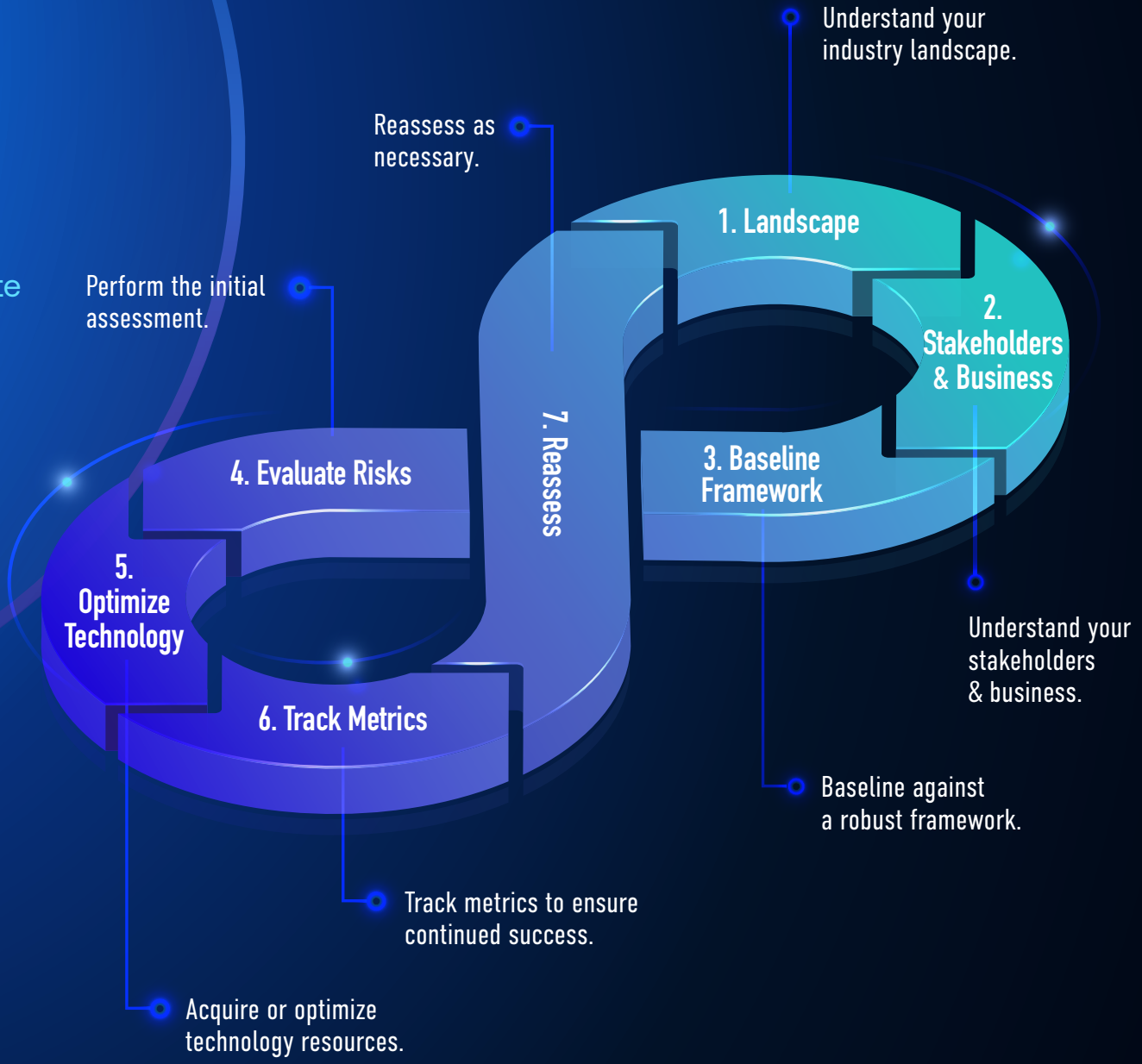
AUDITBOARD

The Continuous Monitoring Lifecycle

7 Steps for Building a Strong Foundation

The Continuous Monitoring Lifecycle

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



The Continuous Monitoring Lifecycle:

7 Steps for Building a Strong Foundation

As the business landscape changes, compliance is becoming increasingly relevant to businesses across all industries. With risks constantly changing and driving new compliance requirements, compliance programs must be able to respond to changes with agility. This highlights the importance of incorporating an approach of **continuous monitoring**.

NIST defines continuous monitoring as: “Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.” A strong continuous monitoring foundation enables an organization to quickly pivot and respond strategically as new compliance requirements come into scope.

Compliance programs are often conceived and developed with short-term goals in mind; for example, complying with an industry standard or achieving a certification. However, compliance is not stagnant; new risks are always coming into scope and the regulatory landscape is fluid. Without scalable policies and procedures in place, no matter how well-conceived your program is, decentralization will ultimately hinder the growth and scalability of your program as time goes on.

Instead of viewing compliance in terms of short-term goals, consider it from the perspective of a long-term investment. The following are seven steps to help you incorporate continuous monitoring into your compliance program at any stage.

7 Steps for Building Continuous Monitoring Into Your Compliance Program

1. **Understand your industry landscape.** It is important to start with a true understanding of your industry landscape. What are the applicable legal, regulatory, and compliance requirements within your industry? Is your business obtaining certifications to provide assurance to customers and/or to 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 is already being done to mitigate the risk.

3. **Baseline against a robust framework.** Frameworks like NIST Cybersecurity Framework, NIST 800-53, and ISO 27001 can help you gain coverage over a wide variety 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?

5. **Acquire or optimize technology resources.** Teams are asked to do more with less everyday and it is impossible to support a program without the use of technology. Simultaneously, compliance solutions have evolved, advanced in sophistication, and are relied upon more and more in the market today. Setting yourself up for success with the right technology is a critical factor in your ability to grow and scale your compliance program.

   - Choose and select technologies that will scale with you and not hinder growth.
   - Have a clear path for the future.
   - Discuss with BoD or relevant internal committees.

6. **Track metrics to ensure continued success.** See our Continuous Monitoring Metrics Checklist below for key metrics to track.

7. **Reassess as necessary.** Compliance is a full-time job and the benchmarks will move. It is important to have a mentality of reassessing your program whenever there are changes to the business in order to ensure your program is keeping up with your business’s compliance needs.

Metrics to Track for Continuous Monitoring Success

Issue Metrics

- ☐ Time to identify
- ☐ Time to remediate
- ☐ Time & Expense calculation per issue
- ☐ Total Number of Issues Currently Open
- ☐ Issue aging after assessment
- ☐ Number of Issues impacting critical 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 & Expense calculation per risk. Dollar cost that can be associated with a risk can help to get 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

While there are many ways to incorporate continuous monitoring into your compliance program, considering continuous monitoring in the early planning stages of your compliance program is an opportunity to lay a strong foundation using metrics, frameworks, and technology.

To learn how CrossComply can help you streamline this process, contact AuditBoard for a personalized product walkthrough today.

About the Author

Michael Condon, CISA, CIA, Certified Blockchain Expert, is a Manager of Compliance Solutions at AuditBoard. He brings over 7 years of experience in the IT Compliance and Cybersecurity industry helping organizations build, maintain, and support their compliance programs.

AuditBoard transforms how audit, risk, and compliance professionals manage today's dynamic risk landscape with a modern, connected platform that engages the front lines, surfaces the risks that matter, and drives better strategic decision-making.