hyperproof

COMPLIANCE OPERATIONS PLAYBOOK

MINIMIZE THE BURDEN OF IT COMPLIANCE AND IMPROVE YOUR SECURITY POSTURE

2

TABLE OF CONTENTS

3

INTRODUCTION: WHAT IS COMPLIANCE OPERATIONS?

Compliance Operations is a new methodology for managing IT risks and compliance projects. It operates on the understanding that cyber risks can change by the minute, regulatory volatility isn't going away, and zero trust is now the default security (and B2B purchase) model. As such, compliance and security assurance professionals need to apply more rigor and discipline to their day-to-day activities and focus on continuous improvement.

The Compliance Operations methodology provides a way for organizations to manage IT risks in a more disciplined, proactive manner and efficiently prove to their customers that they can keep sensitive customer data safe.

KEY PRINCIPLES OF COMPLIANCE OPERATIONS INCLUDE:

1. Starting with your business objectives and risks
2. Breaking down information silos across the IT risk management process
3. Sharing responsibility for security and compliance
4. Breaking down work into small increments and working iteratively
5. Standardizing IT risk management (including compliance) processes
6. Automating manual, routine tasks within the security assurance function
7. Measuring progress and improving iteratively

CHAPTER 1: WHY IT'S TIME TO EVOLVE YOUR APPROACH TO SECURITY ASSURANCE

Businesses today are highly reliant on third-party technology vendors for many critical business processes. Virtually every business function within an organization --from Finance to HR to Marketing -- has gone through some form of digital transformation in the past ten to 15 years. Take a moment to consider some of the key shifts in the business landscape in the past ten to 15 years and the risks those shifts have introduced into our organizations:

1. In 2006, Amazon decided to start offering IT infrastructure services to businesses in the form of web services -- now known as cloud computing. By the end of 2019, **91% of all businesses were using the cloud.** Worldwide spending on public cloud started the decade (2010s) at **$77 billion**, but is projected to be at $411 billion by end of 2021.

2. While organizations have always depended on third-parties and contractors to some extent, organizations' reliance on third parties skyrocketed in the past 10 years (and organizations became increasingly connected and interdependent). The **Ponemon Institute** found that in 2020, on average, companies share their data with **583 third parties.**

3. Ten years ago, the majority of new technology purchased within an organization was handled centrally by the IT department. Today, the amount of new technology purchases made by business units without IT oversight ("shadow IT") dwarfs technology purchases made by IT departments.

As businesses put more valuable data into the cloud and into third-party SaaS applications, they became more attractive targets for hackers and nation-state actors. Cybersecurity experts have seen a massive increase in the frequency, volume, and variety of cyberattacks over the past decade. Additionally, the trend towards BYOD and the adoption of mass remote work due to COVID-19 has led to a widening of attack surfaces for cybercriminals. In 2020, we saw cyber attackers refine their methods to take advantage of the COVID-19 pandemic and the adoption of new technologies due to COVID-19. **Online crimes reported to the FBI's Internet Crime Complaint Center (IC3)** have nearly quadrupled since the beginning of the COVID-19 pandemic.

After making the shift to mass remote work in 2020, many organizations became highly sensitized to the security and privacy risks posed by remote-work supportive technologies (e.g., teleconferencing systems). Companies have realized that when SaaS providers don't have solid security controls within and around their systems, attackers can penetrate their SaaS providers' IT systems and then use the vendor to launch an attack against them.

As more organizations are gaining a deeper understanding of technology risks posed by their vendors, they've shifted from a "trust and verify" model to a **zero trust** model when dealing with IT vendors. In this context, **"zero trust" means viewing third-party software vendors and business service providers as potential attack vectors—and only trusting a third party with your organization's sensitive information after qualified auditors have had the opportunity to audit the third party's security controls and verify their security and compliance posture.**

One recent example of this shift to a zero trust approach to B2B relationships comes from the Department of Defense. Over the course of a few years, the loss and theft of government data became increasingly costly. In the fall of 2020, the DOD rolled out a new cybersecurity requirement for all DOD contractors and suppliers called the **Cybersecurity Maturity Model Certification (CMMC)**. Instead of accepting companies' self-assessment on security questions as valid, the DOD will only conduct business with contractors who have passed third-party audits for the appropriate CMMC level going forward.

At this time, every information business should assume that prospective customers view their business as potentially dangerous until proven otherwise. Meanwhile, there's the simple truth that as organizations adopt new technology in their quest to innovate, and more work gets done over the internet, the risk of data exposure will continue to grow.

The consequences of poor risk management practices have risen quickly. It's not just about the monetary penalty for a compliance failure. There are a variety of costs including:

- Operational costs, such as lost sales, higher operating costs
- Investigations and litigation costs
- Reputational damage
- Lost customer loyalty
- Lower employee morale and higher turnover

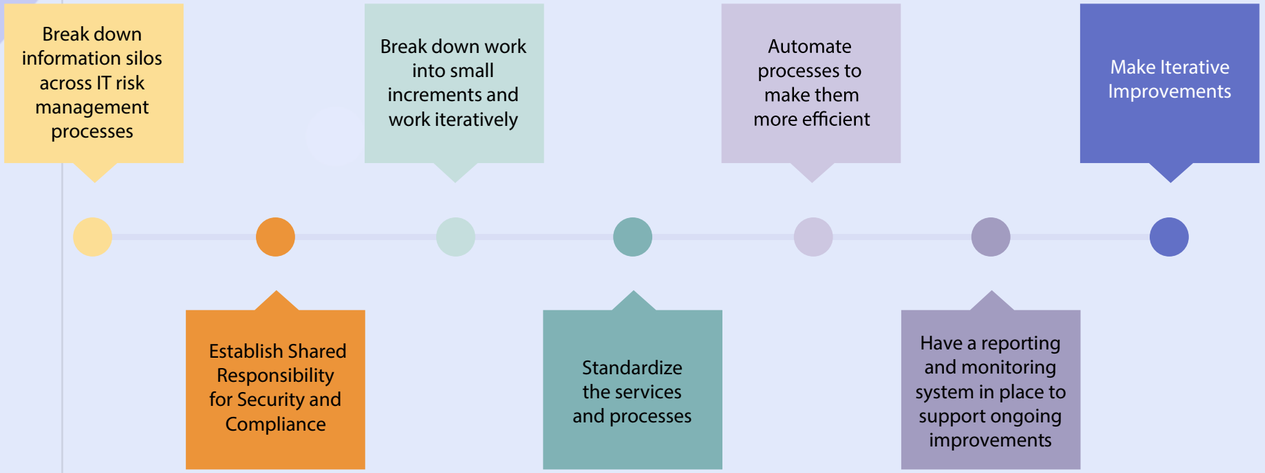
Even though today's risk environment is so dynamic, most organizations don't have a solid approach to managing IT risks yet. According to our **2021 IT Benchmark Survey** (completed by 1,029 IT security assurance/compliance professionals), 65% of global tech companies are still managing IT risks in an ad-hoc way, with siloed teams, processes, and multiple, disconnected tools. Close to **70% of surveyed** IT security assurance professionals do not have a monitoring system to check whether controls designed around their organization's specific risks are operating properly or not.

Because organizations are using multiple, disparate tools throughout their risk management process, collecting critical risk and compliance information is both tedious and difficult. As such, organizations often have a limited understanding of how well existing risks are managed and limited capacity to detect when a safeguard meant to mitigate a risk has failed or hasn't been implemented effectively.

All of this ultimately results in unwanted risk exposure: 61% of all survey respondents surveyed by Hyperproof said they have experienced a data breach or privacy violation in the last three years.

With these factors in mind, organizations today need to take a risk-oriented approach and get better at operationalizing their security assurance and compliance activities. The compliance operations methodology allows you to do both at the same time.

CHAPTER 2: WHAT ARE THE KEY COMPLIANCE OPERATIONS PRINCIPLES?



1. STARTING WITH BUSINESS OBJECTIVES AND RISKS

Cybersecurity is a moving target, so focusing your cybersecurity program on regulatory compliance is no longer sufficient. Meeting those requirements and gaining certain compliance certifications will always be a crucial part of cybersecurity -- but only one part. IT compliance teams have an opportunity to reorient their cybersecurity programs away from a focus on compliance, towards a focus on risk. The security program then becomes more of a strategic advantage for the business.

To adopt a risk-focused approach to cybersecurity, security and IT compliance leaders need to understand the organization's strategic objectives. While compliance will always be one of the objectives, other objectives deserving consideration include:

- **Financial:** How much revenue and profit does the firm want to achieve, and how quickly? What costs is the organization willing to accept or trying to control?
- **Growth:** How is the organization trying to grow: organically, or through acquisitions? Where, physically, is the organization trying to grow? Keep in mind that growth internationally poses a very different set of risks than growth in your home market. Will that growth depend on any new products or services?
- **Personnel:** How will the organization use employees, contractors, or other third pirates to achieve its goals? For example, will everyone work remotely permanently, or return to the office by 2022? Will the mix of full-time and contract workers change over time.

Once you understand those strategic plans and objectives, you can proceed to the next, more relevant question: How is the organization's technology supposed to support those objectives? For example, moving to cloud computing might help to contain costs and expand the hiring pool for personnel, since the company could allow employees to work from home anywhere. Stronger data analytics might help with market segmentation to develop new products or marketing campaigns.

Understanding how technology supports the organization's strategic objectives then lets you ask the most relevant questions of all:
What are the biggest risks to the use of those technologies?
How do your cybersecurity controls and procedures work to keep those risks in check so that mission-critical processes can continue without disruption?

Those two questions above can be the foundation for a risk assessment that considers all the security risks the organization faces. Compliance doesn't fade in importance; instead, it becomes one of numerous concerns you need to address.

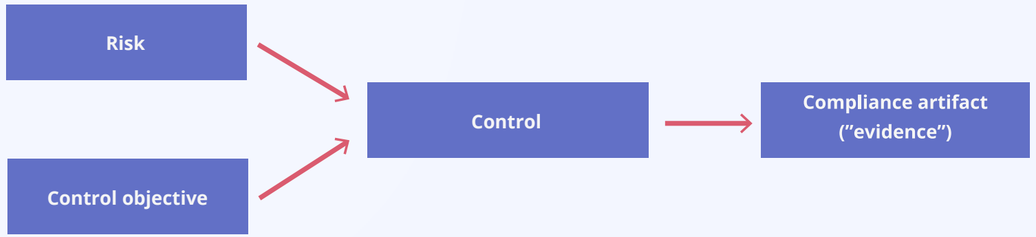
2. BREAKING DOWN INFORMATION SILOS ACROSS THE IT RISK MANAGEMENT PROCESS

To manage IT risks well, security assurance and IT compliance professionals need to safeguard their company's IT assets so that employees can use those assets to pursue the organization's goals -- that's IT governance. The capabilities that are important for IT governance include:

- Data security and data mapping
- Your ability to monitor network activity
- Provisioning and deprovisioning user access
- Security assessments for SaaS vendors your enterprise uses

Today, most security and compliance professionals don't have sufficient visibility into whether all of the work of IT governance (the capabilities we mentioned above) is being performed consistently. That is, compliance officers don't know whether the provisioning and de-provisioning of user access controls happen in a timely manner. They can't tell whether data mapping is up-to-date or whether key SaaS providers in their enterprise have had security assessments completed.

Why is this visibility missing? Because organizations often use disparate tools (e.g., spreadsheets, Sharepoint, G-drive, email, Jira) for different parts of the IT risk management process and information is spread all over the place. Connecting disparate information silos -- so risks, security requirements and the state of the existing internal controls (IT governance activities) are well understood -- is a critical step to take if your organization wants to manage IT risks better.



This mapping process may seem simple, but it can't be implemented effectively unless you have a platform that houses all of your risk information, controls, and compliance artifacts.

3. ESTABLISH SHARED RESPONSIBILITY FOR SECURITY AND COMPLIANCE

If an organization wants to be continuously secure, their information security compliance teams and business stakeholders need to share responsibility for maintaining security and compliance. This is a departure from what we see today, where many business process owners/stakeholders view compliance as something that happens off to the side.

Business process owners from HR, Finance, Engineering, and IT are operating technology and technology-enabled processes that can affect data security, integrity, and privacy. They purchase new technology in order to improve their own productivity and to deliver better customer experiences. When new technology is purchased (or when a new business process is created), new risks to information may be introduced. It's important for the infosec compliance team to understand their business, why these business processes exist, what tools are used in these business processes, and why things are done a certain way -- so they can understand the security and compliance implications.

Compliance and business stakeholders (and product engineers) should work together to ensure that IT systems are configured and used in ways that advance business objectives and adhere to internal security and regulatory standards. It's important that the compliance team knows when business process and technology changes happen.

The compliance team should document what the "proper" processes are so that what's happening can be reviewed against the established standard. They should make this information available to the business process owners -- who are ultimately responsible for following the proper protocols and procedures.

This shared responsibility model can only be enforced when an organization has a platform that makes compliance activities transparent. With a compliance operations platform, a company can document all of their controls (or IT governance and security processes) and store evidence of activities around those controls in a single repository. Compliance teams will be able to see when a control process deviates from what's deemed acceptable and follow-up with control operators to address the issue.

4. BREAK DOWN WORK INTO SMALL INCREMENTS AND WORK ITERATIVELY

Compliance work can feel really intimidating if you think about everything that needs to be done all at once. But if you take an incremental approach, the work becomes much more manageable. A pragmatic approach is one that starts understanding what matters most to the business. For instance, what are the most critical risks within your business that need to be mitigated? Which risks need better mitigation controls? What's the next audit that's coming up? Is there a new security regulation or standard your business has to become compliant with in the coming months in order to do business with certain customer segments?

Knowing your current state and your business priorities, you can start to set realistic, achievable milestones and identify the most important set of tasks that need to be completed in the near term.

If you take a disciplined approach to setting incremental goals in service of improving your security and compliance posture over time, it becomes much easier to figure out the workloads and resources required to meet your objectives and allocate tasks to individuals within, and outside of, the security and compliance function.

Rather than reacting to the demands from other stakeholders, you choose to look ahead and figure out who needs to do what, and by when. For instance, what's the cadence for internal and external audit activities? When do controls need to be implemented, reviewed, and tested? Who's responsible for critical tasks and how do we monitor that? And finally, how can we quickly see if there's a potential issue, like a control not being tested on schedule or if we failed to remediate a key finding?

9

5. STANDARDIZE THE SERVICES AND PROCESSES

To mitigate risks consistently, the security compliance function needs to have clearly defined processes, roles and responsibilities and create a metrics-driven view of these key functions.

Start by defining a process for collecting and reviewing evidence.

If you don't have access to up-to-date evidence, you can't assess whether controls you've implemented are functioning properly or not, which may leave a key IT system exposed. Additionally, in order to pass an independent audit, you'll need to supply your auditors with the correct compliance artifacts. Lastly, collecting evidence tends to be so tedious and time-consuming that it holds security assurance professionals back from tackling more strategic tasks. Hyperproof's 2021 **IT Compliance Benchmark Survey** found that half of the IT security compliance professionals surveyed spend 50% or more of their total time at work on repetitive administrative tasks around preparing for audits.

By having a clearly defined process for collecting and reviewing evidence and a tool that supports a streamlined process, you can save a significant amount of time, money, and frustration and minimize the risk of control failures.

"1 in 2 IT complaince professionals spend 50% or more of their time at work on low-level, administrative tasks."

Hyperproof's 2021 IT Compliance Benchmark Survey

When defining your evidence collection process, it's important to consider the following:

- Evidence should be mapped to controls
- What types of evidence are needed to test whether this control is functional?
- What's the appropriate frequency for collecting that evidence?
- How long do I consider the evidence to be "fresh" or valid?
- What IT/business system does the evidence reside in?
- Who is responsible for submitting the evidence?
- Who needs to review that evidence?

By keeping all this contextual information alongside each piece of evidence in a system of record, you can easily reference this information for future audits -- saving time and money.

6. AUTOMATE MANUAL, ROUTINE TASKS WITHIN THE SECURITY ASSURANCE FUNCTION

When security compliance teams spend much of their time on manual repetitive tasks, they're left with little time to focus on other important tasks aimed at improving security and resiliency (e.g., testing controls on high risk areas, talking to business units to understand what's changing in the business and how those changes may create new risks or amplify existing risks). **Manual, repetitive tasks, such as evidence collection, controls testing, controls monitoring, and reporting, should be automated.**

Further, at the controls level, it's easy to become "over-controlled" as compliance professionals try to meet different but somewhat similar framework requirements. This issue has driven the move towards **unified controls frameworks**. Automation and good processes can help us get there and remain there in light of new or changing requirements.

7. MEASURE PROGRESS AND IMPROVE ITERATIVELY

As your organization grows, you'll face new compliance requirements and new risks that need to be mitigated. It's important to look at your compliance program as a living entity and make incremental improvements on a continuous basis. Controls can quickly become obsolete when a change occurs in an organization, such as when an existing IT system is retired and a new one is implemented.

To achieve continuous compliance, every organization needs to have a reporting and monitoring system that provides real-time insights into the status of internal controls, risks, audits, and automatic flagging of issues that need attention. For instance, one report should help you identify which controls need review because evidence isn't fresh anymore. You should have an easy way to see which security objectives aren't met yet because controls haven't been implemented or tested. There should be a way to track issues and tasks so that involved in compliance know what they need to do next.

Additional resource on communicating about your security program:

What CISOs Should Tell their Boards About Cybersecurity ›

11

ADVANTAGES OF TAKING AN OPERATIONAL APPROACH TO COMPLIANCE ACTIVITIES

The advantages of using this new operational approach compared to a traditional compliance-oriented approach (e.g., rushing to check controls, collect evidence, and fix controls right before an audit) are three-fold:

- First, by reviewing things and making improvements on a cadence, you effectively minimize the chances of experiencing security and compliance lapses
- When your team can easily collect evidence on an ongoing basis, no one needs to scramble or go into fire-drill mode right before an audit. This helps to lower stress levels.
- When the security compliance team keeps track of all of their work in a single compliance operations platform, it becomes easy to prove to customers, auditors, and regulators that your organization has been operating in a secure and compliant way all along. When your organization is good at demonstrating your security posture, you win and retain more business.

CHAPTER 3: THE KEY CAPABILITIES OF A COMPLIANCE OPERATIONS PLATFORM

While it might be possible to bring discipline and rigor to these processes using the same tools we use now, it will be close to impossible to keep it that way. This is intuitive when you look at how various business functions are operating today. Sales teams have Salesforce. HR has Workday. Engineering has a variety of DevOp tools to efficiently execute their work. It's time security assurance and compliance teams got their own platform for managing daily compliance operations -- a place for making project plans, getting work done, tracking progress, and identifying areas for improvement.

Hyperproof's compliance operations platform was built with these key principles of good operations in mind. Hyperproof is your assistant in creating a highly effective Compliance Operations function; it improves the way you plan information security, data privacy, and compliance projects, execute them and monitor progress and keep records:

- **Record-Keeping:** Hyperproof serves as the single source of truth for all of your risks and compliance activities. Hyperproof can be where you house all infosec compliance requirements and standard frameworks (e.g. SOC 2, ISO 27001, PCI, etc.), controls and evidence. Evidence retrieval is easy with Hyperproof, and your organization will be well-prepared for a spot audit at any time. If you choose, you can also use Hyperproof to keep track of your risks. Risks can be mapped back to existing controls -- allowing you to understand how well existing risks are managed.

- **Planning:** You can use Hyperproof to determine your scope of work and what needs to be done to meet compliance frameworks' requirements (e.g., what controls need to be created), identify owners and contributors to the work, create timelines, and assign tasks. Equally important, Hyperproof will help you identify existing controls you can leverage to meet requirements for new compliance frameworks.

- **Workflow optimization and automation:** Cut the time your team spends on manual tasks by up to 70 percent, and free up time to work on the most impactful activities. With Hyperproof, you can improve productivity by automating manual tasks (e.g., collecting evidence, reminding people to review controls) and remove friction points from collaborative workflows.

- **Reporting and monitoring:** Hyperproof makes it easy for everyone within your organization to get on the same page about what the current state of your compliance efforts are and where improvements are needed. With real time analytics, your team knows exactly where they should spend their time and energy. Potential problems, such as out-dated controls, are identified early before they metastasize into costly incidents.

- **Scaling:** Hyperproof helps organizations easily scale up their information security compliance programs and manage multiple audits. With Hyperproof, you can map a control to multiple frameworks' requirements and re-use evidence across multiple audits.

By combining the compliance operations key principles with the Hyperproof compliance operations software, you'll bring rigor, consistency and efficiency to your security assurance and compliance program.

CHAPTER 4: HOW TO IMPLEMENT COMPLIANCE OPERATIONS PRINCIPLES WITH HYPERPROOF

Now, here's how you can operationalize these compliance operations principles step by step with Hyperproof.

1. GET EVERYTHING INTO A SINGLE PLACE

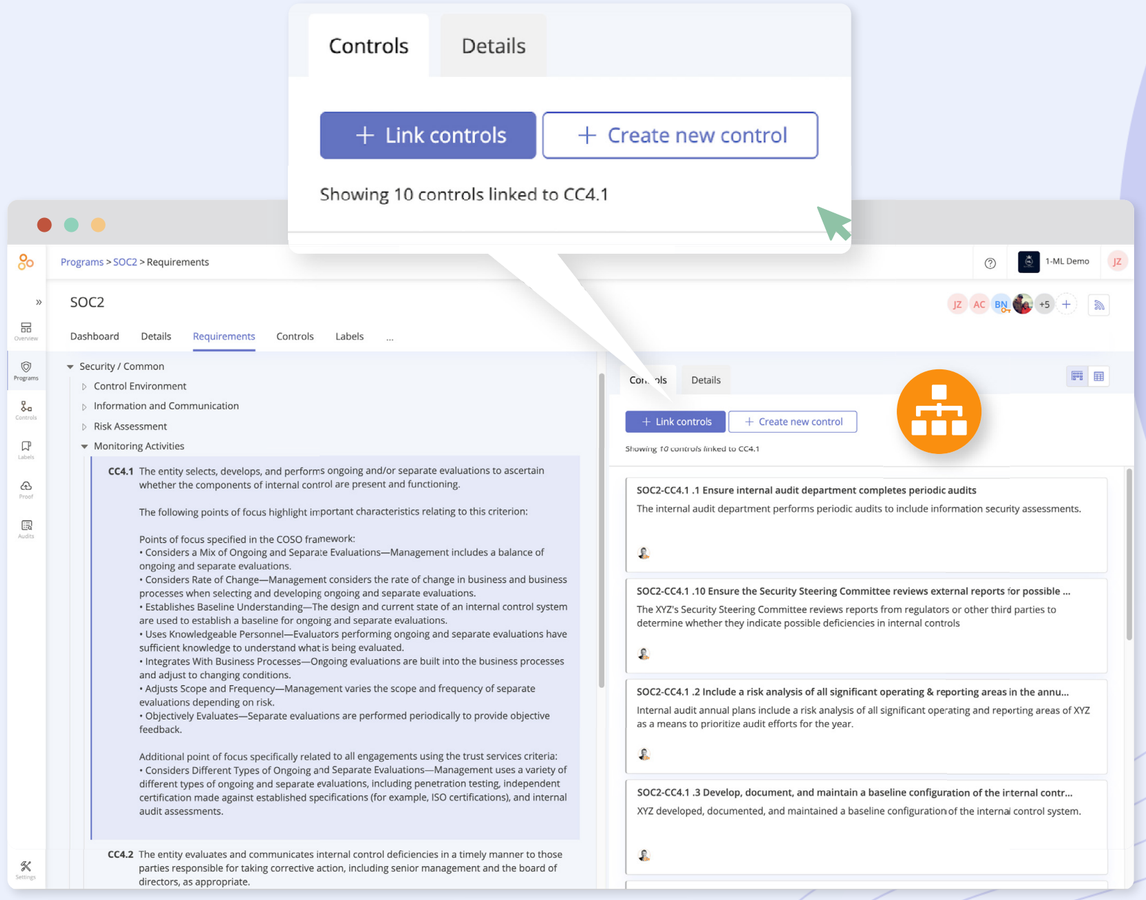
Hyperproof serves as the single source of truth for all of your risks and compliance activities, including documentation of controls, evidence (or compliance artifacts), and records of audits.

Typically, organizations start using Hyperproof by populating an existing framework template. Out of the box, Hyperproof provides requirements and a set of illustrative controls for many of the most commonly used security and privacy frameworks, including NIST-CSF, PCI-DSS, ISO 27001 and many others. These starter controls are linked to program requirements (or security objectives), providing a quick start approach for many organizations. For organizations who already have existing controls in place, it's quite simple to edit the provided controls, add new controls, and remove superfluous ones.

By using Hyperproof, it's easy to keep track of what controls are already implemented and operational, versus which ones are missing - so additional work can be identified and assigned to the responsible parties.

Once you select a specific template, you can immediately start uploading your evidence into the system and link them to the controls.

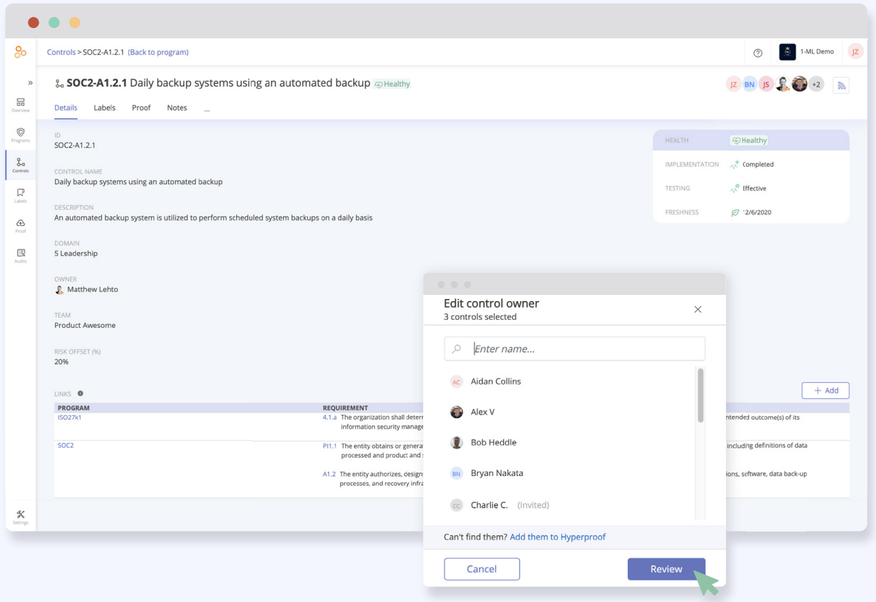
You can also track your risks in Hyperproof in a risk register. Each risk can be mapped back to controls in Hyperproof -- so you can understand how risks are mitigated with existing controls and what the residual risk is.



2. DEFINE THE RESPONSIBLE PARTIES AND THEIR ROLES AND RESPONSIBILITIES

Hyperproof makes it easy to define clear processes, roles, and responsibilities and monitor how key functions are performing, so you're able to avoid compliance slip-ups, control deficiencies, and failing audit results.

Assign control ownership: One of the most common causes of IT system failures and compliance lapses is that companies aren't keeping controls up-to-date. The real problem starts upstream: When no one in the company knows who is responsible for maintaining specific controls. Hyperproof lets you assign controls to individuals or teams and re-assign a control when there's a change in personnel. This visibility into "who is responsible for what" is essential for staying on top of your compliance obligations.



Define cadences for control monitoring: To minimize IT risks, controls need to be critically observed, monitored, and reviewed on an ongoing basis. However, this task is extremely difficult to accomplish if you don't have the appropriate technology that automates the work. In Hyperproof, you can define cadences to review controls and set due dates. Then, the system takes over the job of reminding people to get their work done.

> With Hyperproof, we no longer need to remind ourselves to do specific compliance tasks. The system flags items that are about to expire, helping me keep up with my reviews of controls and evidence.

CARL LOMBARDI
Vice President of Operations, Prime8

15

3. STREAMLINE YOUR EVIDENCE MANAGEMENT WORKFLOWS

With Hyperproof, you can build an organized and highly efficient evidence collection and review process and ensure it stays that way. Here is how our software supports this:

Evidence mapping: Evidence can be quickly uploaded and linked to controls. It's easy to preview evidence in the platform to see.

Keep evidence up-to-date: No one likes bothering their colleagues with multiple requests for the same documents. Yet, this happens all the time within compliance teams. With Hyperproof, you can set up automated reminders to remind teammates to upload new evidence periodically and spend your time on better things.

Re-use evidence across multiple audits and compliance programs:
With Hyperproof serving as a central repository for evidence, you can easily find evidence you'd leveraged for previous audits and identify documents you can re-use. Additionally, with Hyperproof's "Labels" -- containers for storing specific types of compliance artifacts -- you can collect compliance artifacts and tie them to multiple controls. When you upload a new evidence file onto a label, that evidence is automatically reflected across all linked controls.

Automate evidence collection: You can automatically expect evidence from multiple cloud services, apps, and developer tools with **Hypersync** -- our proof collection automation feature. You can also set up automated workflows to remind colleagues to upload new evidence so you can spend your time on higher impact tasks.

> Hyperproof allows me to map one piece of evidence to two or more separate controls and programs, so I don't have to pull the same piece of evidence again and again for each audit. It's also helpful to see the overlap between programs, how one piece of proof can be reused across multiple programs. Across the three audits I am responsible for, I can probably save at least 80 hours.

JOHN THORTON
Information Security Analyst, DigiCert

4. FREE UP TIME BY REDUCING FRICTION POINTS FROM COLLABORATION PROCESSES

In the security assurance and compliance realm, getting work done requires ongoing collaboration between those inside and outside of the security assurance and compliance functions and between those inside and outside of an organization. To operate efficiently, compliance teams need tools in which they can easily assign tasks, track the completion of those tasks, and communicate with stakeholders. It's also important to minimize switching back and forth between multiple tools. If these conditions aren't met, it's all too easy for individuals to drop the ball. With Hyperproof, you can:

Assign tasks and communicate seamlessly:

Hyperproof comes with a native Task Management System, and it works seamlessly with external project management systems such as Jira and Confluence. Compliance managers can create new tasks in Hyperproof and control owners can continue to use their preferred tool of choice to complete the tasks.

You're able to receive notifications about your tasks in several ways, either in Hyperproof or through existing chat tools or via email. If you connect your chat tool (e.g. Slack or Microsoft teams) to Hyperproof, your stakeholders can receive notifications of requests from Hyperproof in those apps, respond to requests directly and those responses will automatically be routed back into Hyperproof.

Start new virtual meetings and store meeting recordings automatically as proof:

Sometimes, to prove that you meet a compliance requirement (or that a control is effective), you need to show that a meeting happened. Hyperproof has made it incredibly easy to collect this particular type of proof: It comes with a native integration to Zoom. You can start a Zoom meeting from any Control in Hyperproof, and the meeting recording will be automatically attached to the control as Proof.

Collaborate with your auditors:

To get ready for an external audit, a compliance manager may spend several days simply pulling together documents for their auditor. With Hyperproof as your compliance operations command center, your auditor can see complete document version history, understand what you've done, and how evidence has changed over time. This reduces the back and forth you'd normally have with your auditor, saving everyone time and money.

17

5. MONITOR, MEASURE, AND ITERATE TO MAINTAIN CONTINUOUS COMPLIANCE

New IT risks can be introduced by internal operational changes or unexpected circumstances. To protect your organization, your security assurance and compliance teams need to understand how internal and external factors introduce new risks, amplify existing risks, and evolve the control environment to keep risks in check.

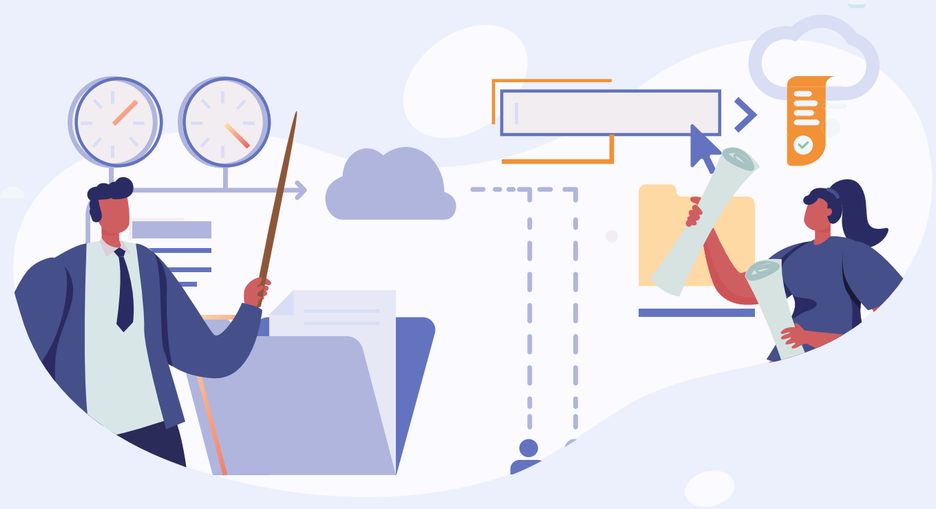
With Hyperproof's dashboards and reports, you can stay on top of risks and your control environment at all times and iteratively evolve and mature your risk management and compliance management practices.

Automate Controls Monitoring: You can define cadences to review controls and set due dates. Hyperproof will automatically alert control owners when they need to provide fresh evidence to verify the efficacy of controls. Control owners are able to define how they want to assess the health of controls; once this is configured, Hyperproof will automatically flag controls that require human attention.

Identify, Assess, and Prioritize Risks: Keeping track of your organization's risks in a central registry is crucial for creating appropriate risk treatment plans. With Hyperproof's intuitive Risk Registry, risk owners from all functions and business units can document their risks and risk treatment plans and organizational leaders can better prioritize risk management activities.

Understand Residual Risk: To ensure that risk managers focus their attention on the right areas, an organization needs to know which risks are most likely to occur and have the highest potential impact. With Hyperproof, once you've documented a risk, you can link a specific control to a risk and determine how much a specific risk has been mitigated by an existing control. With this information, your team can focus their energy on the issues that truly require attention.

Track Risks Over Time: Risks can be exacerbated by new circumstances and controls may become obsolete over time. As such, you need metrics and reports to stay on top of how risks trend over time. With Hyperproof, you can see how your risks change over time and deploy timely responses to keep risks in check.



CHAPTER 5: HOW COMPLIANCE OPERATIONS PLATFORMS DIFFER FROM TRADITIONAL GRC TOOLS

Although GRC tools have existed for over a decade, most have their roots in risk tracking and/or policy management. They weren't built for the tasks today's security assurance and compliance professionals must tackle. This category of software was born at a time when cybersecurity and data privacy regulations were a less onerous burden on information-based businesses than they are now. Fast forward to 2021: it's not unusual for a mid-size organization to have hundreds of business applications and processes that affect the security of information. The number of stakeholders involved in security compliance has risen exponentially. As such, compliance professionals need to collect proof of security controls from many more places and people than they've had to in the past.

Specifically, traditional GRC tools are not meant to help organizations with collecting and managing evidence on a continuous basis -- a highly tedious, yet necessary task for maintaining a solid security posture. Further, they're often not intuitive to use and thus require a lot of training before people are comfortable on the platform.

On the other hand, compliance operations software like Hyperproof is specifically built for today, when protecting information -- and your ability to prove you can protect that information -- has become paramount to business success. Compliance operations software like Hyperproof's purpose is to help security assurance and compliance professionals stay on top of critical risk management activities and manage those activities in the most efficient way. For instance, Hyperproof can help an organization effectively structure their infosec compliance program (e.g., understand similar requirements across multiple frameworks to minimize redundant work), automate evidence collection and management, reduce audit fatigue, and gain real-time visibility into control performance and update controls whenever it's needed.

Implement the Compliance Operations Playbook with Hyperproof

Sign up for a free consultation to learn how you can implement the Compliance Operations playbook with Hyperproof ›

19

ABOUT HYPERPROOF

Hyperproof has built innovative compliance operations software that helps organizations gain the visibility, efficiency, and consistency IT compliance teams need to stay on top of all of their security assurance and compliance work. With Hyperproof, organizations have a single platform for managing daily compliance operations; they can plan their work, make key tasks visible, get work done efficiently, and track progress in real-time. Organizations using Hyperproof are able to cut the time spent on evidence management in half using the platform's intuitive features, automated workflows, and native integrations. Hyperproof also provides a central risk register for organizations to track risks, document risk mitigation plans and map risks to existing controls. Hyperproof is used by fast-growing companies in technology and business and professional services, including Netflix, UIPath, Figma, Nutanix, Qorus, Glance Networks, Prime8 Consulting, and others. For more information about Hyperproof and their products, log on to **Hyperproof.io** or follow Hyperproof on **Twitter** and **LinkedIn**.