established departments and teams, it should implement a comprehensive enterprise risk management (ERM) program to reguarly assess strategic, financial, operational, and compliance risks. The program should:

- Identify risks across departments
- Quantify the impact and likelihood of each risk
- Assign owners for each risk
- Implement and track mitigation strategies

While many risks can be mitigated through direct action, insurance should be essential to your risk exposure limitation plan. Cybersecurity insurance, errors and omissions (E&O) insurance, and directors and officers (D&O) insurance become critical as your exposure increases. Ensure you have coverage that aligns with your business risks, and regularly review policies as your operations grow.

5. Workforce compliance

As your team grows, especially internationally, compliance with labor laws becomes more complex. This includes managing employment contracts, benefits, and workplace safety. You may need HR compliance specialists to ensure adherence to local regulations.

Your employees can be a strength or a liability for risk management. Create and regularly update compliance and security awareness training to ensure they understand phishing attacks, social engineering tactics, and corporate policies on data handling.

6. Legal and intellectual property protections

As you scale, protecting your intellectual property (IP) becomes critical, especially when entering new markets. Work with legal teams to ensure patents, trademarks, and copyrights are in place. For foreign markets, work with experts to understand the varying legal frameworks for IP protection and enforcement across jurisdictions.

7. Financial and tax compliance

Expansion may introduce new tax liabilities, particularly in different states or countries. Consult with tax experts to ensure compliance with tax laws in all regions where you operate.

As your company scales, you may need to adhere to more stringent financial reporting standards, especially if you want to raise venture capital or prepare for a public offering. Implement systems to ensure accurate, timely financial reporting and consider third-party audits.

Adopting new compliance frameworks is necessary for market expansion

As organizations grow and enter new markets, adopting the right compliance frameworks becomes a strategic necessity rather than a regulatory checkbox. Each market brings unique compliance requirements, from data protection standards to financial and operational regulations.

These frameworks not only protect companies from legal risks but also build trust with new customers, partners, and stakeholders. For example, expansion into Canada requires compliance with the Personal Information Protection and Electronic Documents Act (PIPEDA), which outlines strict data handling and consent guidelines.





Similarly, suppose a fintech company aims to do business in Singapore. In that case, it must adhere to regulations from the Monetary Authority of Singapore (MAS), which oversees financial regulations and supervises a wide range of businesses and activities, focusing on the stability, transparency, and security of Singapore's financial system. Businesses handling the personal data of Japanese citizens must follow the Act on the Protection of Personal Information (APPI), a comprehensive data protection law that emphasizes transparency, data security, and accountability in handling consumer information.

Adopting these frameworks early allows companies to establish their operations on a foundation of trust and regulatory compliance, reducing the friction often faced when entering new regions. A proactive compliance strategy signals prospective partners and customers that the company values security and operational transparency, accelerating adoption and acceptance in new markets and ensuring smoother global expansion with minimized risk.

Common compliance frameworks companies have adopted

When organizations adhere to multiple regulations, identifying key **compliance frameworks** helps streamline processes and reduce compliance burden. Compliance frameworks provide structured approaches to managing and securing data in accordance with regulatory requirements. These frameworks help organizations establish processes for data protection, risk assessment, and incident response.

Most customer organizations we've worked with make compliance framework selections pragmatically based on their company stage, the requirements and expectations of their current and target customers, the operational complexity of their business, and the regulations and rules governing their industry. Below, we've published findings on the common frameworks companies have adopted.



Note: Regulations can change quickly, and every organization should consult with an attorney to ensure you are up-to-date with all applicable regulations. The data shown below is not legal advice but rather to help provide information about what peers in the US, Canada, and UK are doing.

By company stage and customer type

Company stage	Target customer type	Frameworks
Early-stage B2B startups selling their first product	US-based for-profit companies	SOC 2® Type 2
Early-stage B2B startups and more established B2B businesses	European and/or global for-profit companies	ISO 27001 / 27002 CIS Controls NIST CSF
Established B2B businesses	US government agencies, for-profit companies that primarily sell products/ services to U.S. government agencies	FedRAMP NIST SP 800-53
Established B2B businesses	US Department of Defense	CMMC
Soon-to-go public companies and publicly traded companies in the US	Variable	COBIT and COSO (to comply with the Sarbanes-Oxley Act)

Data type and applicable data protection regulations

The types of data you store and process will drive your compliance roadmap. Below are the various "protected" data types regulated by multiple laws, standards, and frameworks.

Data type	Applicable regulations and laws governing such data	Frameworks
Patient data / health data of individuals	**US:** HIPAA (US) HITech Act (Health Information Technology for Economic and Clinical Health Act) Federal Trade Commission (FTC) Health Breach Notification Rule Substance Abuse Confidentiality Regulations	HITRUST CSF (Common Security Framework) ISO 27001/27002 NIST Privacy Framework CIS Controls (Center for Internet Security) BS 10012 (Personal Information Management - PIMS)
	EU: GDPR EU ePrivacy Directive (Cookie Law) NIS Directive (Network and Information Systems Directive) UK Data Protection Act 2018 (UK GDPR)	

Chart continues →

Data type	Applicable regulations and laws g overning such data	Frameworks
Personal data of individuals (“data subjects”) within the European Union and European Economic Area (EEA). This can include: Name, address (including email addresses), identification numbers (such as ID card numbers, social security numbers), online identifiers (like IP addresses, cookies, device IDs), and location data. GDPR has stricter rules for special categories of personal data (“sensitive data”), which include health information, racial or ethnic origin, political opinions, religious beliefs, trade union membership, and sexual orientation.	GDPR (EU) UK Data Protection Act 2018 (UK GDPR)	ISO 27001/27002 NIST Privacy Framework CIS Controls (Center for Internet Security) HITRUST CSF (Common Security Framework) BS 10012 (Personal Information Management System - PIMS) EU-US Data Privacy Framework

Chart continues →

Data type	Applicable regulations and laws governing such data	Frameworks
Personal data of minors Depending on the specific rule, minors may be children under the age of 13 or teens under the age of 16.	**US:** California Consumer Privacy Act (CCPA): this law includes provisions that provides additional protection to minors under the age of 16. Children's Online Privacy Protection Act (COPPA)	While there isn't an official framework to adhere to laws around managing the data of children/ minors, the key requirements are: • **Parental Consent:** Getting verifiable parental consent when collecting, processing, or selling data from children below certain age thresholds • **Privacy Policies:** Creating clear, concise, written privacy policies in language understandable to children and parents • **Security:** Implementing strong security measures to protect the data of minors from unauthorized access, breaches, or misuse • **Right to Control and Delete Data:** Allow parents and in some cases children to review, control, and delete data
	EU: GDPR - children's data is considered a special category that requires extra protection. EU ePrivacy Directive (Cookie Law)	

Chart continues →

Data type	Applicable regulations and laws governing such data	Frameworks
Financial data (credit card numbers, bank account details, loan information, and investment records)	**US:** Gramm-Bliley Act (GLBA) - Privacy Rule & Safeguard Rule California Consumer Privacy Act (CCPA) California Privacy Rights Act (CPRA) New York Department of Financial Services (NYDFS) Cybersecurity Regulation SEC Cybersecurity Rules Sarbanes-Oxley Act (SOX)	Payment Card Industry Data Security Standard (PCI DSS) ISO 27001/27002 ISO 27701 NIST CSF SOC 2® CIS Controls (Center for Internet Security) COBIT CSA STAR Certification
	EU: Payment Services Directive 2 (PSD2) GDPR	
	Global: Anti-money laundering and Know Your Customer Regulations	

Chart continues →

Data type	Applicable regulations and laws governing such data	Frameworks
Intellectual Property and Trade Secrets	**US:** Defend Trade Secrets Act (DTSA) of 2016 Economic Espionage Act (EEA) of 1996 Uniform Trade Secrets Act (UTSA) Computer Fraud and Abuse Act	NIST CSF ISO 27001/27002 SOC 2 CIS Controls (Center for Internet Security) CSA STAR Certification Non-Disclosure Agreements (NDAs)
	EU: Directive (EU) 2016/943 on the Protection of Trade Secrets The Network and Information Security (NIS) Directive GDPR	

Chart continues →

Data type	Applicable regulations and laws governing such data	Frameworks
Government data (If you are contracting with a government agency or are a sub-contractor of an entity contracting with a government agency)	**US:** Federal Information Security Management Act (FISMA) Defense Federal Acquisition Regulation Supplement (DFARS) - Cybersecurity Requirements Gramm-Leach Bliley Act (GLBA)	FedRAMP NIST SP 800-171 CMMC Criminal Justice Information Services (CJIS) Security Policy ISO 27001/27002
	EU: The Network and Information Security (NIS) Directive EU Classified Information (EUCI) Framework Data Act (Upcoming) Germany's Federal Data Protection Act (BDSG) France's Law on Military Programming European Defence Fund (EDF) and Related Security Regulations National Critical Infrastructure Laws (various) GDPR	

Chart continues →

By industry/business type

Industry	Business type	Common frameworks
IT/Technology	Software/SaaS/Cloud Companies	SOC 2® Cloud Security Alliance Cloud Controls Matrix NIST CSF ISO 27001 / 27002 NIST Risk Management Framework NIST AI Risk Management Framework
IT/Technology	Healthcare providers, hospitals, health insurance, Healthcare IT, pharmaceutical and biotech	HITRUST
Banking / Financial Services / FinTech	Banks and fintech companies	Payment Card Industry Data Security (PCI DSS) ISO 27001/27002 SOC 2® Open Banking Standards

How to budget for new compliance frameworks

Implementing compliance frameworks requires both strategic planning and financial commitment. By setting realistic timelines and budgeting appropriately, compliance professionals can manage the costs and complexities of these frameworks while positioning their organizations for growth, market expansion, and successful audits.

Here's a breakdown of what to expect regarding timelines, steps, and cost estimates for common frameworks.





SOC 2® Type 2

For companies aiming to achieve SOC 2® Type 2, the timeline generally ranges from four months to a year, depending on the organization's maturity and preparedness. SOC 2® compliance requires establishing controls to meet the Trust Services Criteria, which include security, availability, processing integrity, confidentiality, and privacy.

The process begins with a gap analysis to identify existing controls and documentation deficiencies. Next, the organization must close control gaps and create any missing documentation. Following this, the controls must operate effectively for three to six months to ensure reliability before the audit. Securing an auditor and scheduling the audit is another key step that can take additional time. The audit itself may range from a few weeks to several months, depending on the organization's size and complexity.

Estimated cost:

SOC 2® audits typically cost between $15,000 and $60,000, depending on the organization's size, maturity, and chosen audit provider.

ISO 27001 Certification

ISO 27001, a widely recognized information security standard, has a timeline that varies based on organization size and internal resources. Smaller companies may complete the certification process in under a year (or two to three quarters if they are quite mature), while larger organizations may need a year to a year and a half. To gain the ISO 27001 certification, your organization should already have staff with internal auditing expertise.

The process includes several key steps:

- **Gap analysis of controls and Information Security Management System (ISMS) assessment:** This involves defining the ISMS boundary, completing the Statement of Applicability, and determining required controls. This typically takes one month to one quarter. Organizations without prior ISO 27001 experience often hire specialized consultants.
- **Risk assessments and risk treatment planning:** This typically takes a couple of weeks for mature organizations or up to a quarter for less prepared ones.
- **Documentation completion and control implementations:** This step requires a few months to a few quarters.
- **Internal audit to ensure controls function correctly before formal certification:** This can take several months to quarters.
- **External audit:** An auditor reviews documentation, interviews employees, and observes processes to confirm compliance. This can take anywhere from 8-15 months, depending on organization size and complexity.

Estimated cost:

ISO 27001 certification can cost organizations between $15,000 and $100,000, depending on size, maturity, and the depth of pre-existing security measures. Costs include preparation (e.g., consultant fees paid for assistance with risk assessments, control selection, and policy creation), implementation (staff training and security tools), and certification audit costs.



FedRAMP Moderate

For organizations pursuing FedRAMP Moderate designation to bid on U.S. government contracts, the process is both rigorous and costly. On the low end, it takes 16 to 18 months minimum, extending to over two years for complex systems.

FedRAMP requires organizations to establish continuous monitoring (ConMon) systems, requiring around-the-clock staffing for system monitoring, log management, and threat response. This can involve hiring three shifts of staff solely for monitoring and incident response, representing a significant staffing commitment.

The process begins with a gap analysis to evaluate prior compliance experiences and define the authorization boundary. Organizations must then close any identified gaps and produce detailed compliance documentation, particularly the System Security Plan (SSP), which outlines precise operational procedures. The SSP must be kept updated as controls or systems change.

An agency sponsor is required, and securing one can be challenging. Different agencies, such as the Department of Defense (DoD) or the Department of Housing and Urban Development (HUD), may have varying processes and expectations.

After preparing the SSP and securing an agency sponsor, organizations must schedule an assessment from a FedRAMP Third Party Assessment Organization (3PAO). This evaluation is extensive; it includes vulnerability and penetration testing in addition to a thorough review of the SSP.

The 3PAO then sends assessment results to the sponsoring agency. Depending on the assessment results, the time it takes to receive an Authority to Operate (ATO) will vary.

Estimated cost:

FedRAMP implementation will most likely exceed $1 million due to extensive control requirements, staffing needs, and audit costs. However, the return on investment can be substantial for organizations pursuing high-value government contracts.



CMMC 2.0 compliance

For DoD contractors, Cybersecurity Maturity Model Certification (CMMC) 2.0 will soon be essential. CMMC requirements are expected to take effect in mid-2025, but many DoD contracts already assume compliance with the DFARS clause. Organizations should implement necessary controls to meet the DFARS clause requirements stipulated by prior contracts.

Estimated cost:

For organizations pursuing CMMC 2.0 certification, costs can vary widely depending on the certification level required and the organization's existing cybersecurity practices.

Here's an overview of estimated costs for each level:

CMMC Level 1 (Foundational)

This level generally involves self-assessment and is the least expensive, typically around **$4,000 to $6,000**. These costs cover readiness assessments, minor technology investments, and self-assessment efforts for basic cyber hygiene, suitable for businesses handling Federal Contract Information (FCI) with limited security requirements.

CMMC Level 2 (Advanced)

This level targets companies handling Controlled Unclassified Information (CUI) and requires a third-party assessment. This level can be more involved, with estimated costs ranging from **$20,000 to $60,000** for organizations that need minor technology upgrades and documentation work. For a full third-party assessment, however, costs can escalate to **$102,000 for small companies** and **$112,000 for larger ones**, including the triennial assessment and additional annual affirmations (Secureframe).

CMMC Level 3 (Expert)

This level is the most demanding, expected to cost more than one million dollars. This level involves advanced controls, extensive documentation, and readiness for sophisticated threat defenses against advanced persistent threats (APTs). The preparation includes significant cybersecurity infrastructure investments, like multi-factor authentication, endpoint protection, and continuous monitoring systems, and the assessment is often carried out by specialized government-led teams.

Additional preparation costs for gap assessments, CUI scoping, and risk assessments typically range from **$15,000 to $50,000**. Consultant fees vary based on the scope and the duration of engagement needed to meet CMMC requirements. Despite these costs, certification is essential for securing DoD contracts, with potential returns offsetting the investment.

Digital Operations Resilience Act (DORA)

The **Digital Operations Resilience Act (DORA)**, effective January 2025, mandates resilience and data security measures for financial and information communication technology (ICT) providers operating in the European Union. Requirements include comprehensive ICT risk management, timely incident reporting, regular resilience testing (e.g., penetration and disaster recovery), and stringent third-party risk controls.

This legislation's extraterritorial reach also requires non-EU ICT providers with critical roles in EU financial institutions to comply. For instance, B2B software companies doing business with EU financial institutions must create robust data protection programs and ensure regulatory compliance as an extension of contractual commitments.

For a company with solid foundational IT controls and risk management processes in place, preparing for DORA compliance would likely take six to twelve months, assuming foundational IT controls and risk management processes are already in place. DORA mandates additional requirements, such as advanced resilience testing, incident reporting frameworks, and stringent third-party risk management specific to the EU financial services sector. The timeline depends on the organization's existing security controls, capabilities, and resources allocated for its compliance program.



Estimated cost:

DORA is a new framework, so organizations are still in early stages of implementation and do not have a reliable cost estimate for implementation.



GDPR

GDPR applies to any company processing the personal data of EU residents, regardless of location. This includes AI companies with European users, as they process identifiable user data.

GDPR compliance generally takes between 6 months to 1 year for companies with mature data privacy practices, while others may need longer to establish compliance across key areas.

By setting realistic timelines and budgeting appropriately, compliance professionals can manage the costs and complexities of these frameworks while positioning their organizations for growth, market expansion, and successful audits.

Estimated cost:

Costs typically range from **$50,000 to $150,000** for initial setup, with recurring annual costs for data protection officers, compliance tools, and audits.

Other frameworks

Planning and budgeting for other compliance frameworks follows the same general pattern. Conduct a gap analysis between what's required under the new compliance framework and what compliance frameworks and controls are currently operational at your organization. Based on the gap analysis, work with business owners to identify new controls and estimated costs (including staff and solutions, as appropriate). Additionally, work with the go-to-market team to set realistic schedule expectations about when the new framework will be implemented and referenceable in marketing materials and contracts. Once you have an agreed-upon plan to close the gaps, work to close those gaps and establish evidence of control operation proactively and automatically.





How to prioritize and decide which compliance framework(s) to implement next

To figure out the next compliance framework(s) your company needs, consider the following questions:

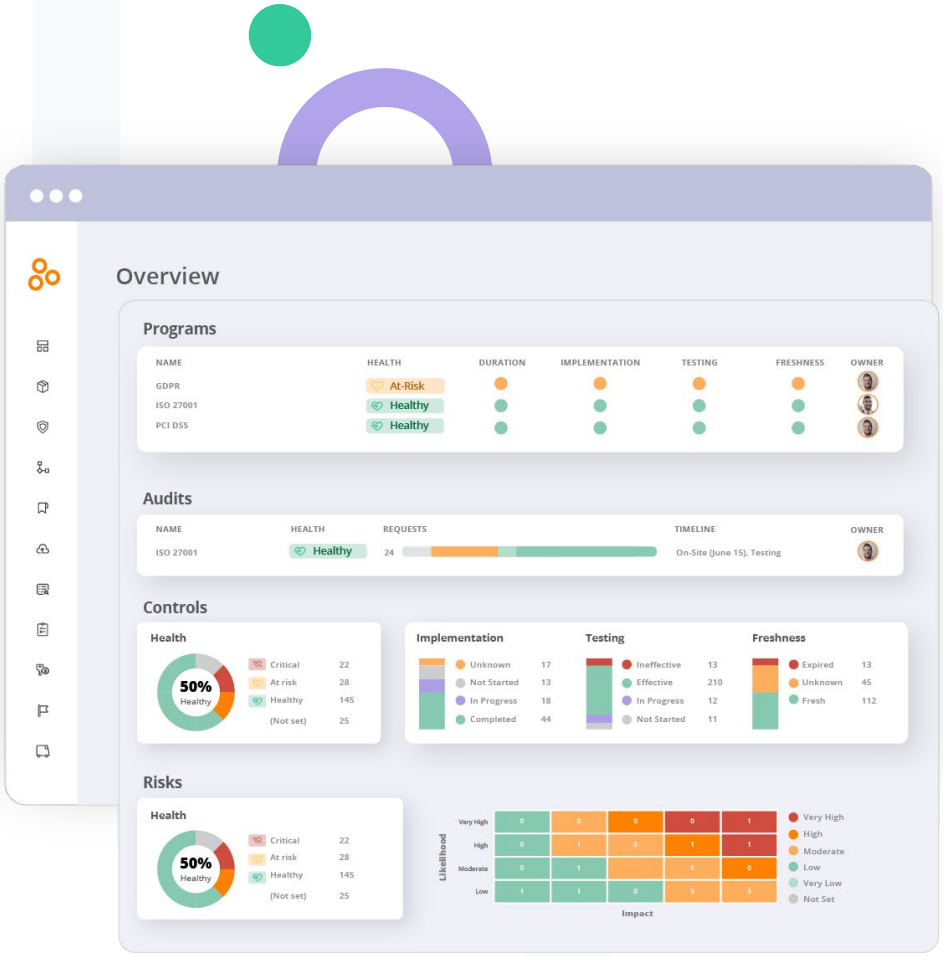
- What market(s) are you going after? What do buyers in this market expect from their vendors?
- Are your target buyers already asking you to comply with this framework?
- Has your company already signed contracts requiring compliance with a given framework?
- What types of data do you need to manage and how sensitive is it?
- How many resources is your company willing to allocate to a new compliance framework?
- Is there a sufficient return on investment if you allocate enough time, money, and effort? For example, do you have enough customers asking for this compliance framework, and what's the size of each contract?
- What does your current state look like? How much would you need to change in your systems, processes, and practices to meet this new framework? Would you need to hire experts and purchase new technology?

Talk to your business stakeholders, legal counsel, security team, IT, and engineering team to find the answers to the questions on the previous page.

For additional perspective, we recommend you talk to similarly situated companies and those you aspire to be like to learn how they approach this decision. Outside experts and advisors can also provide valuable insights.

Be realistic and honest about your company's current state and where you'd like to be in the next 1-2 years. It's not helpful to compare yourself to a company that is so much further ahead of you.





Reduce your compliance burden and manage multiple frameworks efficiently with Hyperproof

Hyperproof is an intuitive and powerful software platform that helps organizations of all sizes efficiently implement compliance frameworks. Organizations take advantage of our extensive library of compliance framework templates, automation, and integrations to easily implement new compliance frameworks, create standardized and unified compliance and risk management practices, and remain continuously compliant.

Get a Demo

About Hyperproof

Hyperproof is a SaaS platform that empowers compliance, risk, and security teams to automate and scale their workflows without the burden of jumping between multiple legacy platforms and spreadsheets. The Hyperproof platform enables teams to get complete visibility into their organizational risks, streamline the audit process, and reduce their ever-growing compliance workloads in one seamless platform. Hyperproof is trusted by leading organizations like Veeva Systems, Fortinet, Motorola, Outreach, and Solventum.

To learn more about Hyperproof, visit **hyperproof.io**

