The Complete Guide to Continuous Compliance

hyperproof

Introduction

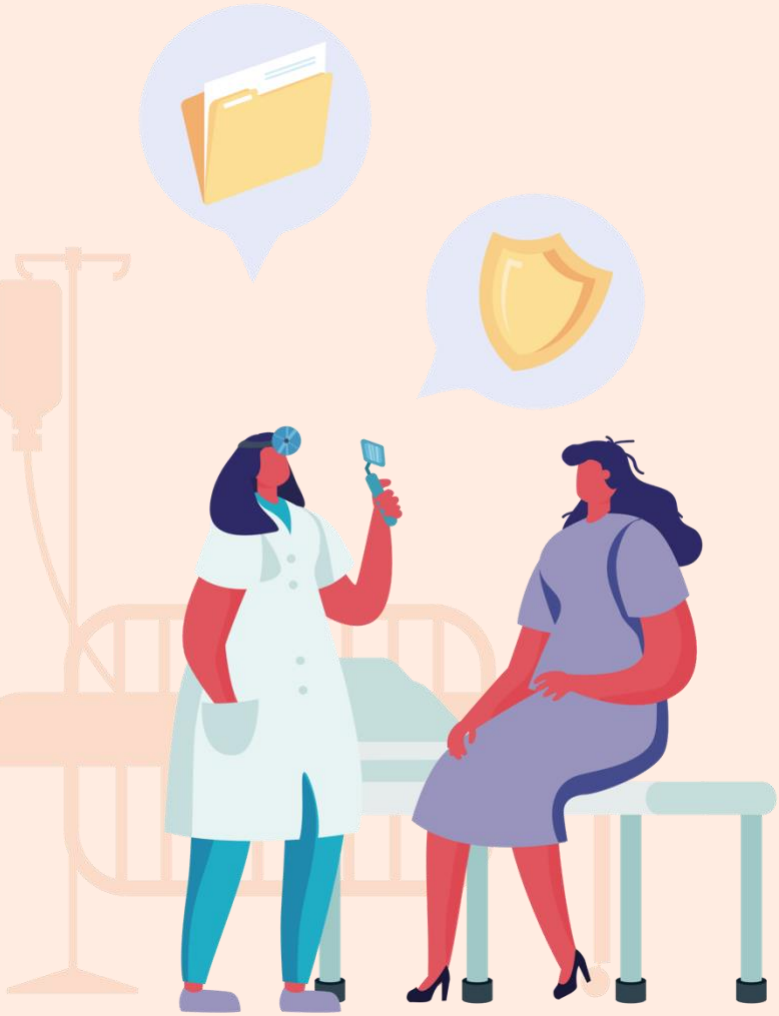
These days, the cost of compliance and the cost of non-compliance are rising for organizations of all types and sizes. We see an influx of new regulations, more stringent enforcement actions from regulators, and an uptick in customer-driven audits. So many organizations have been swept into a never-ending cycle of audit-related work.

When organizations must address an increasing number of regulatory requirements and customer audits each year, they need to have a well-defined, measurable, and repeatable approach to managing their compliance efforts. Without a methodology in place, they're all too likely to suffer from audit fatigue.

Audit fatigue results when a compliance team must work overtime to prepare for every audit, scrambling to remediate issues merely days or hours before an auditor shows up. Audit fatigue occurs when compliance officers struggle to find the evidence they need to present to auditors because documents are poorly labeled and spread across a myriad of systems. Audit fatigue becomes inevitable when operational staff responsible for business processes and controls must frequently put their core projects on hold to respond to compliance requests and remediate issues.

Fortunately, audit fatigue does not need to become a chronic illness for any organization. When you create and stick to a well-defined, measurable, and repeatable approach to compliance, you can say goodbye to audit fatigue once and for all and achieve a state of continuous compliance.

A Definition for Continuous Compliance



Many organizations today approach their compliance efforts in an ad hoc, reactive manner. Compliance-related work is done in surges; the workload picks up when an organization must pass an audit or meet a regulatory deadline. Compliance work is put on the backburner once these events have passed. The cycle starts all over again when the next audit or regulatory requirement rolls around.

Continuous compliance takes the opposite approach; it is an ongoing process an organization engages in to proactively manage their risks. Continuous compliance is about developing a culture and strategy within your organization that continually reviews your compliance position to ensure you are meeting industry and regulatory demands while maintaining secure systems.

Here are some signs that you're operating in a state of continuous compliance:

1. You and your team are fully aware of how your policies, processes and operations stack up against your relevant standards.
2. Your staff knows -- and, more importantly, understands -- what is expected, how those expectations are addressed day-to-day, and how to measure the effectiveness of those requirements.
3. You have streamlined compliance processes. You've automated monitoring of controls and the collection of evidence. Compliance staff no longer need to spend countless hours gathering evidence for external audits. Rather than waiting to find out whether you've passed an external audit, you know whether a control is effective or not in real-time.

When you shift to a mode of continuous compliance, you can expect to spend less time preparing for audits and see more predictable operational costs and lowered security and compliance risks.

Depending on the nature of your business and types of customers you serve, operating in a mode of continuous compliance can create a competitive advantage for your business. When you demonstrate a commitment to compliance, it sends a positive message to the marketplace that you are a mature and developed company, not a fly-by-night operation. When you have a sterling reputation, customers will be more likely to choose you over the competition, qualified candidates will be more likely to choose to work for you, and investors are more likely to fund your growth.

The Playbook to Achieving Continuous Compliance

Getting to a state of continuous compliance requires people, processes, and technology coming together. It involves an organization-wide strategy and focus. Below, we'll provide a simple playbook to help your organization get to a state of continuous compliance.

People

1. Tone from the top

To make continuous compliance a reality, there needs to be strong support from the senior leadership team. Upper management has to set the right tone and send the message that the business intends to take compliance seriously. Additionally, leadership must set well-defined business and compliance goals. There should be a clear understanding of how compliance and security goals support key business objectives.

2. Appropriate incentives

The leadership team should calibrate the rewards system to prompt people to make the right choices. When making promotion and compensation decisions, the leadership team must not only look at people's results but also how they got to their results. Further, leadership must enforce the rules so employees get the message that unethical behavior and compliance lapses will not be tolerated.

3. Dedicated compliance officer

Continuous compliance requires a clear owner. It is important to have a dedicated compliance leader who has the authority and resources they need to get things done.

4. Integration of security and compliance functions

Continuous compliance also requires ongoing collaboration between the compliance team and operations teams like IT and Engineering. After all, operations teams are the ones responsible for implementing IT controls, ensuring adherence to best practice security procedures, monitoring systems, and documenting the controls.

To get operations teams onboard, it is important to communicate how operating from a state of continuous compliance benefits them. When controls are continuously tested and monitored, it reduces the likelihood of operational problems and improves the quality of services IT and engineering delivers. When process owners understand the effectiveness of controls under their purview at all times, it saves them from having to find out about a risk exposure during an audit and having to do unplanned work. It means that they can do a little bit of compliance work on a regular basis and devote the bulk of their time to core projects.

From a practical perspective, the best way to ensure that IT and engineering teams take responsibility for compliance is to work with them to design the controls. This will give IT and engineering teams a sense of ownership over continuous compliance practices. The compliance team should be involved early in the software development cycle so that they can raise security, privacy, or regulatory concerns during the design phase. This is much less disruptive to the business than having compliance raise issues during the review cycle right before the software becomes publicly available.

Processes

Continuous compliance is a process of proactive risk management. It's about putting in place processes so that your team always knows what the highest priority is, the workload becomes predictable, and you understand your compliance posture at all times. Here are the steps you can take to get to a state of continuous compliance:

1. Take inventory of what exists today.
2. Identify common controls that cut across regulations.
3. Implement a process to keep evidence fresh and visible to the compliance team at all times.
4. Implement a testing plan.
5. Create a well-defined project management process.
6. Define a process for keeping up with regulatory changes.

1. Take inventory of your existing policies, procedures, and controls.

To get to a state of continuous compliance, you need to align what you have today -- policies, procedures, and controls -- to the compliance frameworks that matter to your business and your customers. If your policies, procedures, controls and evidence live in an assortment of places today (e.g. spreadsheets, file storage, email attachments), it will be difficult to manage your program and identify your top priorities. The first thing you'll want to do is to centralize all of your documents and files in a single location so you can understand exactly what already exists today. There are tools such as Hyperproof that can serve as a system of record of all of your compliance data.

Once all of your compliance data is in one central location, you'll need to organize the information in a way that's easy to understand. Link your policies, procedures, and controls to the appropriate requirements within regulations that matter to your business. Categorize the data and tag each document so you can easily retrieve this data and reference it in the future.

2. Identify common controls that cut across regulations

The requirements and controls in various regulatory frameworks often overlap, and differing schedules for updates to these frameworks can make meeting all your governance requirements an exercise in duplicative work and wasted resources. The way to reduce the work is to identify common controls that cut across multiple frameworks or standards.

To get to a state of continuous compliance, you need to answer the question: "*how compliant am I with X standard, given that I am Y% compliant with Z standard?*" You'll want to figure out how much one set of requirements overlaps with another requirement, and identify where you can implement one common control to satisfy multiple frameworks (e.g. ISO 27001 and SOC2). There are tools that make it easy to identify overlapping content among frameworks.

> Implementing common controls to meet multiple security frameworks and compliance regimes is not a new practice by any means. But this practice has become especially salient now because the pace of regulatory change has picked up.

In the last couple of years, we've seen numerous new data protection and privacy laws being passed around the world. GDPR came into effect in May 2018. CCPA, the most comprehensive U.S.-based privacy law governing the data rights of Californians will be in effect shortly. Individual states within the U.S. and countries all over the world are creating new laws around data protection and user privacy.

At this point, trying to meet each new law on its own terms will become too expensive, too inefficient and too legally risky to bear. In the realm of user privacy, rather than taking a "wait and see" approach, it is easier, faster, and safer for organizations to create a global data compliance policy framework. Organizations should seek to understand the requirements of different laws, the common intent behind the laws, opt to adhere to the most robust of the laws, and design a common set of controls to satisfy these requirements. By taking this approach, your organization can mitigate the need to re-evaluate legal, operational and engineering practices each time a regulatory body makes a new law.

3. Streamline your evidence collection and management process

One of the tenets of continuous compliance is removing the need for compliance staff to spend time collecting evidence to demonstrate compliance to external auditors. To be continuously compliant, by definition, it means that you have current evidence on hand at all times. Thus, it is important to have a streamlined process to collect evidence and keep it fresh and visible to the compliance team at all times. Later in the piece, we'll discuss tools that help you with evidence collection.

4. Implement a testing plan

Another hallmark of a continuous compliance program is defining success and failure in relation to your controls and collected evidence. Good testing is critical to identifying issues and resolving them before they escalate to the point they cause monetary or reputational damage. It is important to define testing parameters for controls and collected evidence so your organization can ascertain whether inbound evidence adheres to stated policies or falls outside them.

5. Create a well-defined project management process

From collecting evidence to reviewing and updating policy, compliance teams have a lot of projects to juggle at once. When there's so much to do, it is all too easy for a few balls to drop. Continuous compliance requires you to have a logical process for keeping track of your work and getting it all done. Thus, you must have a system that makes task assignment and collaboration as seamless as possible.

6. Define a process for keeping up with regulatory changes

Continuous compliance requires diligent maintenance. Going forward, we can expect to see governments -- local, state, federal, and international -- pass more regulations in areas like user privacy, information security, and others. To reduce compliance risks, smart organizations will establish a method for keeping up to date with new laws and regulations and create workflows to make sure their internal control environment is always compliant with external requirement.

Technology

Technology can help your organization put the key processes we outlined above into practice. For example, you need to have a system of record to store all of your compliance data before you can streamline your evidence collection process. People are much more likely to follow established project management processes when they include minimal work. Technology can help ensure that the desired processes are followed and even automate certain manual processes.

To move to a state of continuous compliance you'll need:

1. A place to store all of your compliance data
2. A compliance system of record that's connected to the core business applications and productivity tools you're already using
3. To automate the testing of controls and the collection of evidence, so you can see your compliance posture in real-time
4. A project management system that allows you to easily collaborate with stakeholders in your compliance ecosystem.

Let's take a closer look at each of the technology components that support continuous compliance.

1. Data Storage/System of Record

You are likely familiar with how Customer Relationship Management (CRM) systems work. CRMs provide organizations with the ability to organize their contact data, segment customers, run sales reports, forecast sales and scale up their sales processes. Similar to a CRM system, a compliance management system provides these benefits too.

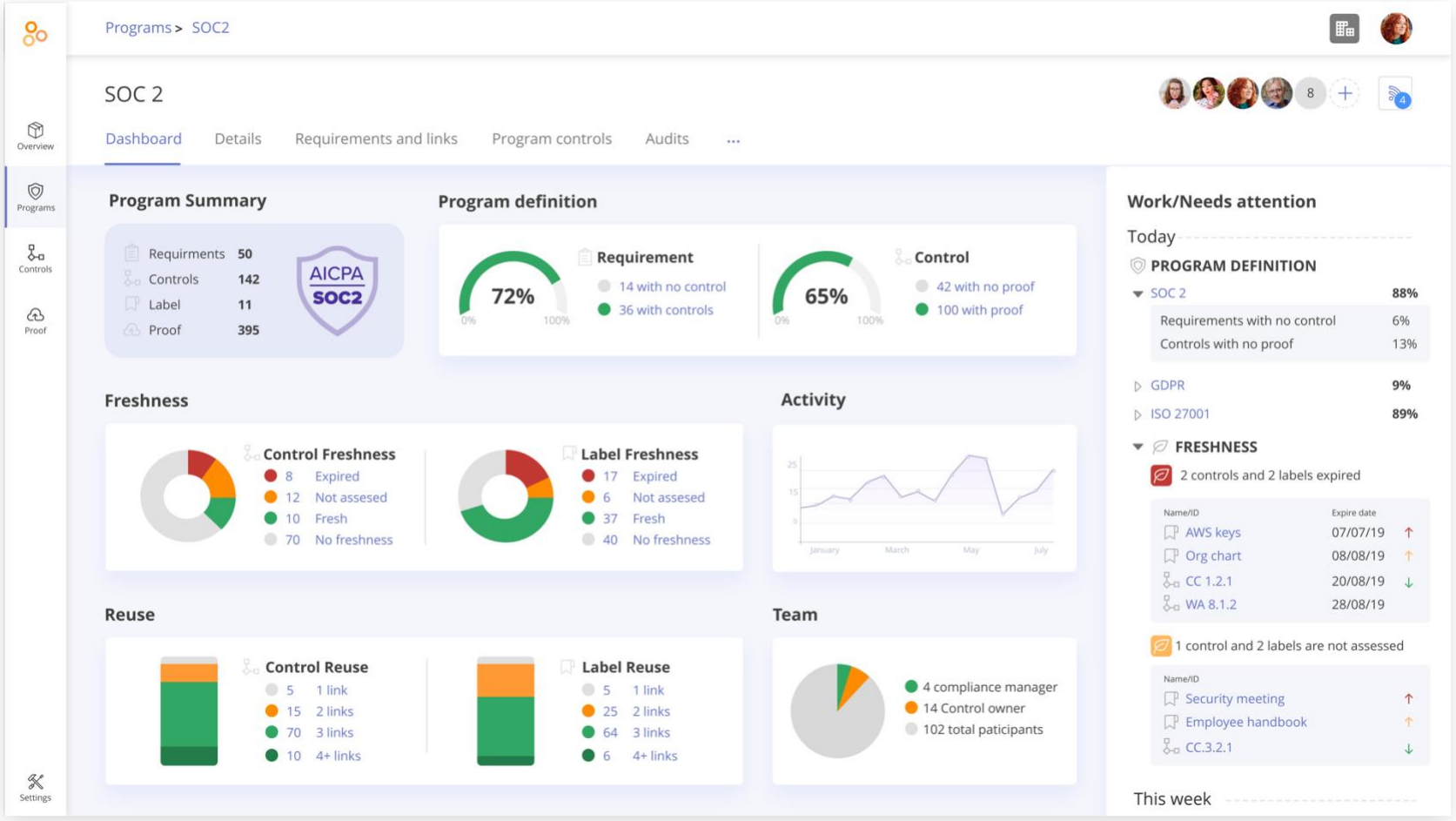
With a compliance system of record, you can easily keep track of all of your compliance data. You'll be able to see whether you have controls, policies, and procedures that satisfy a specific requirement. When you have a centralized and secure digital system of record of all your compliance data, it becomes much easier to assess how your policies, procedures, and controls stack up against relevant standards.

Furthermore, a system of record comes with content on various compliance frameworks (e.g. SOC 2, ISO 27001, GDPR, etc.). The structure of compliance frameworks within the tool makes it easy to translate between frameworks and leverage work done in one framework to meet other compliance requirements.

Another core feature of a CRM is that it provides a logical, flexible data structure for your customer records so that you can run reports to answer any questions you have about the state of sales and customers. Similarly, a compliance system of record can provide you reports on the state of your compliance program in detail and identify the work that still needs to be done. For example, you'll see how many controls are linked to a requirement and understand how close you are to 100% compliance with a given framework. A compliance system of record should give you the ability to highlight those requirements that are not covered by your existing controls, allowing you to focus your resources on those high-priority areas.

Another benefit of a CRM system is its ability to log all interactions your organization has had with each customer account. It creates a record for each event a lead or customer has had with your organization, which helps a

salesperson tailor the way they communicate with each customer. It ensures that when a salesperson or account manager leaves the organization, customer knowledge isn't lost. Similarly, a compliance system of record tracks all the changes you and your team make to your compliance program and saves all previous versions of evidence. It ensures that you won't lose valuable knowledge if and when a key compliance personnel leaves your organization.



Example of a program dashboard from Hyperproof

2. Integrations

Organizations today spend a lot of time on compliance related work because the work is done in disparate systems such as spreadsheets, email, and file stores. If you are tracking regulations in spreadsheets, sending different versions of policies back and forth via email, and storing pieces of compliance evidence in Google Drive, finding everything you need at the time of an audit will be difficult and stressful. On the other hand, if you know whether a control is working or not at all times and have all of the evidence at your fingertips, you can be confident when an audit rolls around. To know your compliance posture in real-time, you need to connect your compliance system of record to the business applications and productivity tools you are using today to manage your compliance program. When the systems are integrated, you can automate the testing of controls, streamline the way you collect evidence and easily collaborate with stakeholders in your compliance ecosystem

3. Automation

Driving down your long-term compliance costs isn't possible without automation. A compliance management system can automate traditionally manual processes such as evidence collection and control monitoring. For example, an integrated compliance management system can automatically extract evidence as needed. In addition, compliance management systems allow you to develop testing parameters that can be automatically run against inbound evidence and notify you of exceptions.

4. Collaboration & Task Management

You'll always have to rely on colleagues in departments like Engineering or IT to keep certain controls up-to-date and document the effectiveness of controls under their purview.

A compliance management system gives you the ability to easily collaborate with stakeholders across your compliance ecosystem. The system helps you manage your projects in a way that ensures people always know what's expected of them and what they need to do next. An effective collaboration system needs to provide the means to assign roles for each compliance project and assign tasks and due dates. It should ensure people complete their work by automatically reminding people when something needs to be done; ideally, it will provide a place for the entire project team to have conversations about their work.

When you put data storage, integration, automation, and collaboration together, you'll have a system in place that gives you the ability to operate in a mode of continuous compliance.

Fortunately, you do not need to build or buy four separate tools to gain the benefits of these technologies. In fact, compliance management software such as Hyperproof is specifically designed to help organizations mature their compliance management processes and reach a state of continuous compliance.

Hyperproof provides organizations with a system of record for their compliance data and automates the evidence collection and controls testing processes. Hyperproof integrates with many productivity and data storage tools that organizations are already familiar with -- such as Outlook, Slack and Dropbox -- so it's easy for all parties to get the work done. It also comes with project management capability so all parties know what's expected of them and what they need to do next.

Conclusion

When your organization must address a growing list of compliance standards and their hundreds of seemingly unique requirements, operating in a reactive mode doesn't cut it anymore. If you want to eliminate audit fatigue once and for all, it is important to implement a well-defined, scalable process for your compliance projects. When you get everyone on board and implement the continuous compliance playbook, you can dramatically reduce the costs of compliance, reduce your team's workload, and gain confidence that your compliance program is truly effective in mitigating the risks facing your organization.

About Hyperproof

Hyperproof is a cloud-based compliance management solution for organizations of all sizes. We help organizations launch new compliance programs quickly, collect evidence automatically, and manage their rcompliance programs intelligently. To learn more about Hyperproof, visit us at https://hyperproof.io or follow us on LinkedIn.