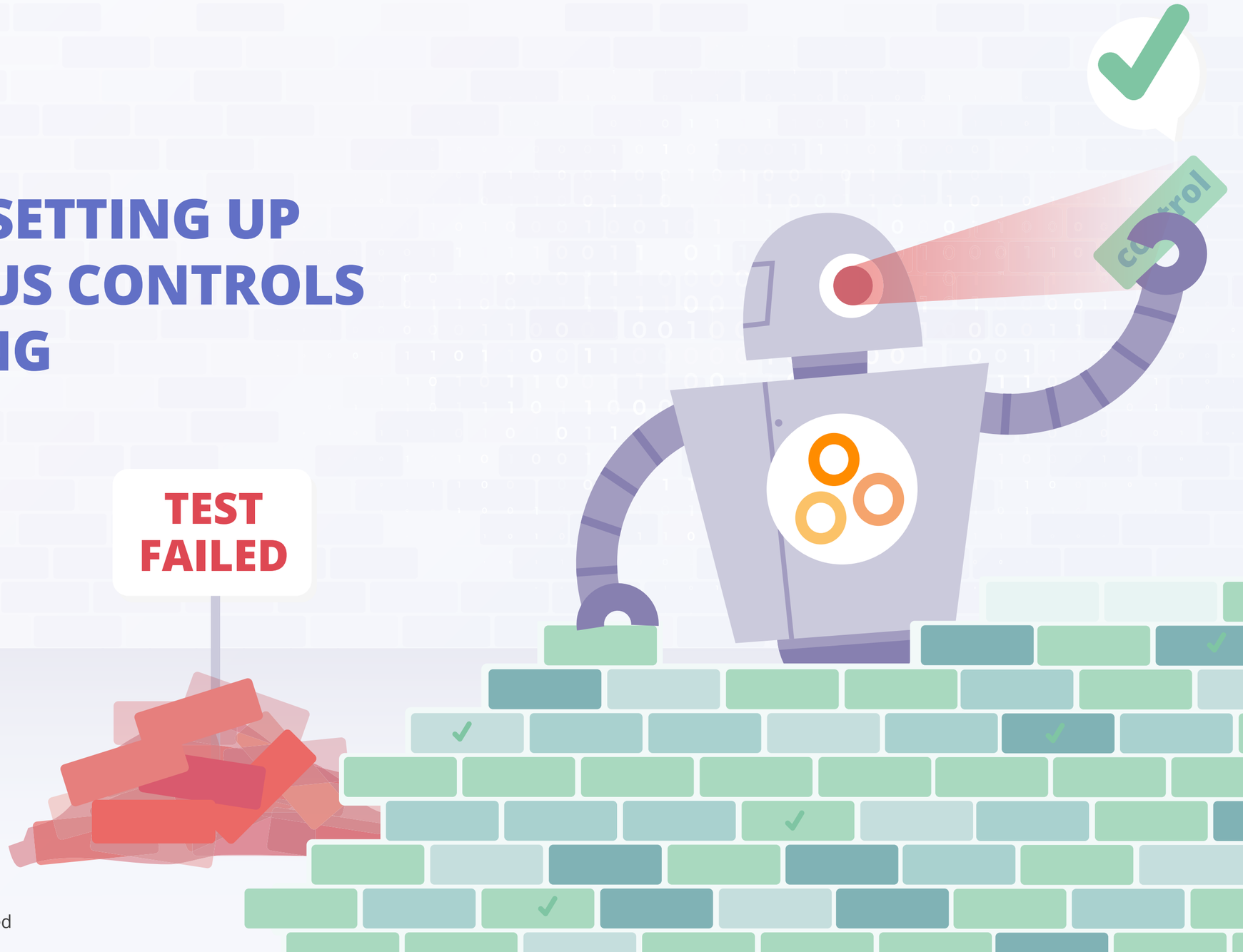
hyperproof

5 STEPS TO SETTING UP CONTINUOUS CONTROLS MONITORING



INTRODUCTION

In today's volatile environment, organizations need to have strong risk management capabilities if they want to maintain strong performance and trust with customers. To effectively manage risk, compliance and internal audit teams need to ensure that internal controls are operating effectively on a continuous basis. Rigorous controls testing is an essential activity for any organization that wants to be highly confident that its critical risks are actively managed.

Yet, control testing becomes increasingly hard to manage as a firm scales up and implements more controls to keep pace with new regulations and an ever-growing tech stack.

Despite their best intentions, compliance professionals often face tight constraints that keep rigorous control testing out of reach. In fact, many compliance and internal audit teams end up testing only the controls being examined in the next external audit.

Taking an ad-hoc approach to controls testing is likely to result in gaps within an organization's control environment, duplicative work, and unexpected expenses. For instance, Hyperproof's 2022 **IT Benchmark Compliance Survey** found that the vast majority of surveyed organizations have holes in their third-party risk management process:

64% **of all respondents reported that they'd been negatively affected by a third-party data breach in 2021.**

Organizations must seek new ways to use technology to increase control testing coverage and to become more productive in their control performance evaluation efforts. Continuous Controls Monitoring (CCM) can go a long way in solving this pervasive challenge.

CCM is defined as applying technology to allow continuous (or at least high-frequency), automated monitoring of controls to validate the effectiveness of controls designed to mitigate risk, including combating cyber attack attempts, and ensuring business continuity and regulatory compliance.

Continuous monitoring of controls is only made possible when control testing can be automated by software. Being able to *automate a control test* means that after initial set up, all activities, including the extraction of relevant data/evidence for testing, initiating the test, generating test results, and triggering follow-up communication based on the test result (e.g., sending a task to a control owner to address a deficiency with a control) are all automatically performed by software.

Deploying CCM not only improves the productivity of compliance and internal audit professionals by decreasing the amount of manual testing they must conduct, but it can yield a range of additional benefits, including:

Keeping business unit stakeholders accountable for managing the risks associated with operating systems and control processes.

We've all heard the saying, "*Security is everyone's job.*" Yet too often, compliance professionals have no consistent way of knowing whether their colleagues in the business units – IT staff, engineers, sales operations managers – are doing their part to protect an organization's assets.

By automating control testing and setting up an alert system based on test results, assurance professionals are able to push compliance and risk management responsibilities to the first line of defense while retaining a mechanism for determining whether control activities have been performed as designed.

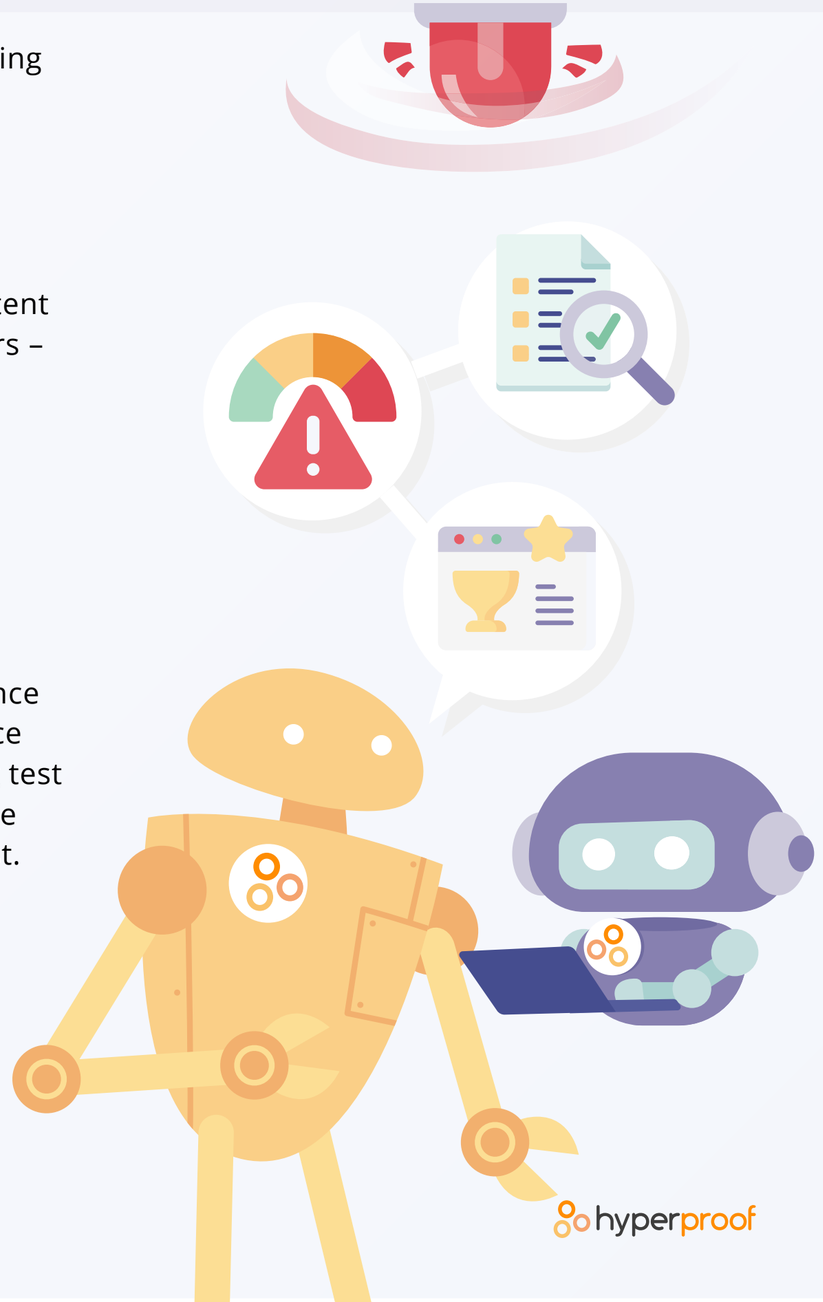
Streamlining audits, thereby reducing audit costs.

When evidence of key control activities are collected automatically according to designated policies, compliance professionals no longer have to scramble to gather evidence and evaluate controls right before an audit. Once CCM is implemented, an external auditor can easily review complete records of control processes – including test results with times and dates linked to the records – all in a central location. This helps to cut down the volume of questions that typically come up during an audit, thereby expediting the process and cutting down the cost.

Improving a company's standing in the eyes of regulators, customers, and auditors.

When an organization has readily available evidence of risk mitigation, protection of valuable assets, and an ability to meet its legal obligations, their reputation benefits. In highly competitive markets, a solid reputation can be the saving grace for a business.

In this ebook, we'll show you how you can implement CCM within your organization in just a few steps.



PREREQUISITES FOR IMPLEMENTING CCM

Implementing CCM in some cases can be as simple as turning on certain settings in the source operating system and using its built-in reports for monitoring. But to have a comprehensive CCM system in place that monitors a wide range of controls across business domains, an organization needs to have a single repository that documents and manages its controls and gathers evidence of controls' effectiveness. This type of system, commonly known as a **compliance operations platform**, is built to test and monitor controls at scale.

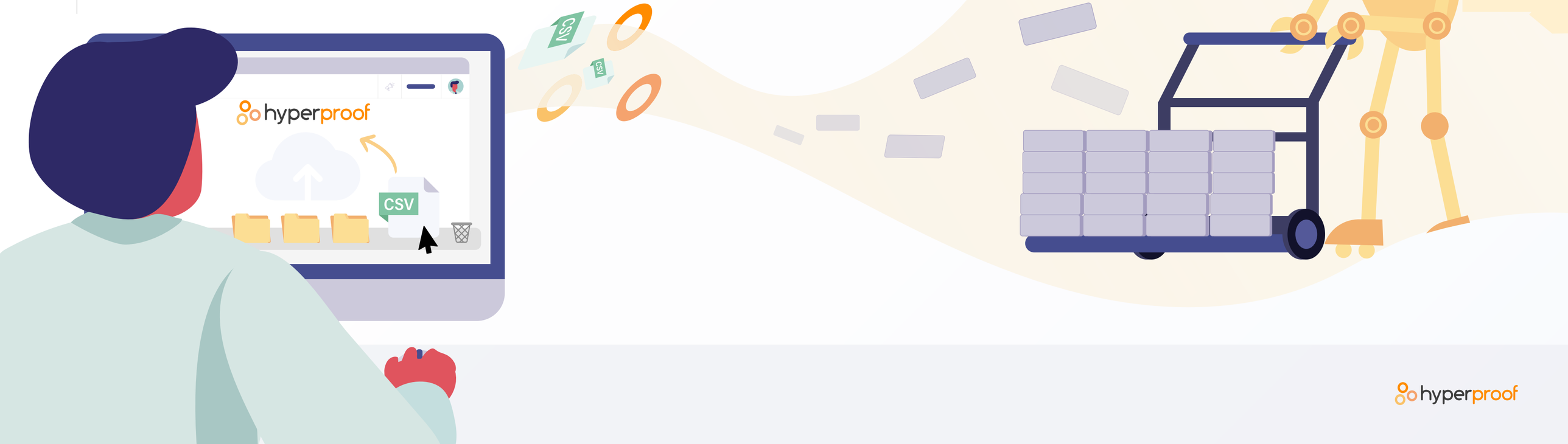
A compliance operations platform has connectors to common business applications across IT, Development, Security, HR, Sales, and Finance, and can automatically pull relevant data about many types of controls into its platform for streamlined controls assessment and validation.

From there, a compliance professional can define tests with pass/fail criteria that run at needed intervals. Compliance operations platforms make it simple to set up automated workflows to manage alarms, communicate, investigate, and correct the control weaknesses.

While building your own CCM system from scratch is an option, it's also quite easy to take advantage of third-party compliance software that comes with CCM out of the box. Regardless of the option you choose, the steps involved in setting up a CCM system are generally the same.

1. IDENTIFY EXISTING CONTROLS

Before you can set up a test, you need to identify the existing controls in your organization and bring them into a central compliance operations platform. Some compliance platforms allow you to upload a CSV with fields about your controls and organize them by traits such as criticality, domain, control, team, and more. Control language, ownership, and other fields can be updated anytime directly in a compliance operations platform.



2. SELECT CONTROLS TO AUTOMATICALLY TEST AND MONITOR

If you're abiding by a security framework such as the NIST Cybersecurity Framework or ISO 27001, you'll already have a number of controls that need to be continuously monitored as part of these programs' requirements.

To the right, we've outlined some common controls that should be continuously validated and monitored because they play an essential role in protecting an organization's network and assets and/or in product security.

These security controls are also good candidates for automated control testing and monitoring because they occur at a high frequency (i.e., continuously, daily, weekly, monthly, etc.) and the source systems often generate well-structured, tabular data for testing.

With a compliance operations platform, evidence of these control activities can be automatically pulled into a central place and normalized for automated testing.

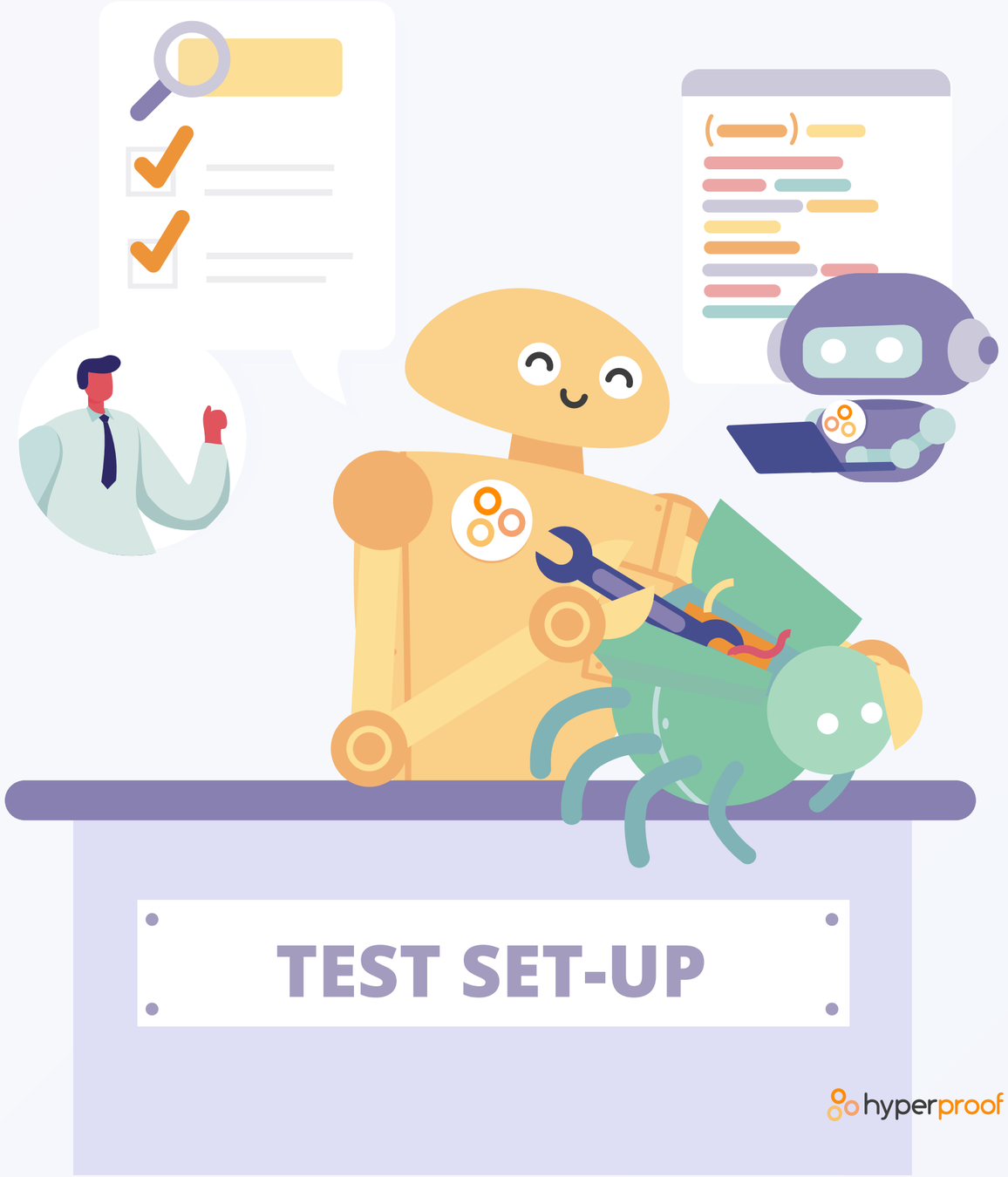
Control type	Common systems
Access control: Ensure that employees and contractors get access to company systems in a controlled manner (e.g., password policies are enforced).	okta, Azure, Google Cloud, salesforce, auth0, aws, Azure Active Directory
Key Monitoring Tools Availability: Ensure that key monitoring tools are running and collecting logs (e.g. check that the firewall is configured correctly). Get reliable access to log files to demonstrate that logging requirements were met.	DATADOG, Cloudflare
Change management: Validate that a designated approval process has occurred before new code is deployed into the production environment.	GitHub, GitLab, Azure DevOps
Vulnerability management: Validate that critical vulnerabilities are fixed in a timely manner, according to the service level agreement (SLA) within our company.	Qualys, tenable
Data encryption/security: Verify that all of a firm's confidential data is restricted to authorized personnel. Make sure that data is transferred in a secure manner.	aws, Azure, Google Cloud
Data integrity: Test that there aren't any data backup failures, or that the number of data backup failures per 100 of backups is below a certain threshold.	aws, Azure, Google Cloud

3. SET UP A TEST FOR EACH CONTROL

Set up a test for each control or a group of related controls at once.

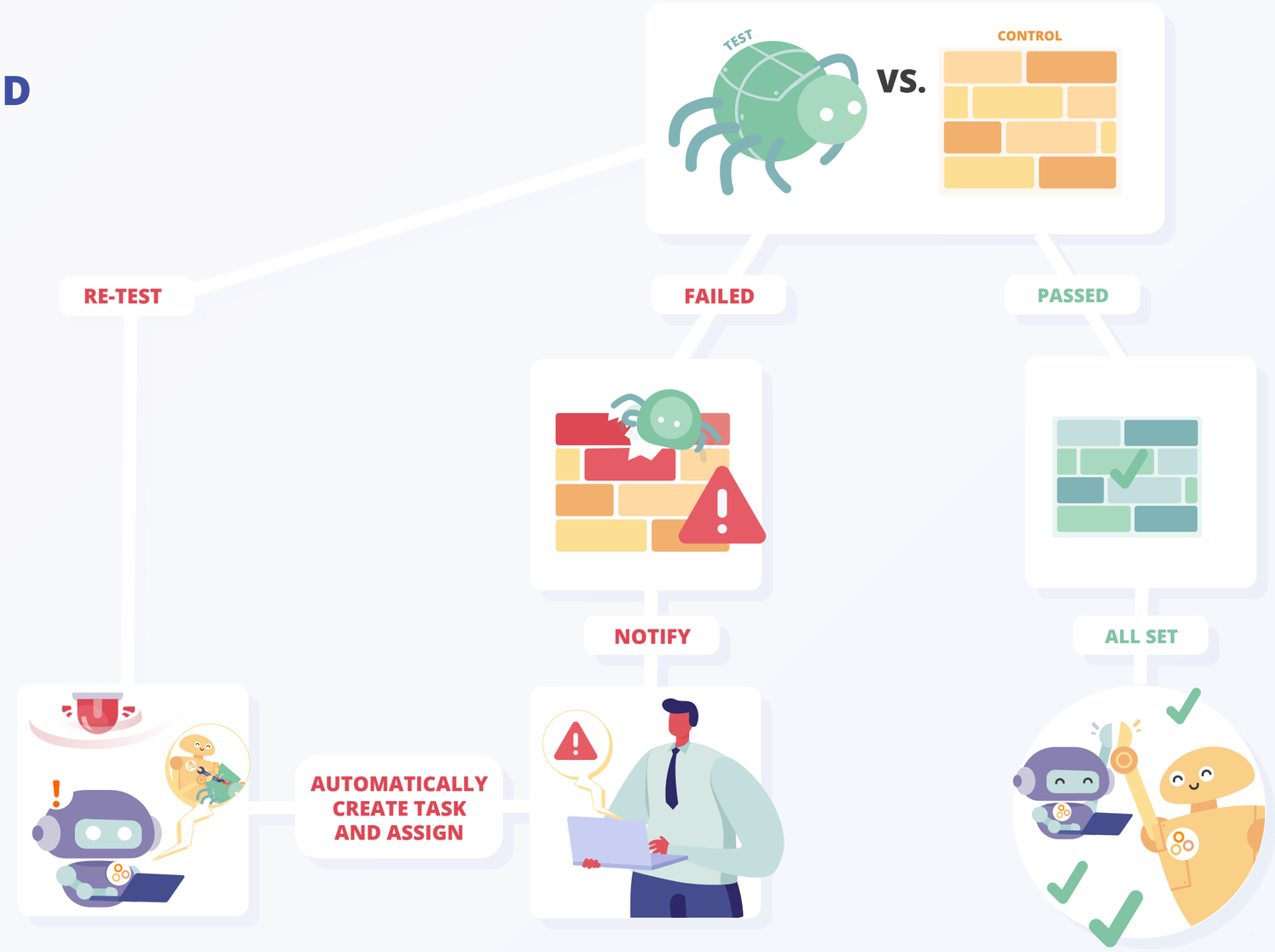
If you choose to use third-party software for automated controls testing, select one that supports many types of tests and is intuitive for non-developers to use. At a minimum, the tool should support multiple types of data, including text strings, numbers, and dates for testing. It should also support common conditions such as Contains, Does Not Contain, and Comparisons (e.g., greater than, less than, equal to, before/on/after/ a certain date). If you can find a test engine that supports Regex, you'll have even more flexibility.

Some Compliance Operations platforms, such as Hyperproof, come with an intuitive and highly flexible test builder that supports many types of tests using simple business logic – similar to the way you'd write functions in Excel (IF(), VLOOKUP(), and HLOOKUP()). Hyperproof also automatically normalizes the data on a user's behalf.



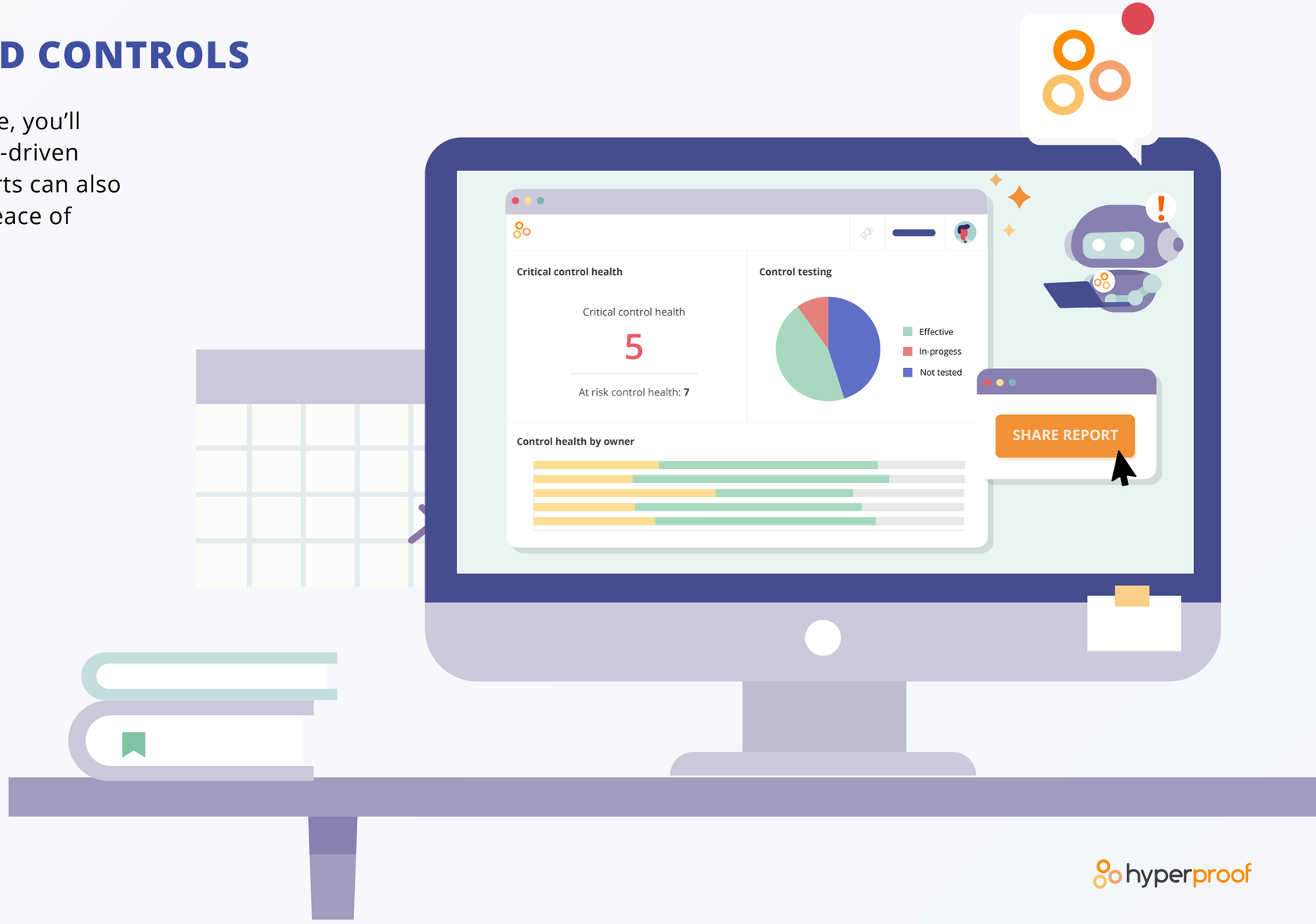
4. DETERMINE WHAT SHOULD HAPPEN IF A TEST FAILS

Once you write a test, determine what type of response is appropriate when a test fails or the result is unexpected. For instance, you may choose to set up an automatic notification and send it to the control operator when the control test fails.



5. BUILD REPORTS FOR EASY MONITORING OF AUTOMATED CONTROLS

By using a report that can be refreshed at any time, you'll be able to easily ensure that control tests and test-driven notifications are working as intended. These reports can also be shared with other stakeholders to give them peace of mind that critical controls are actively managed.



SETTING UP CCM AT ABC, INC.: AN ILLUSTRATIVE EXAMPLE

The Situation

Dani Work is a Senior IT Compliance Manager at ABC Inc., a rapidly growing software company with 600 employees across the United States. At this time, ABC, Inc. sells AI software that supports multiple industry-specific use cases; all of ABC's customers are mid-size and large companies in the private sector. The company has plans to expand its customer base to include more Fortune500 organizations and government agencies in the coming year.

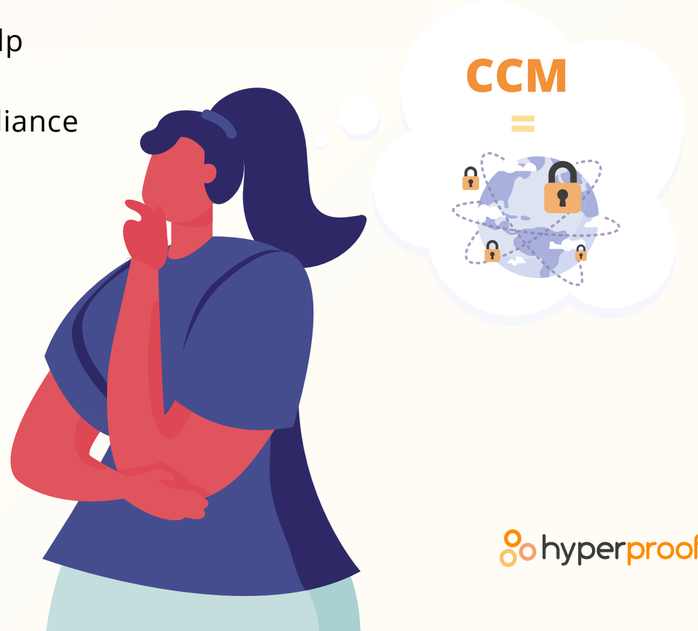
Dani reports to Janet Brown, ABC Inc.'s CISO. Today, ABC Inc. needs to maintain SOC 2 and ISO 27001. Under Janet's direction, Dani has recently started an effort to critically assess ABC's controls against best-in-class frameworks, including the NIST Cybersecurity Framework.

As ABC Inc. adds larger companies and federal agencies to its customer base, and as its own visibility increases in the marketplace, Janet feels strongly that the organization needs to focus more on improving its security and compliance operations. Both Janet and Dani agree that their company needs to do a better job of consistently monitoring and improving their security controls and identifying the imminent threats that are likely already in their environment.

The Challenge

Over the past two years, ABC Inc. grew rapidly across the board. As each department has added new headcounts and purchased new tools (often without the IT team's knowledge), the company's small compliance team is no longer able to stay on top of all controls across the organization. While some teams are good at taking responsibility for maintaining effective controls within their domain, other teams aren't as diligent. In some cases, Dani's team has scant information on which controls are working and which aren't.

Dani believes that CCM can help her team foster a culture of security and continuous compliance – without having to add more headcounts to her team.

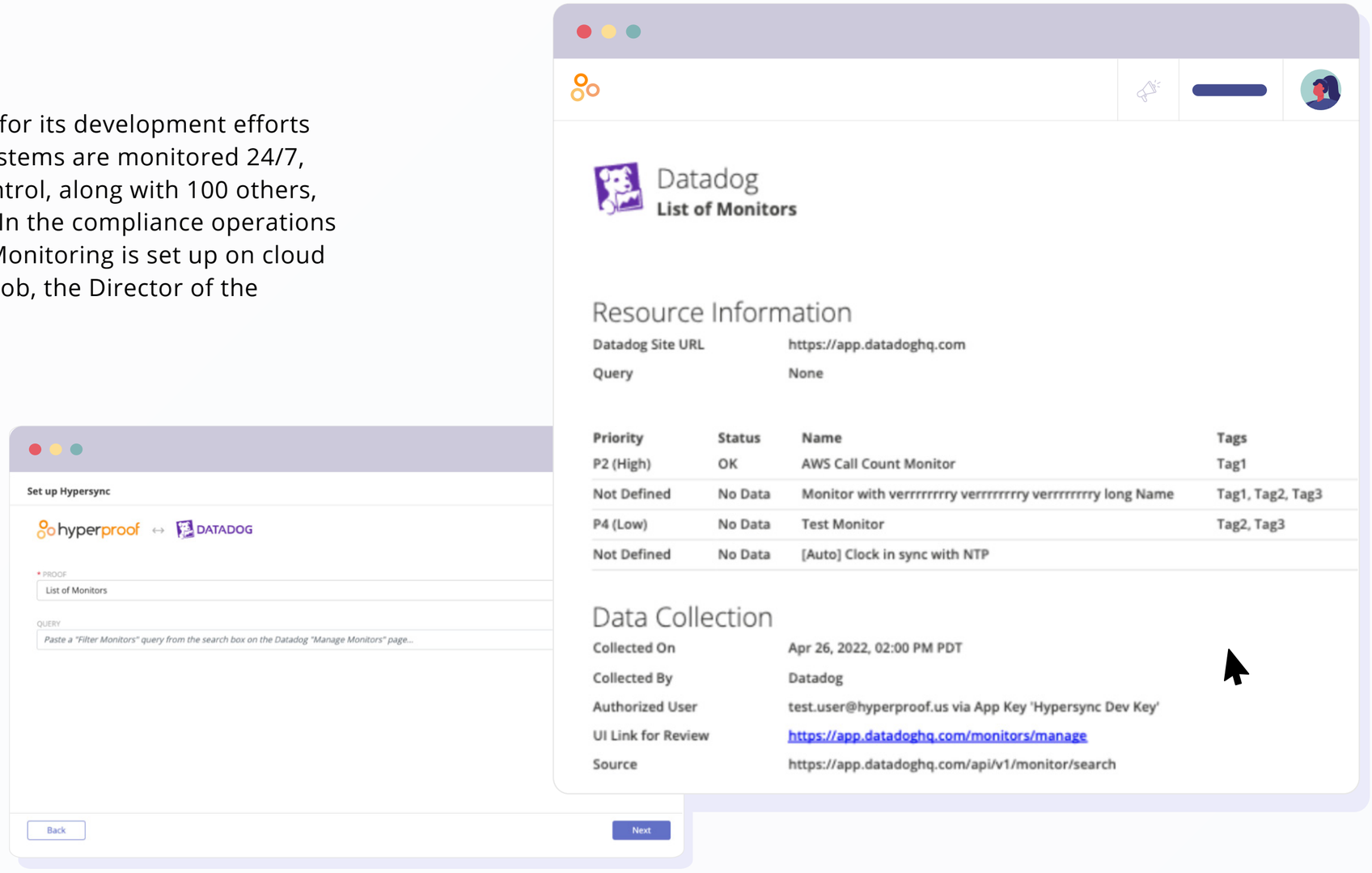


1. Select a control to monitor

In this case, ABC, Inc. uses Microsoft Azure for its development efforts and DataDog to ensure that all of its key systems are monitored 24/7, 365 days a year. Dani has imported this control, along with 100 others, into their compliance operations platform. In the compliance operations platform, Dani set up a control that says, “Monitoring is set up on cloud infrastructure.” The control is assigned to Bob, the Director of the Infrastructure Engineering Team.

The evidence of this control’s effectiveness would come from DataDog, which generates a report called “List of Monitors”.

Dani goes into this particular control and sets up a new automated data collector to have the most current “List of Monitors” report from DataDog pulled into her compliance software on a daily basis.

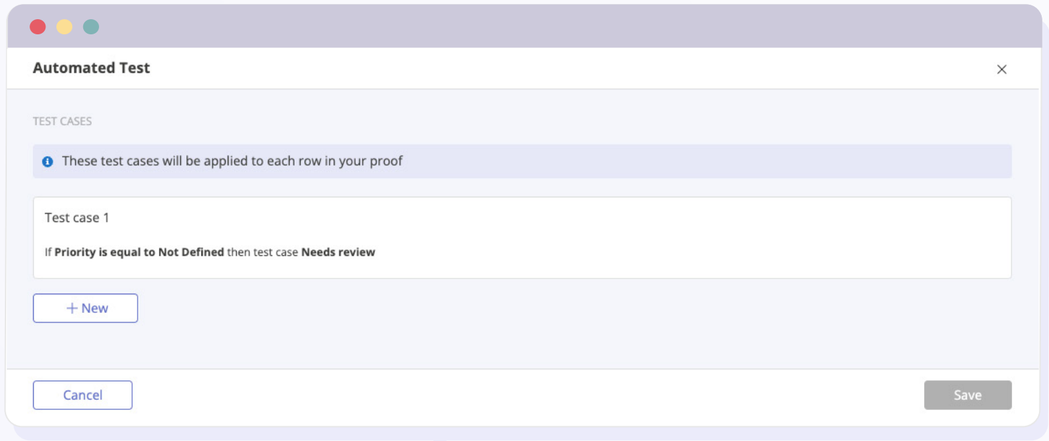


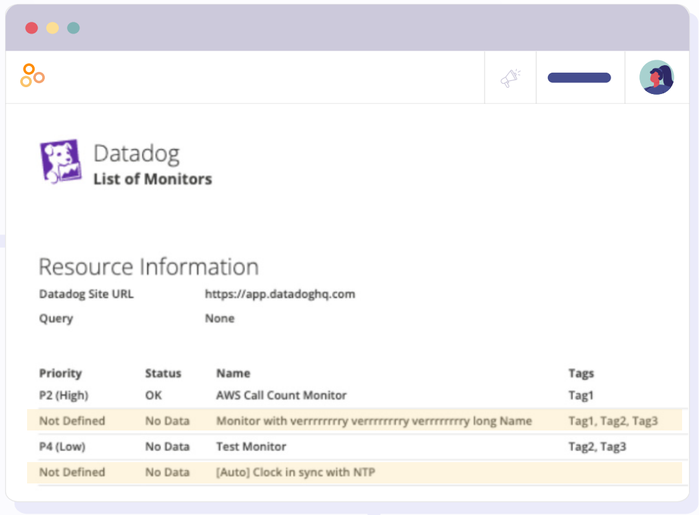
2. Set up a test for the control

Dani wants to ensure that all newly set up monitors have a defined priority. If a new monitor is set up without a defined priority, Dani wants to alert Bob that someone on his team needs to review the monitor and set up a priority for it.

To accomplish this, Dani writes a test in her compliance operations platform that says:

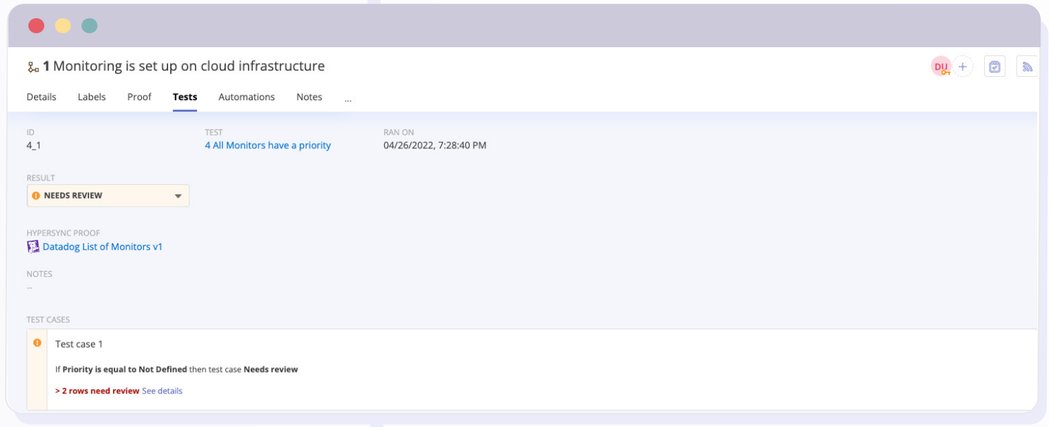
If **Priority is equal to Not Defined** then test case Needs Review





In this case, we can see that there are two monitors without a defined priority (row 2 and row 4).

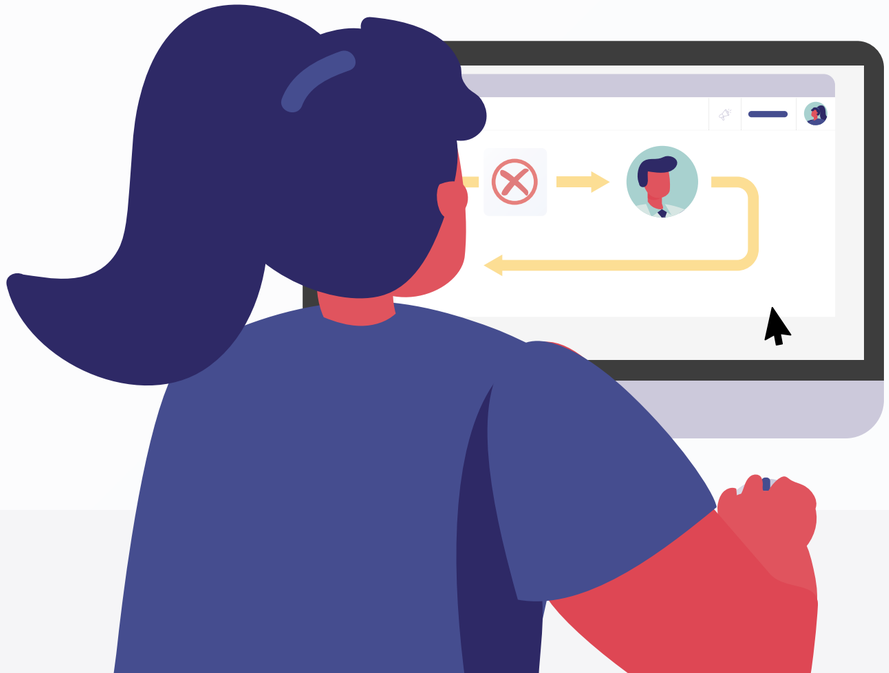
Thus, when the test is run, it will fail.

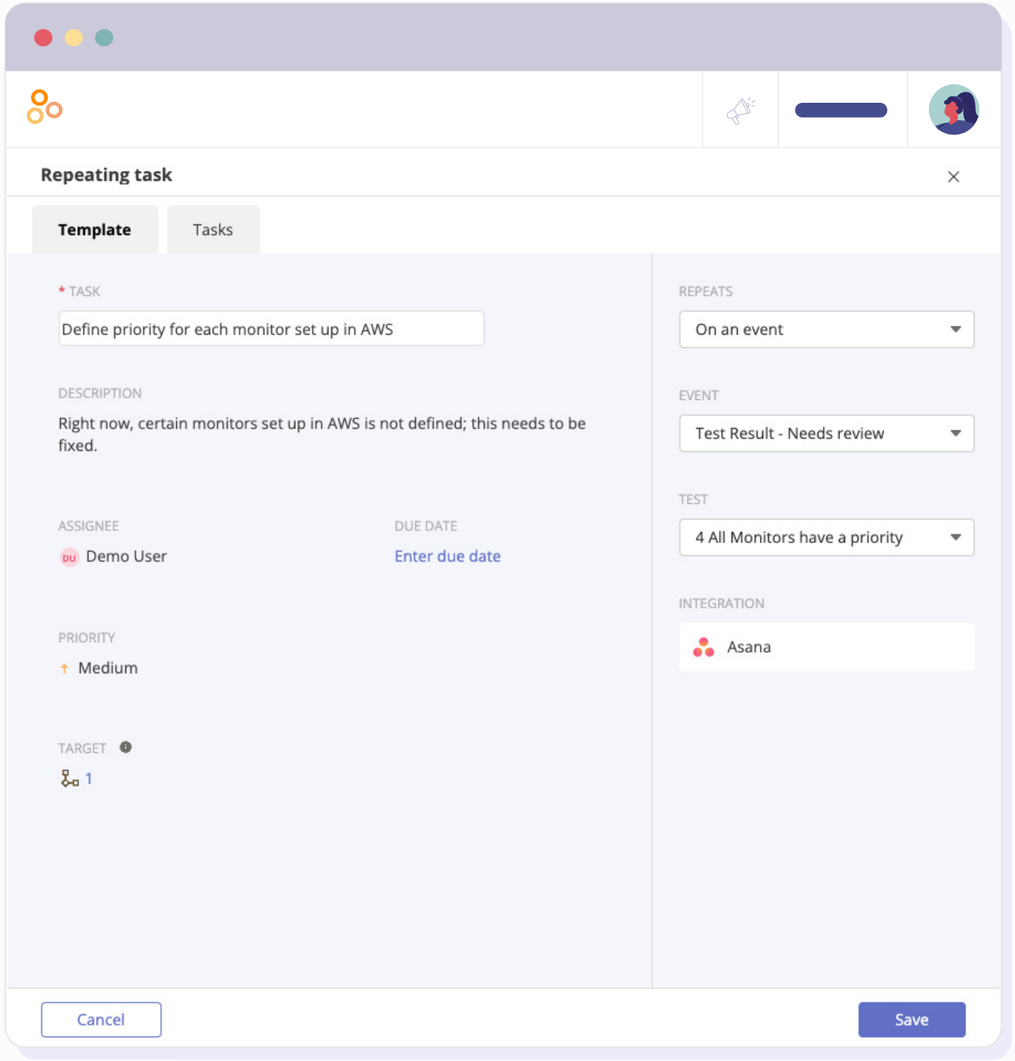


3. Define what should happen next if a test fails

With a compliance operations platform, Dani can simply set up a repeating task that is automatically created and routed to Bob whenever this particular control test fails.

If Bob and all of his team tracks all of their work in Asana, the Repeating Task can be set up to be automatically sent to Asana and turned into a new task. Bob does not need to log into the compliance operations platform.

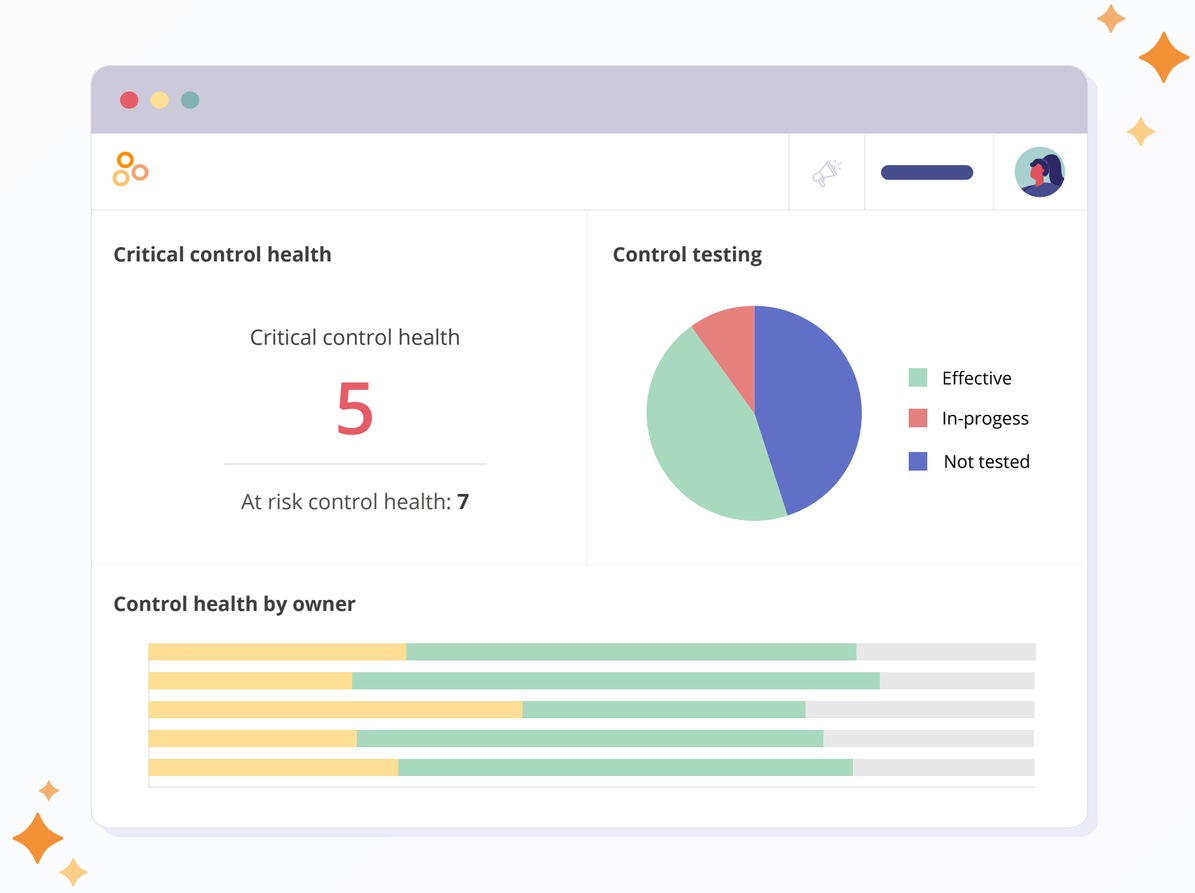




4. Set up a report to track all controls that are automatically monitored

After setting up automated testing on the control illustrated above, Dani identifies additional controls that can benefit from CCM and sets up tests and follow-up actions for each of them. This takes her a week to implement, and she spends another week educating key stakeholders about this process.

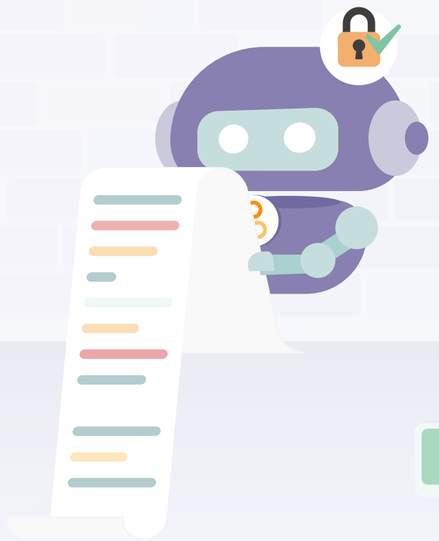
Now, Dani simply turns to the Analytics tab in her compliance operations platform. A new report of all the automated controls, including details on which control tests have passed and failed, is waiting for her. She can look at the controls by teams and domains and see people's progress on remediation tasks. Dani remembers a conversation she had with Janet last week during which Janet asked her about the progress on the CCM implementation project. Dani subscribes Janet to the report, and going forward, Janet will receive this report in her email inbox every Monday morning – without Dani having to do any manual work.

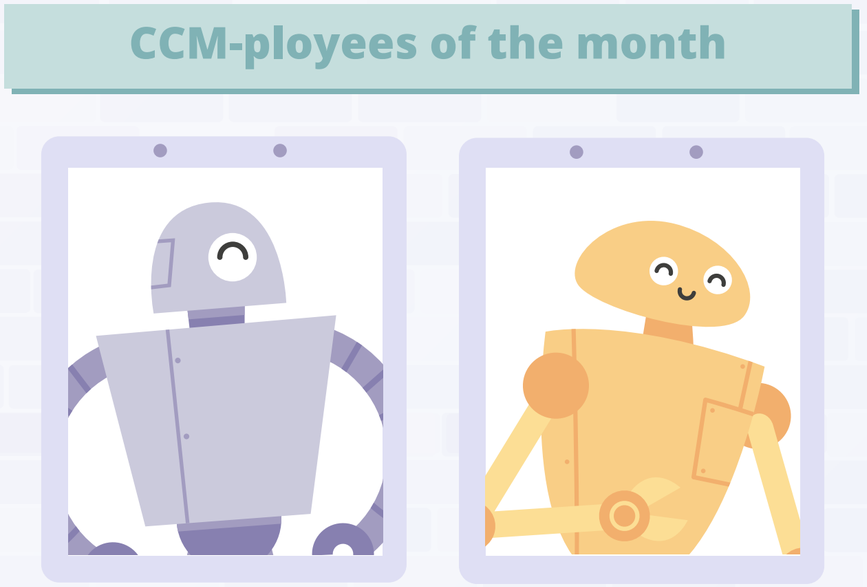


CONCLUSION

All in all, CCM is a key aspect of Governance, Risk and Compliance that can help organizations of all sizes save time and money in their compliance efforts while improving their overall risk management. Now that the GRC software market has evolved to a point where highly intuitive platforms exist, even small organizations with just a single compliance professional on staff can take advantage of CMM to mature their compliance operations.

To see how a compliance operations platform like Hyperproof can help you jumpstart CCM, **request a demo**.





ABOUT HYPERPROOF

Hyperproof is a software company focused on creating revolutionary software that brings trust to life. To date, Hyperproof has delivered an innovative SaaS compliance operations platform that empower compliance, risk and security teams to stay on top of all compliance work and manage organizational risks (including vendor risks) on a continuous basis. Hyperproof has disrupted the GRC space by tackling a pressing problem ignored by others: helping compliance pros gain control over and effectively manage their ever-growing workload. Hyperproof is used by market leaders in security tech, enterprise software, fintech, healthcare tech, and data communications.

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