7 tips to build a continuous control testing program

Optro

Table of contents

The continuous control testing lifecycle

Seven steps to help you incorporate continuous monitoring into your compliance program at any stage.

1. Landscape

Understand your industry landscape.

2. Stakeholders and business

Understand your stakeholders & business.

3. Baseline framework

Baseline against a robust framework.

4. Evaluate risks

Perform the initial assessment.

5. Optimize technology

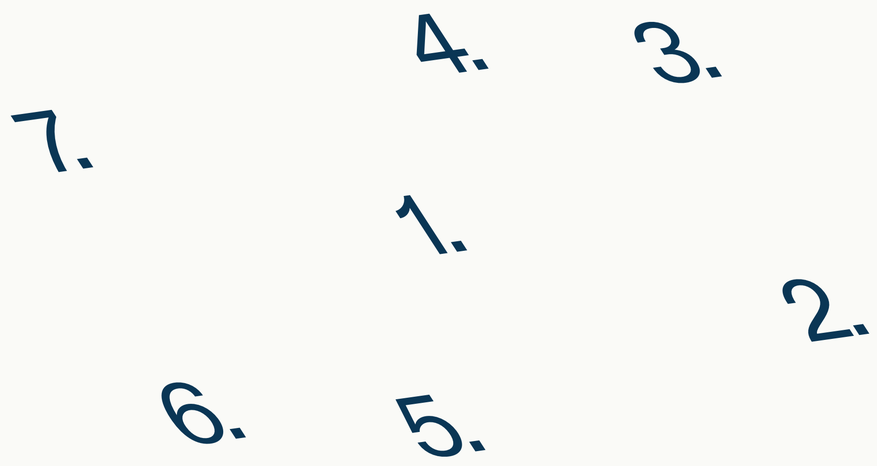
Aquire or optimize technology resources.

6. Track metrics

Track metrics to ensure continued success.

7. Reassess

Reassess as necessary.



As IT compliance teams contend with a proliferation of new cybersecurity controls and complex, multi-framework environments, building efficiency into their internal control programs is becoming increasingly necessary. In a fast-evolving risk and regulatory landscape, compliance programs must be able to respond to new requirements with agility. Yet, despite teams being asked to do more with less every day, they are often insufficiently coordinated, prepared, and aligned — leading to significant delays, friction, and redundant efforts.

Why a continuous approach is necessary

Compliance programs are often conceived and developed with an initial objective in mind, such as complying with an industry standard or achieving a certification to strengthen the business's security posture. However, remaining compliant in periods of change is not easy; expansion of business operations, systems, and locations often **increases the scope of risk and control requirements**. No matter how well-conceived your program is, **ignoring the impact of changes will hinder its growth and scalability as time goes on**.

Instead of viewing compliance in terms of that initial objective, consider what is needed to support your internal control processes from a long-term investment perspective. **A continuous approach to control testing** — anchored in a common control set and automated control tests on a regular cadence (e.g., quarterly or semi-annually) — **can help alleviate resource constraints and enable you to focus on emerging areas and improvements.**

Why technology is critical to continuous control testing

Enlisting the aid of **AI, automation, and other advanced technologies is critical to helping modern compliance teams keep pace with today's expanding control environments.** Simultaneously, technology solutions that support continuous control testing have advanced to meet the growing market need for them.

Evidence has shown that forward-thinking compliance teams **embrace technologies that help them automate repetitive, manual tasks**, including common control tests such as **user access reviews, new user access testing, and terminated user access testing**; evidence collection; and data cleansing and manipulation.

A September 2024 Optro flash poll of over 1,400 IT security and compliance professionals found that **37% of organizations are leveraging AI to automate, enhance, and improve their internal controls.** A November 2024 flash poll of over 900 audit, risk, and compliance leaders revealed that **40% of organizations are using GRC solutions and 15% are employing an integrated risk management solution** to automate and streamline their processes.

By automating common cyber control tests, IT compliance teams can improve their organization's risk posture with minimal strain on resources, aiding their efforts to keep up with rapidly expanding control environments.

7 steps for building a strong foundation

The following seven steps can help lay the foundation for continuous control testing.

1.

Understand your industry landscape.

It's important to start with an in-depth understanding of your industry landscape. What are your industry's applicable legal, regulatory, and compliance requirements? Is your business obtaining certifications to provide assurance to customers and/or reduce cyber liability insurance premiums?

2.

Understand your stakeholders and your business.

What does compliance mean to the individual — and what does it mean to the organization as a whole? Is the culture of compliance in your organization top-down or bottom-up? Conduct interviews with your business process owners to understand how their processes work and what controls already exist to mitigate related risks.

3.

Baseline against a robust framework.

Frameworks like the NIST Cybersecurity Framework, NIST 800-53, and ISO 27001 can help you gain coverage over a wide range of areas. The NIST and ISO frameworks are commonly regarded by the IT security industry as best practice baseline frameworks.

4.

Evaluate/assess the risks.

Evaluate the business risks and quantify your risk exposure. Ask yourself what the impact of the risk itself is. What do you know? What don't you know? What happens if you don't address the risk — reputational damage, fines, loss of customers/business? Utilize industry-standard guidance for risk assessments, such as NIST SP 800-30, NIST CSF, and ISO 31000:2018.

How Optro can help

Optro Analytics helps teams automate common, time-intensive cyber control tests with our pre-built, pre-configured workflows, including User Access Reviews, New User Access Testing, and Terminated Users. In addition to these ready-to-deploy control tests, you can also easily build custom workflows to streamline your cyber control testing efforts. Implementing these automated workflows can help you build a strong foundation for a continuous control testing program that enables proactive risk management and swift remediation of emerging issues.

5.

Acquire or optimize technology resources.

Setting yourself up for success with the right technology is critical to growing and scaling your control testing program. Wherever possible, leverage automation and integrations to enhance the efficiency of your program. For example, using a tool that can collect evidence automatically can save significant time, enabling your team to focus on other important areas.

6.

Track metrics to ensure continued success.

See the list of metrics to track for continuous control testing success on the following page.

7.

Reassess as necessary.

Compliance is a full-time job, and benchmarks will move. It's essential to reassess your control testing program whenever there are business changes to ensure it remains aligned with your compliance needs.

Continuous control testing success metrics

Issue metrics

- Time to identify
- Time to remediate
- Time and expense calculation per issue
- Total number of issues currently open
- Issue aging after assessment
- Number of issues impacting criteria certifications, applicable regulatory requirements, or other issues that could cause severe reputational, financial, or operational damage to an organization

Risks

- Time to identify risks; how much of my compliance program do my risks affect
- Time to mitigation plan implementation
- Time and expense calculation per risk. Dollar cost that can be associated with a risk can help to get the attention of decision-makers
- Risk treatment by category (accepted, mitigated, transferred, monitored)

Compliance assessments

- How long to complete an assessment
- Coverage of assessments (what controls, processes, risks, etc. are reviewed)

Overall compliance

- Compliance status by framework
- Percent compliant with new frameworks

How Optro can help

Optro's automated control testing capabilities reduce the manual effort of common control tests, speed up data collection and validation, and improve accuracy and consistency by minimizing human error and standardizing control assessments.

To learn more, request a personalized walkthrough at Optro.ai.

About the author

Alan Gouveia

Director of Enterprise Customer Success at Optro

Alan has worked in the GRC and cybersecurity space for over 20 years across multiple industries and organizations of different sizes. He specializes in a collaborative approach to GRC and cybersecurity, showing customers how to work across the entire organization to achieve business goals. Connect with Alan on LinkedIn.

About Optro

Optro is the leading AI-powered GRC platform, transforming the way the world's biggest companies manage risk. More than 50% of the Fortune 500 trust Optro to elevate their audit, risk, and compliance management. Optro is top-rated by customers on G2, Capterra, and Gartner Peer Insights, and was recently ranked for the sixth year in a row as one of the fastest-growing technology companies in North America by Deloitte.