AUDITBOARD

The InfoSec Survival Guide

Achieving Continuous Compliance

Table of Contents

Section 1

Introduction

1.1

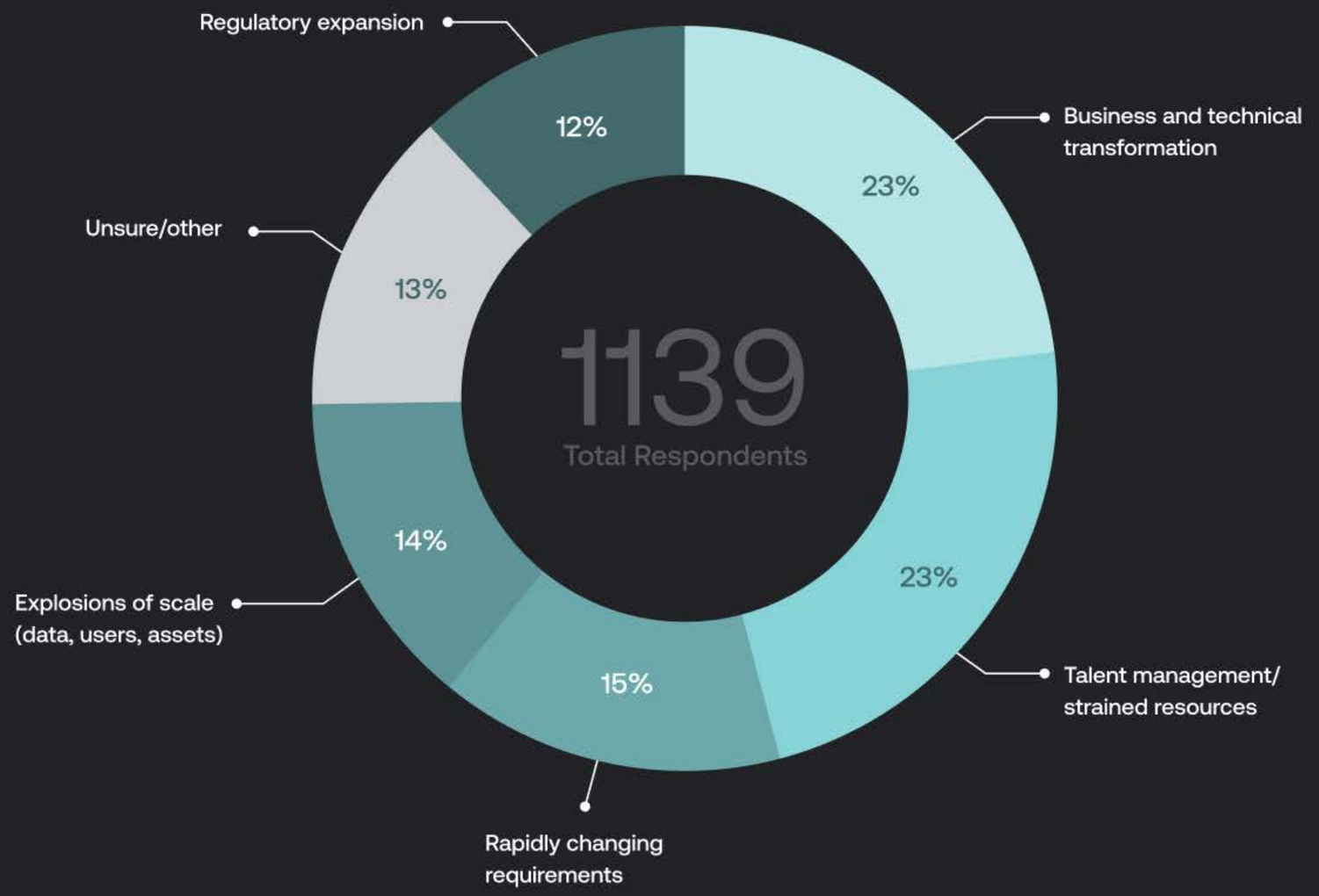
The Benefits of a Continuous Approach to Compliance

Compliance is never as simple as documenting everything once a year, then setting it aside. As long as data continues to be an integral part of societies, the information security risk landscape will continue to be in flux; the only constant is change.

In addition, regulatory oversight continues to expand. The new White House cybersecurity initiatives, latest SEC rules to standardize ESG reporting, and recent updates to the PCI DSS, ISO, and CMMC frameworks offer just a few examples of added pressures on compliance teams.

A February 2023 AuditBoard flash poll of over 1,000 compliance, risk, and audit professionals across a range of industries revealed that **most InfoSec professionals are facing significant challenges in managing their compliance programs.** The biggest challenges include: business and technical transformation (23%), talent management/strained resources (23%), and rapidly changing requirements (15%).

What is the biggest challenge for your compliance program right now?



For a security compliance program to be effective, it must be built into the fabric of the organization, its processes, and its people. This is the underlying motive for adopting a continuous approach to compliance, also known as continuous monitoring.

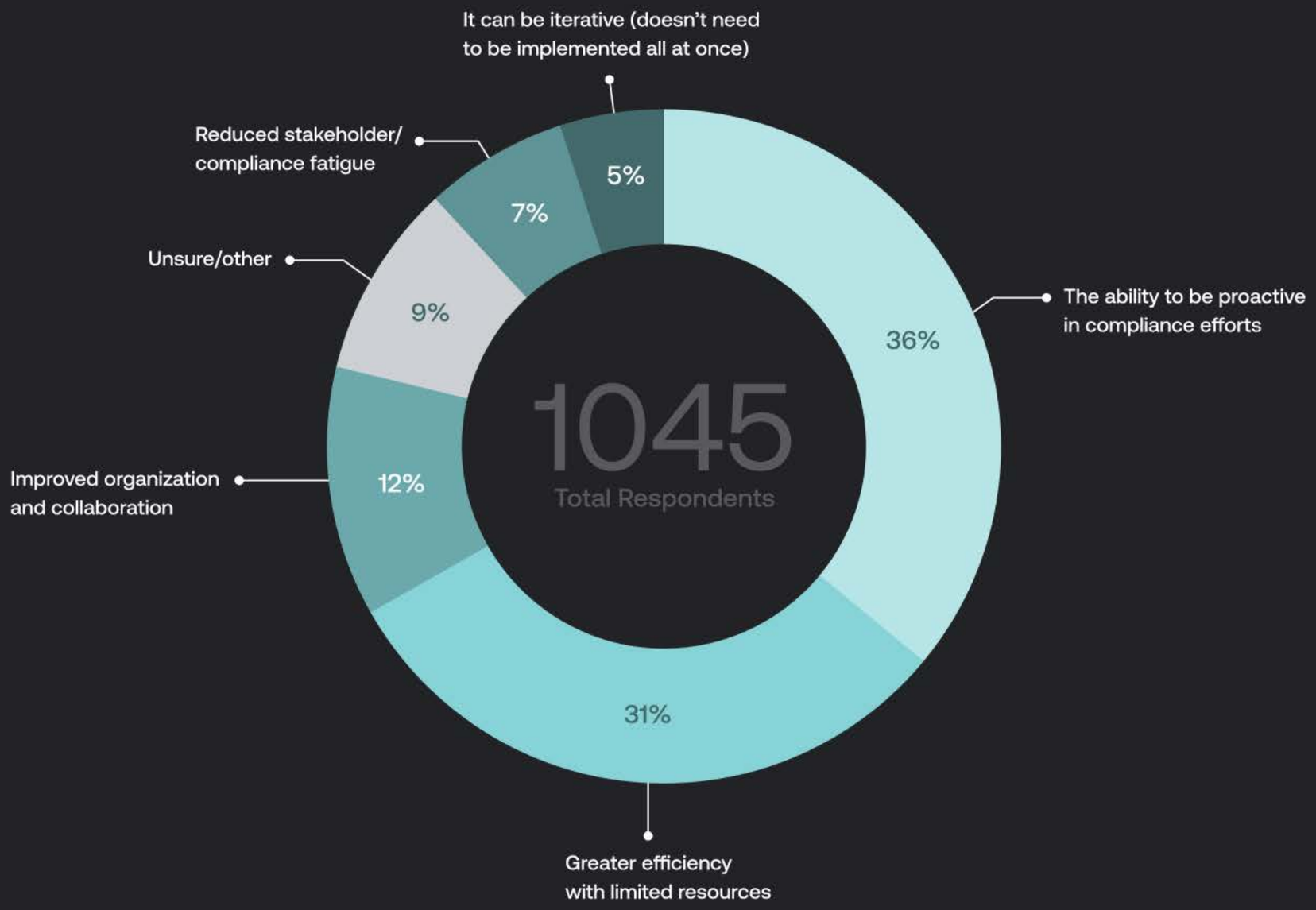
> The **National Institute of Standards and Technology (NIST)** defines continuous monitoring as:
>
> Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

The same AuditBoard flash poll found that 67% of respondents believe a continuous monitoring approach benefits compliance teams by enabling them to be proactive and more efficient in their compliance efforts.

A strong continuous monitoring foundation enables an organization to quickly pivot and respond strategically as new compliance requirements come into scope. Continuous monitoring can also help course-correct the challenges and shortcomings of a traditional approach to compliance, such as:

- **Point-in-time compliance results**. Teams with limited time and resources will perform point-in-time audits or assessments and build their control testing programs around these annual rituals. This produces results that are point-in-time in nature, which may lead to missed findings that can appear during other times of the year.
- **Finite resources.** Many compliance teams must contend with limited time, staff, and budgets. This forces teams to make tough decisions regarding what can be realistically assessed in a given timeframe. Teams sometimes have to make sacrifices, such as audit scope, depth of testing, or even longer gaps of time between tests.
- **Process owner fatigue.** The evidence request process is time-consuming and takes away from process owners' day-to-day jobs, which can lead to friction between stakeholders and compliance teams. Furthermore, stakeholders are sometimes subject to requests from teams performing different assessments with overlapping scope.

What do you see as the greatest benefit of a continuous monitoring approach?



Benefits of a Continuous Monitoring Approach

1

A continuous monitoring approach is risk-based.

It focuses on prioritizing compliance activities by risk level, enabling compliance teams to work more efficiently with limited resources.

2

A continuous monitoring approach is proactive.

Requirements always exist, not just during an audit, but as part of daily operations. When this is the expectation, compliance control owners understand that at regular intervals, they will need to provide evidence they have been maintaining, instead of scrambling to create or produce evidence reactively.

3

A continuous monitoring approach can be iterative.

Adopting continuous monitoring does not necessarily need to be accomplished in one fell swoop. No matter where you are in your journey, you can take steps to move your compliance program toward more continuous compliance.

4

A continuous monitoring approach uses automation and technology in the name of efficiency.

Continuous monitoring utilizes technology, e.g., governance, risk, and compliance (GRC), project management, and analytics applications to automate and streamline areas of your compliance program. Doing so creates efficiencies and can result in other benefits including better organization, improved collaboration, reduced stakeholder fatigue, and improved reporting.

This guide will help you incorporate a continuous monitoring approach into your InfoSec compliance program at every stage — from planning to preparing for third-party audits. These resources have been curated by AuditBoard's security and compliance experts for forward-thinking InfoSec leaders. We hope these tools will serve you and your organization in its journey to achieving continuous compliance.

Section 2

Planning and Scoping

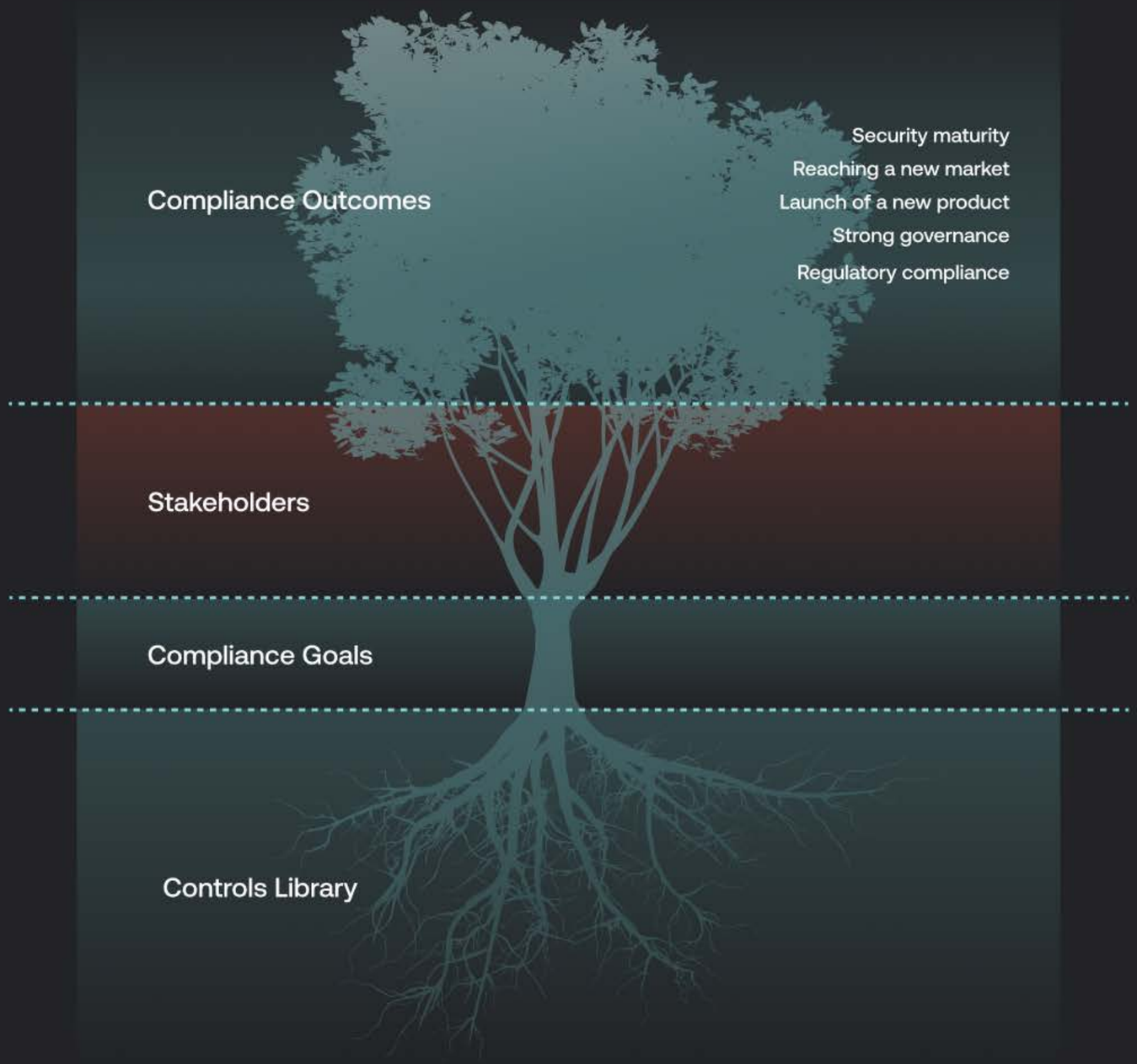
2.1

6 Tips for Creating a Positive Relationship With Your Stakeholders

Continuous compliance begins with leadership and strategy — after which the responsibility must be passed off between compliance teams and their stakeholders. **Stakeholders are as essential to compliance as branches are to a tree.** A healthy tree's branches support its foliage and fruit by delivering water and nutrients from the roots and trunk; without the branches, a tree is unable to reach its full potential. Without stakeholders, a compliance program is unable to produce its desired goals and outcomes, including:

- Security maturity
- Reaching a new market
- Launch of a new product
- Strong governance
- Compliance with regulatory requirements

The Compliance Ecosystem



Your stakeholders play a necessary role in driving governance and continuous monitoring because they own the processes in the organization and understand the vision and the goals for their line of business better than anyone else. Thus, **developing a positive rapport with stakeholders is essential to continuous compliance.**

The relationship with your stakeholders begins during discovery. This is an essential time to set up your relationship to succeed and thrive through testing and beyond. However, this is often a stage where things can go wrong. Furthermore, mistakes made here can lead to potential gaps in assurance down the road.

The challenge

For process owners, the overarching goal and need for satisfying a regulatory requirement can often get lost in the minutiae of managing all the responsibilities that come with governance.

The solution

From the very start of your relationship, ensure your stakeholders understand the purpose of governance work and how their responsibilities tie to compliance outcomes that support larger organizational objectives.

> "Communication with all stakeholders is key in developing the strategy and implementing the program."
>
> — NIST SP 800-137, *Information Security Continuous Monitoring*

6 Tips for Creating a Positive Relationship With Your Stakeholders

1

Understand their POV to build rapport.

Gaining a true understanding of your stakeholders' day-to-day activities, as well as their business unit's goals, will help you embed governance into their processes in a practical and considerate way that ideally helps improve their processes. In your discovery process, **aim to understand any objections or concerns from your stakeholders.** This empowers you to identify potential roadblocks down the road and proactively address them from the start. Doing so establishes an environment where stakeholders feel their voices and concerns are heard, building rapport.

2

Define risk in terms any employee would understand, from the analyst to the executive level.

When performing discovery on your stakeholders' processes, make an effort to define the risk involved in their day-to-day process in terms anyone in the business would be able to clearly understand. **Risk statements should distill relevant information into their most basic, actionable form.** This helps to ensure your stakeholders grasp the risk to their world, increasing your chances of winning their buy-in.

3

Prove the value.

Stakeholders will always wonder "Is the time and effort we're being asked to spend on governance **worth it**?" Approach them prepared to provide a compelling and convincing argument for why their work is valuable to the business, **e.g., driving revenue, helping to reach new customers/markets, increasing the business's compliance maturity score, etc.** Let them know you want to help empower them to make their process more efficient. Sometimes, even putting things in terms of the resource hours you might be able to save them in their processes can help to set stakeholders' expectations while also gaining their buy-in.

4

Leverage a common control set.

Build a compliance framework crosswalk to map your controls to multiple frameworks and requirements at once. **The resulting common (or baseline) control set effectively allows you to test a control once to satisfy its compliance with multiple frameworks and requirements.** This saves stakeholders from multiple documentation requests and duplicative control activities, reducing audit fatigue that could strain rapport.

5

Have regular check-ins.

Set check-in meetings on a scheduled cadence for you and your stakeholders to review milestones and KPIs, identify any bottlenecks, and address any internal changes that may have affected the process or control. Whether they happen on a monthly or bi-quarterly basis, these status meetings are **opportunities to tie compliance duties back to larger organizational needs and objectives** — and continue to develop rapport with your control owners.

6

Share your KPIs.

If applicable, sharing certain KPIs with stakeholders is an excellent way to drive accountability and continue to connect the importance of your stakeholders' control responsibilities to larger organizational objectives. Some examples include:

a. **Number of issues impacting critical certifications,** applicable regulatory requirements, or other issues that could cause severe reputational, financial, or operational damage to an organization.

b. **Time to remediate issues.**

c. **Time and expense calculation per issue.**

d. **Compliance status by framework.**

2.2

8 Keys to Success: Performing Gap and Readiness Assessments

Assessments are vital tools for planning and scoping throughout every stage of maturity in your compliance program. Gap assessments and readiness assessments serve similar purposes, and you can utilize either, or both, to help you determine and prioritize your compliance needs as they evolve over time.

- A **lightweight gap assessment** helps a business estimate how much effort it will take to comply with a framework or requirement.
- A **readiness assessment** is a full analysis of the business environment, performed after the business has made the commitment to comply with a framework. A readiness assessment helps compliance teams understand the areas of the business already operating as intended — as well as identify deficiencies to allow time for remediation ahead of a formal, third-party audit.

Common Reasons for Performing an Assessment

While reasons for electing to comply with a new framework or requirement are unique to every business — its industry, regions of operation, customers, and strategic objectives — the following are several common scenarios that call for assessments:

Customer/contractual commitments.

Obtaining a certification is a way for businesses to develop or maintain trust with customers and formally demonstrate compliance with a security framework or a regulatory mandate. This is commonly seen with ISO and SOC 2 certifications, which are often regarded as the "industry standard" in information security.

If your business plans to expand into new markets.

For example, a business that plans to expand into the European market will benefit from complying with ISO 27001, the leading international standard for information security management systems, in addition to the EU's GDPR standard.

Federal, state, and industry-specific regulations.

There are specific requirements that your business will be obligated to comply with depending on industry and location. Updates to regulatory requirements and new laws are also reasons for re-performing assessments.

If you are a software and/or security company.

Software and security vendors want to ensure they are up-to-date with InfoSec standards as well as industry-specific standards. For example, a SaaS platform that is expanding into the healthcare sector might aim to become HIPAA-certified to get a leg up on competitors, in addition to obtaining ISO and SOC 2 certifications.

If your business works or plans to work with government entities.

This may necessitate going after additional compliance certifications such as FedRAMP authorization and NIST validation.

Internal initiatives.

Businesses are recognizing the importance of not only complying with regulatory mandates and frameworks but ensuring they have the right resources and solutions in place to develop and mature their compliance program.

Selecting a Robust Baseline Framework

Choosing an appropriate baseline framework is foundational to continuous monitoring. Rather than focusing solely on your business's immediate compliance goals, consider where its compliance needs might be five years from now. This is prudent because some frameworks naturally overlap well with others.

Taking your business's immediate, short-term, and long-term needs into account can help you choose the framework that best satisfies multiple compliance goals at once. A holistic approach like this can save you from dealing with costly inefficiencies down the road, such as duplicative controls or winding up with an overwhelming control environment with no sense of prioritization right out of the gate.

Example:

The NIST 800-53 framework largely overlaps with FedRAMP — a notoriously difficult standard that often takes years to achieve compliance. However, NIST is a more risk-based framework with different maturity levels to benchmark your environment against, allowing your business to mature its control environment incrementally.

The following are some initial questions to ask yourself when deciding which framework makes the most sense to baseline your compliance program against:

- What are our immediate compliance needs?
- Where does the business want to be in five years compliance-wise?
- Where is there overlap between our immediate compliance needs and our longer-term compliance goals?
- Which framework satisfies the most areas we want to be compliant with in the long-term?

auditboard.com

Common baseline frameworks include:

- NIST Cybersecurity Framework
- NIST 800-53
- ISO 27001

The NIST and ISO frameworks are commonly regarded by the IT security industry as "best practice" baseline frameworks.

- The Secure Controls Framework
- The Control Objectives for Information and Related Technology Framework (COBIT 5)
- The Health Information Trust Alliance's Common Security Framework (HITRUST)

The Secure Controls framework is a super framework that covers NIST CSF, ISO 27002, NIST 800-53 and over 100 other laws, regulations, and frameworks.

8 Keys to Success When Performing Assessments

While there is no one-size-fits-all framework or solution for compliance, the following are some general keys to success when performing assessments.

1

Know where your business is headed.

Understand the scope of your business's compliance needs in the context of your industry landscape. In addition, understand your business's strategic objectives, as they will provide important insights that can affect the scope of your compliance activities.

2

Don't be shortsighted when selecting your baseline framework.

Do not make the mistake of limiting your compliance program to your business's short-term compliance goals — consider where your compliance program is headed within the next five years. You might save yourself valuable time and resources sooner than you think.

3

Create visibility into compliance status.

Visibility into status is essential for ensuring the business is on track to achieving its compliance objectives. Right off the bat, ensuring your evidence and controls data is organized, centralized, and reliable will streamline testing, issue remediation, and reporting. This is especially important as new business developments inevitably affect the scope of your compliance activities.

4

Reassess whenever necessary.

Any change to the business will bring with it new risks that will need to be folded into your existing compliance program. Compliance can often slip through the cracks with departmental reorganization. Even the smallest business change can cause a shift in control activities. Reassessments are essential tools for ongoing monitoring because they help identify what is new in scope, out of scope, and what controls and activities are duplicative.

5

Transform your stakeholders into allies.

Process owners might fail to understand how their control activities impact compliance and can even be resistant to completing compliance tasks outside of their day-to-day. From your first interactions with your stakeholders, take the time to help them understand why compliance is important for the business and how their activities are connected to overarching business goals.

6

Perform due diligence with third-party vendors.

Third-party risk is an integral part of compliance and should not be overlooked. It is vital to have a formalized, efficient process for vendor management in place that is also well-documented. As a best practice, third-party risk should be assessed and managed not only prior to onboarding new vendors, but also on a regular basis as relationships with those vendors continue. Defined policies and procedures should be in place that guide personnel in how to respond to breaches and significant events that affect third-party vendors.

7

Risk-rate the business to help drive continuous compliance.

Compliance is more dynamic than an annual, check-the-box exercise; when operating as intended, it should be an ongoing monitoring process. Frameworks like NIST can help you determine and rate maturity levels across different areas of the business. This can help you address high-priority risk areas first while having a plan for addressing lower-risk areas later. Risk maturity scales can also be utilized to determine where additional assessments should be performed.

8

Deploy technology to help manage multiple frameworks and drive continuous monitoring.

As your compliance program grows and evolves, you may wind up with multiple frameworks with areas of overlap. A compliance management solution can help you identify these areas of overlap when mapping new requirements to your existing framework. The right solution can also help drive organization, visibility, centralization, and automation throughout your compliance workflows. If technology is not a priority for your compliance team, take the time to consider how technology can contribute to your continuous monitoring efforts.

Section 3

Testing

3.1

Six Efficiency Hacks to Streamline Controls Testing

Without the right context, control owners can easily let their compliance responsibilities slide to the bottom of their priority list. One way to proactively combat this is to **turn compliance into a collaborative process, rather than enforcing a testing methodology on your stakeholders.** This period is full of opportunities to show your stakeholders you are their allies while creating efficiencies in the process.

Build efficiency and positive rapport throughout policy development and testing

1

Design control activities with the input of process owners.

The goal of continuous compliance is to recognize that requirements always exist — not only during an audit, but as a part of daily operations. If this is effectively conveyed, control owners will understand that at regular intervals, they will be providing evidence they have been maintaining — instead of scrambling to create or produce the evidence reactively. Utilize the control design stage to help your stakeholders improve and optimize their business processes. Not only does this help to embed compliance into their process as naturally as possible, but it also makes compliance a clear win for your control owners by adding value to their line of business.

2

Ask for process owner feedback during requirement review.

Oftentimes control owners can have limited insight into their applicable framework requirements because they have not been sufficiently briefed by compliance teams. Get ahead of this by requesting stakeholder feedback during your requirement review stage. Not only does this help to refine your scope, but it also can result in de-scoping something from a stakeholder's world — creating more efficiency all around. This underscores the importance of truly understanding your stakeholder's day-to-day process during discovery: you may learn something is not even applicable based on how their process actually works.

3

Define the test procedures and share them with control owners.

It is essential to create a defined and repeatable way to test controls. This is important because failing to establish the correct principles, information, and understanding of your compliance environment will render any automation or continuous monitoring efforts useless. Your test procedures should:

a. Include prescriptive guidance on what evidence you will be requesting — and define what qualifies as evidence.

b. Define the steps assessors are expected to follow in order to evaluate the effectiveness of a control.

c. Include the references to the systems, locations, and personnel that you will need access to in order to complete the test. (This is useful for automation and preventing loss of continuity if you have turnover on your team.)

d. Be shared with control owners before testing to minimize any confusion or surprise during testing.

4

When planning your testing schedule, take a proactive and risk-based approach.

Aim to create efficiency and efficacy, not to boil the ocean all at once.

a. Group your requirements by business function or overarching regulation, and specify the time frame when each of those groups will be tested (monthly, quarterly, etc).

b. Use a risk-based approach to stagger your testing to focus on higher-risk areas first, which may even result in de-scoping some areas.

c. Add the scheduled period as a data point within your risk assessment to ensure testing coverage of all necessary requirements.

5

When building your common or baseline control set, start small.

Focus on what is most relevant to your industry and organization — and most importantly, what the highest risks are. Biting off more than you can chew can result in ending up with an enormous control count that is neither efficient nor aligned with risk priorities. A better practice is to start small by taking a risk-based approach, focusing on the most urgent risks first, then expanding. For example, consider starting with the CIS top 20 controls as your baseline rather than NIST 800-53.

6

Lean on trusted industry peers and resources.

There are peers in your industry — external and co-source auditors — who have gone through the work of designing control libraries and common control sets before and have insights into the process. Starting from scratch can be daunting — and inefficient — when you can access these resources instead. An expert's knowledge and experience will benefit your control design process from a data integrity perspective, as they have vetted the process before and can provide best practices and proactive solutions to common pain points.

3.2

Optimizing Testing and Evidence Collection Using Technology

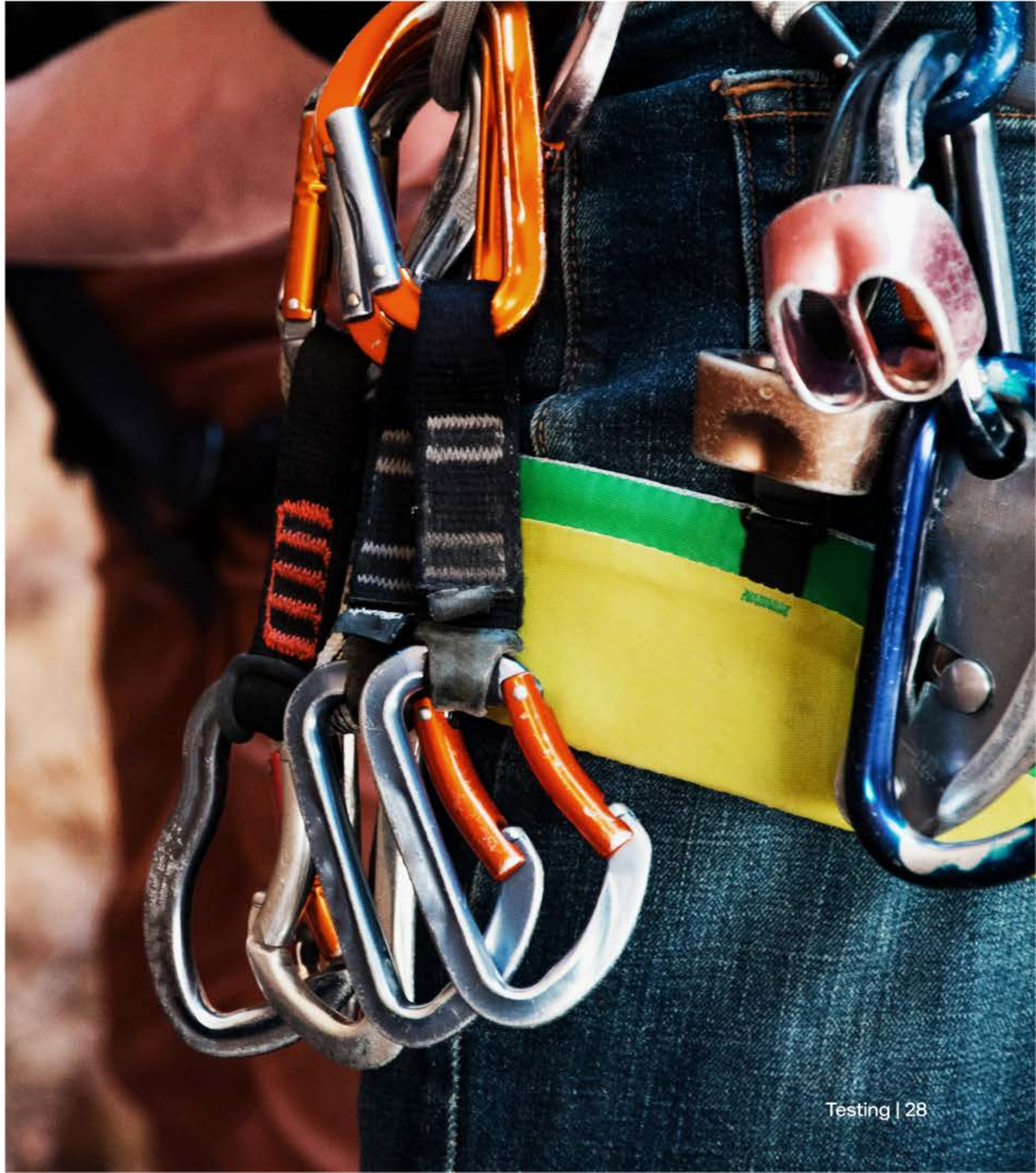
Controls testing and evidence collection can be burdensome not only for audit and compliance professionals, but also for the stakeholders that they engage with. **Teams can save time, improve consistency, and move closer to real-time results by designing automations to perform testing or collect evidence.**

There are some common questions to ask when approaching automation:

- Do we have the foundation that an automation can sit on?
- Should we focus on controls testing, evidence collection, or both?
- What are the strategic elements where automation provides the most benefit?
- What are the quick wins that allow me to focus time on things that matter?
- What information is available for me today to apply to an automation?

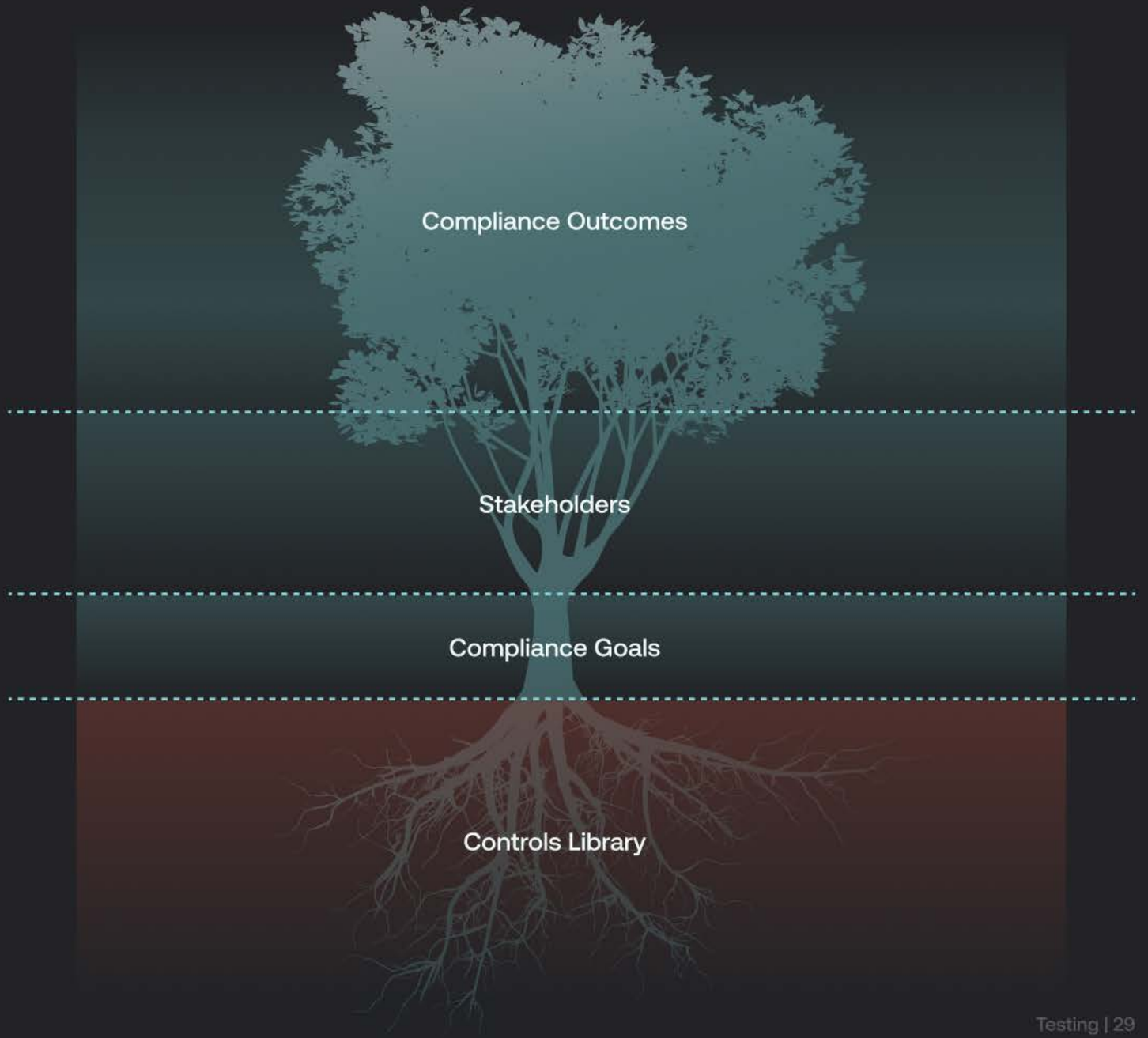
Controls Testing Foundational Elements

The most important consideration for your compliance program is your controls inventory (or controls library). Going back to the metaphor used in Chapter Two, if stakeholders represent a tree's branches, **your controls library represents the root system of your compliance program.** Like a tree's roots, which absorb the nutrients and water needed to support growth, the controls library contains the essential nutrients — data — needed to support a compliance program's growth and goals.



The Compliance Ecosystem

Just like a tree, where your roots live will determine the health of the entire system. Place your roots in a pot too small, or fail to transfer them to a larger environment as the system grows, and the roots will grow convoluted and suffocate. The wrong environment can make all the difference between a thriving compliance program and a weak one.



Controls Library

A clearly organized controls inventory should provide traceability to your frameworks, requirements, and assets, allowing you to scope your assessments with ease. Traditionally, control inventories are built from a spreadsheet-based risk and control matrix. However, this method often yields data inconsistencies, especially when users forget to update their data, which can lead to repeating inconsistencies throughout the spreadsheet.

Building your controls library using a connected risk solution helps to establish an organized database where your controls can be inventoried by asset owner and framework — a dependency for any optimization you build into your testing program thereafter. Automating any process depends on having complete jurisdiction over your assets and their underlying data structures, otherwise, there will be breaks in the linkage between your data points as they start to change. An integrated compliance management solution is one of the best available means to ensure your data is organized in a meaningful and reliable manner.

Controls Testing Procedures

In many cases, controls testing procedures are poorly documented or not documented at all. Maintaining testing procedures builds consistency in the approach taken by compliance professionals, but also level sets expectations when surfaced to stakeholders. **Once you have built your testing processes, incorporating automation and technology is the next step to maximize the efficiency of your testing program.**

For example, instead of manually checking if a password configuration meets a standard once a quarter or once a year, teams can build an automation to check the password configuration daily and produce a failing result on a control.

In cases where the testing requires more discretion by a professional, automation can be applied to other areas of the testing process such as pulling a population and sample selection.

Evidence Collection

Evidence collection is also an ideal area to begin optimizing using automation, which can eliminate the urgent fire drills of evidence collection to the benefit of both control owners and testers. Scheduling repeatable requests can save testers time following up manually. Some ways to achieve this are cloud-based collaboration and project management applications, including Slack and Jira.

Another way to achieve automated evidence collection is by using a compliance management solution to schedule evidence requests from a centralized location. The benefit of a centralized platform is that it provides a structured repository of evidence collected. Because your controls data is linked throughout the platform, the linkages between a control, its associated framework/requirement, and its evidence are clearly delineated.

This allows testing workflows to be easily created, scheduled, and repeated. Furthermore, questions from control owners can be answered in the platform itself, relieving a huge administrative burden for testers in terms of following up over email. Other features of a modern compliance solution that optimize the evidence collection process include:

- Automated timestamps when evidence is submitted in the platform.
- Automatic notifications to reviewers when it is time to validate the effectiveness of a control.
- Record of prior year's responses, allowing new team members to understand what was done the previous year.
- Consistent and standardized report formats.
- Real-time reporting, allowing for faster issue identification and longer remediation time.

Section 4

Issues Management

4.1

Issues Management Under a Risk-Based Approach to Compliance

While issues management often begins in silos like InfoSec, internal audit, and SOX, **a mature issues identification and reporting structure follows a risk-based approach by connecting issues back to the organization's risks.** To accomplish this, it is necessary to establish common and shared elements of issues management across departments. This typically involves a standardized issues nomenclature and risk scoring methodology that can be applied to issues as they are pushed into the larger, organization-wide issues ecosystem.

Consolidate Your Issues in a Centralized Database

Once departments establish a common or shared issues management methodology, it is time to consolidate your issues data in a central system of record. This process is typically led by a second-line function such as compliance or InfoSec. **A centralized technology solution is essential to keep your issues data organized and readily available to query for analytics and reporting.** Without a proper structural database to support your issues and link different data points to each other, analytics and automation are not possible.

An integrated solution can also help the InfoSec team and external audit to easily draft issues during identification, follow up with issue owners during remediation, and leverage issue dashboards and list views to facilitate weekly touchpoint meetings. An ideal solution should:

1. Enforce the issues management methodology. A standard issues rating and identification framework is either applied or formally standardized during implementation, which provides the basis for organization-wide compliance with the standard methodology.
2. Automates the issues follow-up process, letting the InfoSec team initiate an automated workflow that sends notification reminders to issue owners.
3. Have agile reporting capabilities. Issues should be automatically reportable anytime they are logged, and status will update in real time as issues move through the remediation process (validated, outstanding, overdue).

Leveraging Issue Dashboards for Reporting

When an issue is identified, it is also important to challenge the risk it is being mapped to and examine any other risks that should be considered along with it. **Ideally your issues should be mapped to their corresponding risks in the risk register, facilitating issue analysis by risk level — which plays a key role in issue prioritization.** The ability to map your issues to the risk register additionally enables KPI and KRI tracking for inclusion in executive management reporting.

One of the greatest benefits of selecting an integrated technology solution is that it can synthesize the various data points involved in issues management into real-time dashboards. Ideally, you want a flexible issues dashboard that can be tailored to convey different metrics, depending on your audience. The following are metrics that are a good idea to have on your dashboards for day-to-day compliance teams and executive level reporting.

Metrics to Track for Day-to-Day Team Reporting

The Checklist

- ☐ Number of open issues
- ☐ Number of open high-risk issues
- ☐ Number of controls or assets without owners
- ☐ Action plan progress
  - Mitigation plans due in X days from today
  - Number of action plans past due
  - Number of action plan extension requests
- ☐ New gaps and exceptions
- ☐ Overall issues remediation status
- ☐ Number of past due issues
- ☐ Issue due dates, owners, and reviewers

Metrics to Track for Executive-Level Reporting

Metrics for executive-level reporting should always be catered to what management is looking for, but here are some general examples of good metrics.

The Checklist

- ☐ Number of new high-risk InfoSec findings
- ☐ Number of overdue high-risk findings
- ☐ Number of approved high-risk exceptions with expired target dates
- ☐ Issues that are repeatedly identified (provides value for poorly managed processes, technologies, or teams)

The issues management arm of your compliance program is a natural extension of the groundwork laid in the preceding chapters. Its maturity and strength will depend on the planning that went into your assessments, design of control testing procedures and your controls library, and choices regarding automation and technology. **If your InfoSec program does not have a baseline system of record for your issues, make it a priority to advocate for one as soon as possible.**

Section 5

Reporting

5.1

Reporting on Continuous Monitoring

No matter how far along you are in establishing continuous monitoring, **you should be reporting on the performance of the InfoSec compliance program and events that impact the organization's position on security, compliance, or risk.** Access to reliable reporting is essential to continuous monitoring because it:

- Informs the InfoSec team of day-to-day compliance status, which helps the team drive compliance activities forward and address areas requiring attention.
- Informs executive management of issues management effectiveness and potential topics of relevance to the board.
- Informs the board of high-level issues and risk areas that require additional board support to address.

Good metrics should measure the performance of established measures (e.g., controls, baselines, SLAs) across tactical areas impacting the business, allowing you to escalate red flags or concerning trends to executive management. These consist of Key Risk Indicators (KRIs), Key Performance Indicators (KPIs), and analysis. The design of your continuous monitoring program should support your level and frequency of reporting metrics.

The following are some general metrics to track when reporting on continuous monitoring:

1

KRIs

COBIT 5 for Risk defines KRIs as metrics that show the enterprise is, or has a high probability of being, subject to a risk that exceeds the defined risk appetite. Because KRIs are pre-event metrics, they provide InfoSec the opportunity to engage with process owners and stakeholders before something becomes an issue. KRIs to consider tracking include:

- Number of critical systems or applications
- Number of users with access to all records (in a critical system)
- Number of competitor data breaches in the past year
- Number of malicious firewall events month to month
- Percent of third parties without a current security review
- Percent of incomplete security awareness training (or past due)
- Percent of systems without endpoint protection coverage
- Percent of systems with past due security patches

2

KPIs

Key performance indicators are metrics that provide executive management and sometimes the board with a snapshot of how your security program is functioning over time. Use KPIs to illustrate a story about your environment when updating management. Helpful KPIs to track include:

- Compliance status by framework
- Control effectiveness by process
- Number of phishing emails reported, last campaign
- Number of phishing failures per quarter
- Percent of vulnerabilities remediated in/out of SLA
- Percent of completed policy acknowledgements

3

Issues Management Effectiveness

KPIs specific to the performance of your issues management program are often what management is interested in most. Some helpful ones to cover in your reporting include:

- Number of new high-risk InfoSec findings
- Issues identified by root cause
- Issues that are repeatedly identified
- Issues by department, owner, or system
- Trend of past due action plans
- Expiring risk acceptances

Creating a Strong Reporting Foundation

The following are some basic requisites for creating a strong foundation for reporting on continuous monitoring.

Define critical events.
As compliance events occur, InfoSec must prioritize the ones that will impact the business the most. Defining critical events assigns an appropriate level of urgency to events based on risk, enabling InfoSec and the business to respond accordingly. Defining critical events can also help you structure your reporting frequency, as different areas require daily, weekly, or monthly reporting.

Critical event example

- High-risk vulnerability is approaching the remediation SLA (14 days to remediate and today is day 13).
- High-risk vulnerability has exceeded the remediation SLA (14 days to remediate and today is day 15).

Implement streamlined dashboards.
When configured effectively, reporting dashboards act as an alarm system alerting your team to emergencies in addition to tracking the progress of compliance day to day. Ensuring you have such a system that operates as intended is critical for driving continuous compliance. Once you establish your KRIs and KPIs, your dashboards become the source for helping your team make decisions and escalations.

Dashboard examples

- Chart with distribution of open vulnerabilities within x days of SLA: 1 day, 7 days, 30 days, 60 days.
- Chart with distribution of vulnerabilities (by owner, team, product, system, etc.) over SLA.

Establish reporting protocols with your team.
Once established, your KRIs and KPIs will naturally give rise to a cadence for reporting current standing against a given baseline, target, or goal (or historical reference). Based on this general structure, InfoSec can further build out its reporting protocols. These reporting protocols may include escalating point in time insights or summary reports provided to stakeholders at a set cadence.

Reporting protocol example

- Make metrics to account for critical events (high-risk vulnerabilities must be mitigated within 14 days from severity assignment).
  - KRI (# of high-risk vulnerabilities within three days of SLA)
  - KPI (# of high-risk vulnerabilities over SLA this quarter)
- Based on your event, create alerts to inform relevant parties to correct nonconformities before or after they happen.
  - An alert is sent to the security or engineering team to inform them of the vulnerability three days before its due date.
  - An alert is sent to the compliance team to indicate that the vulnerability is overdue.
  - The compliance analyst reaches out to the remediation owner to determine why this is delayed.

Continuous Monitoring Metrics and Reporting Outcomes

The alerting and reporting practices described above enable teams to identify when there is a high number of vulnerabilities approaching an SLA. When this happens, InfoSec should ask:

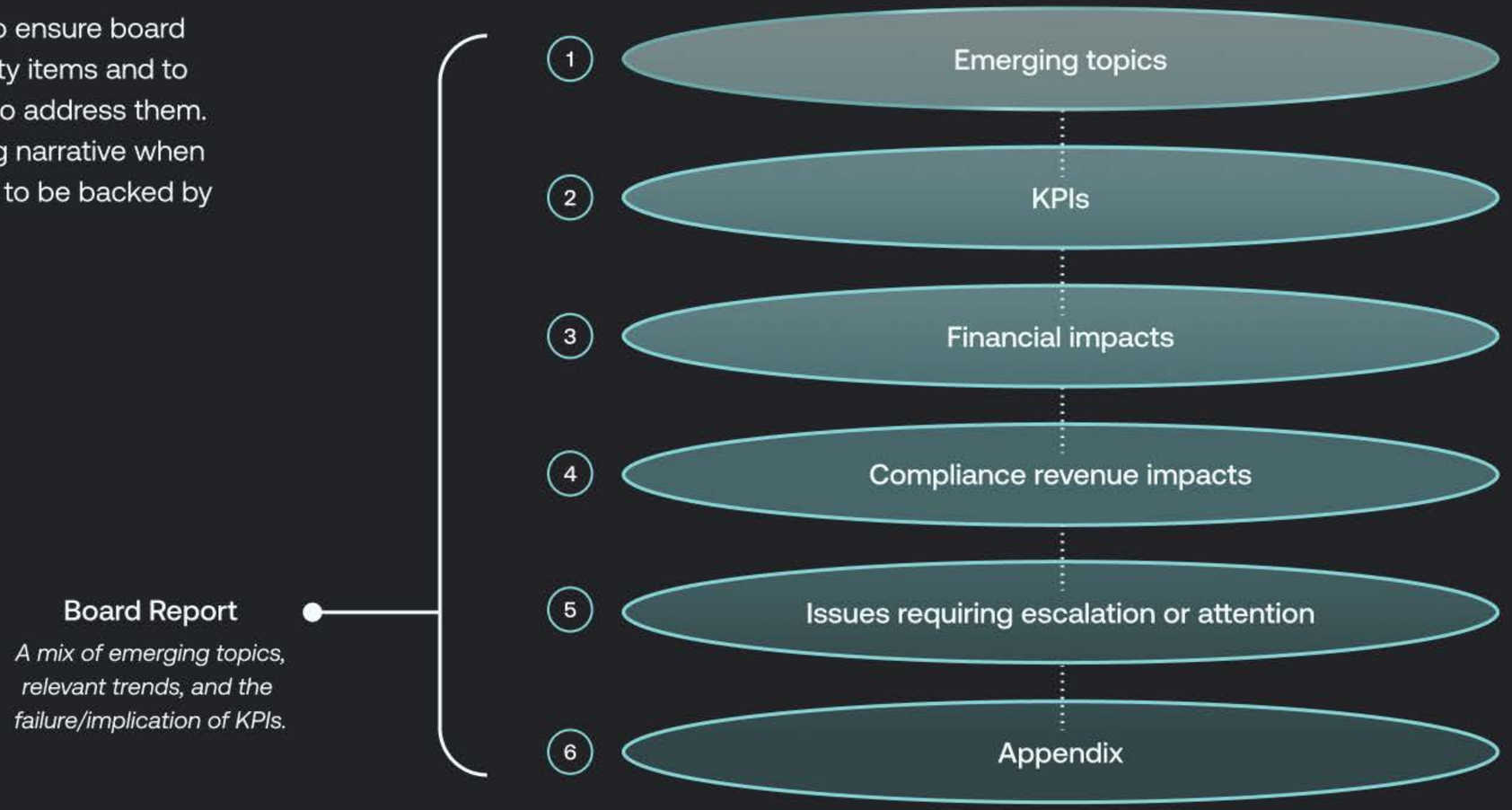
- Can the organization really mitigate these in time? Does the breach of SLA pose a risk? Why are there so many now in comparison to last month?
- Why are there so many SLA breaches for a given platform? Do we not have enough capacity to mitigate timely? Was the SLA designed too aggressively?

By answering these questions, the team can make improvements to the process and continue to monitor for effectiveness and compliance following their change.

5.2

What to Include in Your Board Report

The main goal of the report to the board is to ensure board members are aware of high-risk cybersecurity items and to ensure InfoSec has the appropriate budget to address them. It is important for InfoSec to prepare a strong narrative when presenting to the board, and for any request to be backed by compelling evidence.



1

Emerging topics

The goal of this portion of your report is to provide sufficient context — the “Why” — for any investment you are receiving or asking for. Use current events or trends from within your organization or your industry that will have an impact on the InfoSec program, either because they present new risks or threats, or because they present new requirements or expectations. Connect these emerging topics to organizational goals or objectives. Examples of emerging topics include:

a. Recent incidents and their business impact.

b. Rise in supply chain security incidents across competitors, representing an emerging threat for the organization.

c. Emerging regulatory pressures from the federal government or privacy regulators.

d. A macroeconomic situation that increases the likelihood of insider threats.

2

KPIs

Key performance indicators provide a snapshot of the effectiveness of your InfoSec efforts. Good KPIs are a measurement of the company's own performance against key security metrics. KPI attributions by leader, department, or team demonstrate where executive attention is needed on corrective action. Examples of KPIs include:

a. Percent of compliance framework requirements met.

b. Number of overdue action plans by team.

c. Percent of systems meeting patch levels by team.

3

Financial impacts

This section of your board report covers financial loss due to security incidents or regulatory fines. Financial impacts can be motivators for increased investment in compliance resources, such as integrated risk technology, analytics software, or outside expertise.

4

Compliance revenue impacts

Compliance revenue impacts cover the number of deals or revenue amount won or lost based on the company's ability to meet InfoSec requirements. Compliance revenue impacts can be motivators for taking on new compliance goals, such as obtaining a new security certification.

5

Issues/Areas requiring board support

Coverage of issues in the InfoSec report to the board is a subset of KPIs. While audit management also reports on issues to the board, the board should be made aware of any InfoSec issues at a high level to help enforce issues remediation.

6

Appendix

This is your opportunity to tie your metrics to revenue-generating impacts, connect KPIs to KRIs, and include any appropriate information required to gain board support for non-compliant events. This is also an opportunity to provide supporting materials that are often referenced when presenting the summary of the topics above. For example: if you are seeking board approval for FedRAMP compliance (which may be presented as an emerging topic), the appendix may contain a cost-benefit analysis of pursuing FedRAMP certification (authorization) that covers:

a. Loss of existing revenue if not pursued vs. cost of certification.

b. Increase in total addressable market if pursued vs. cost of certification.

c. Cost of continued reporting.

d. Timelines for implementation/remediation, certification, and renewal.

While there are many ways a CISO can go about board reporting, applying a risk-based approach allows them to summarize InfoSec's efforts and align them to critical areas of focus – enabling a higher level of communication in the boardroom. A risk-based approach enables the CISO to direct the board's attention to high-risk areas, justify why InfoSec is not focusing on lower-risk areas, and provide a reasonable rationale for why things are being done the way they are.

Section 6

Third-Party Audit

6.1

Six Best Practices When Preparing for Third-Party Audits

Depending on your business's size, industry, and compliance needs, it will be subject to third-party audits. **Businesses will typically choose to undergo a third-party audit with the goal of achieving or maintaining a security certification, such as SOC 2 (I and II), ISO, or PCI DSS.** While these audits are time-intensive, obtaining certifications are one of the most effective ways to provide assurance to prospective customers that your business adheres to industry-level security standards.

Audit Type	Time to Complete Audit	Period of Coverage
SOC 2 Type I	3-4 months	12 months
SOC 2 Type II[1]	2-3 months	12 months
PCI DSS	6 months	12 months
ISO 27001	3-6 months	3 years

[1] A Type II assessment provides more assurance than a Type I because auditors opine on the design and operating effectiveness of controls in a Type II.

Benefits of a Continuous Compliance Approach

If your business has taken a risk-based, continuous approach to compliance throughout the year, it is likely that it will have been preparing for its third-party audits throughout the course of its day-to-day compliance activities. Your choice of baseline controls framework, as discussed in Section 2.2, is also influential in preparing for third-party audits, because there is often crossover between frameworks. **If your InfoSec leaders have chosen wisely, your baseline controls framework will meet multiple requirements across frameworks, allowing you to achieve your compliance objectives more efficiently.**

Even if you are at the start of your continuous monitoring journey, you can take steps to incorporate third-party audit preparation into your compliance program. The following are best practices InfoSec teams can take to prepare in advance for third-party audits.

1

Understand and clearly define the scope of the third-party audit.

Many frameworks require a risk assessment over the subject matter in question in order to set the scope of a report. Look at the guidance provided by the governing body for the chosen compliance framework. Not only will this help determine what your initial steps should be, but it is also essential for setting and communicating timelines and deadlines. Be sure to loop in your internal stakeholders early on and communicate to them the purpose and objectives of the audit.

2

Prepare your internal stakeholders for what they will be responsible for.

Take the time to debrief your stakeholders on the purpose and goals of the audit, and to clearly outline the scope involving them. Be sure to share due dates and timelines well in advance. Define processes in a way that are scalable, as nothing exists in a vacuum from a compliance perspective.

3

Collect evidence early on.

This allows you to get a pulse on the environment well in advance to eliminate surprises. Being able to self-identify and communicate issues you are already aware of is advantageous to early remediation. If available, review audit and compliance projects that have already occurred that year to leverage any evidence or areas of overlap. This can help prevent duplicate requests and questions to stakeholders.

4

Get the right level of executive leadership involved.

Educate management on why the audit is taking place and when/where they will need to step in to get additional support for ensuring things are done timely. Agree to these protocols in advance so you can rely on their push when the time is needed.

5

Be familiar with the scope of your certifications and reports.

If you have a SOC report but are getting questions from customers that are not related to the report – make sure you are tracking this data. Doing so will allow you to address these areas in the scope of your SOC report for next year, and you will be better prepared to answer those questions next year.

6

Establish a good relationship with the external audit team.

Set communication expectations early on and agree to protocols for communicating potential issues, how they will be communicated, format of communication, etc. The more you can hold your external auditors accountable to pre-discussed protocols, the less likely there will be surprises in the audit cycle.

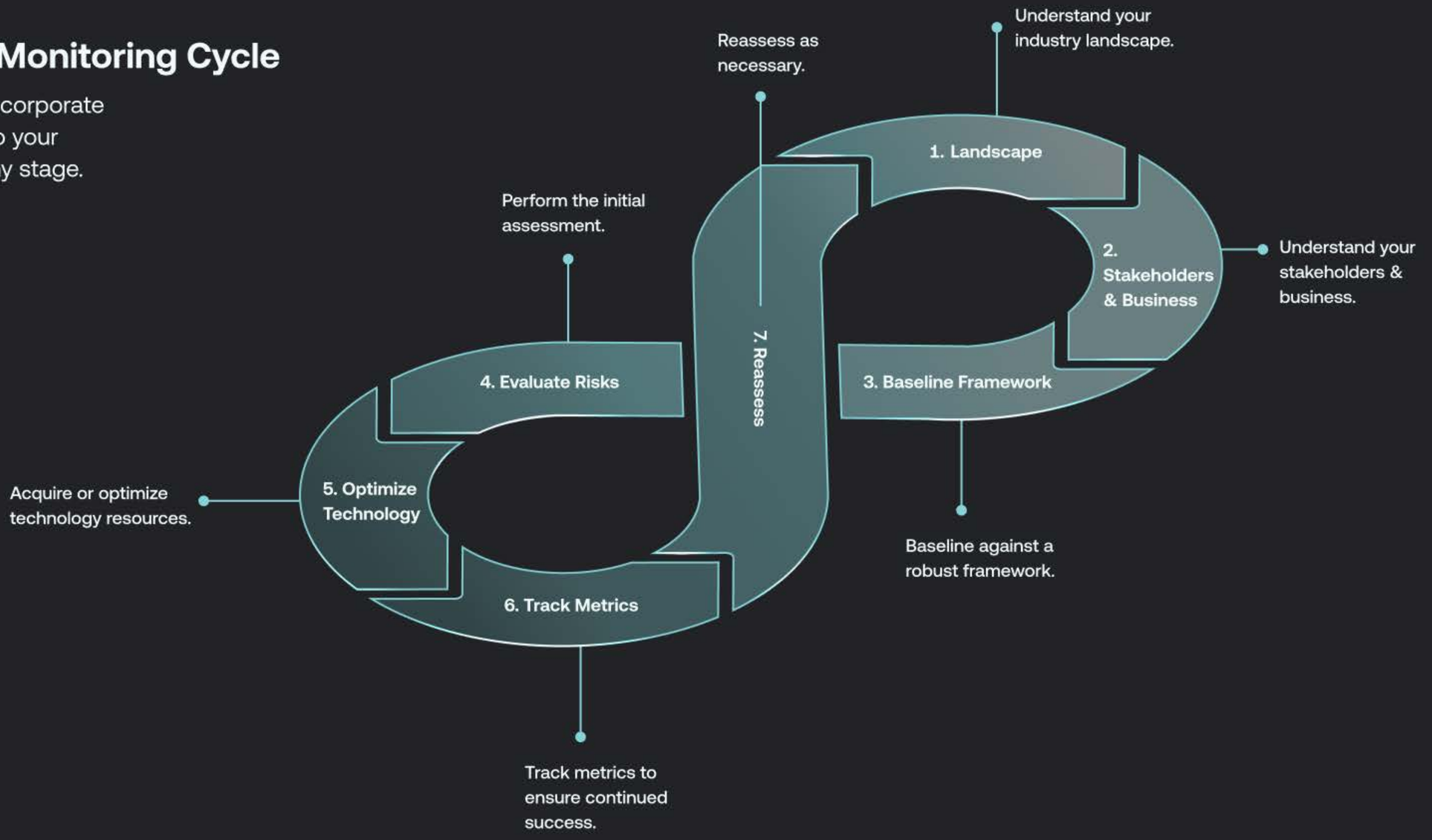
Section 7

Scaling

7.1

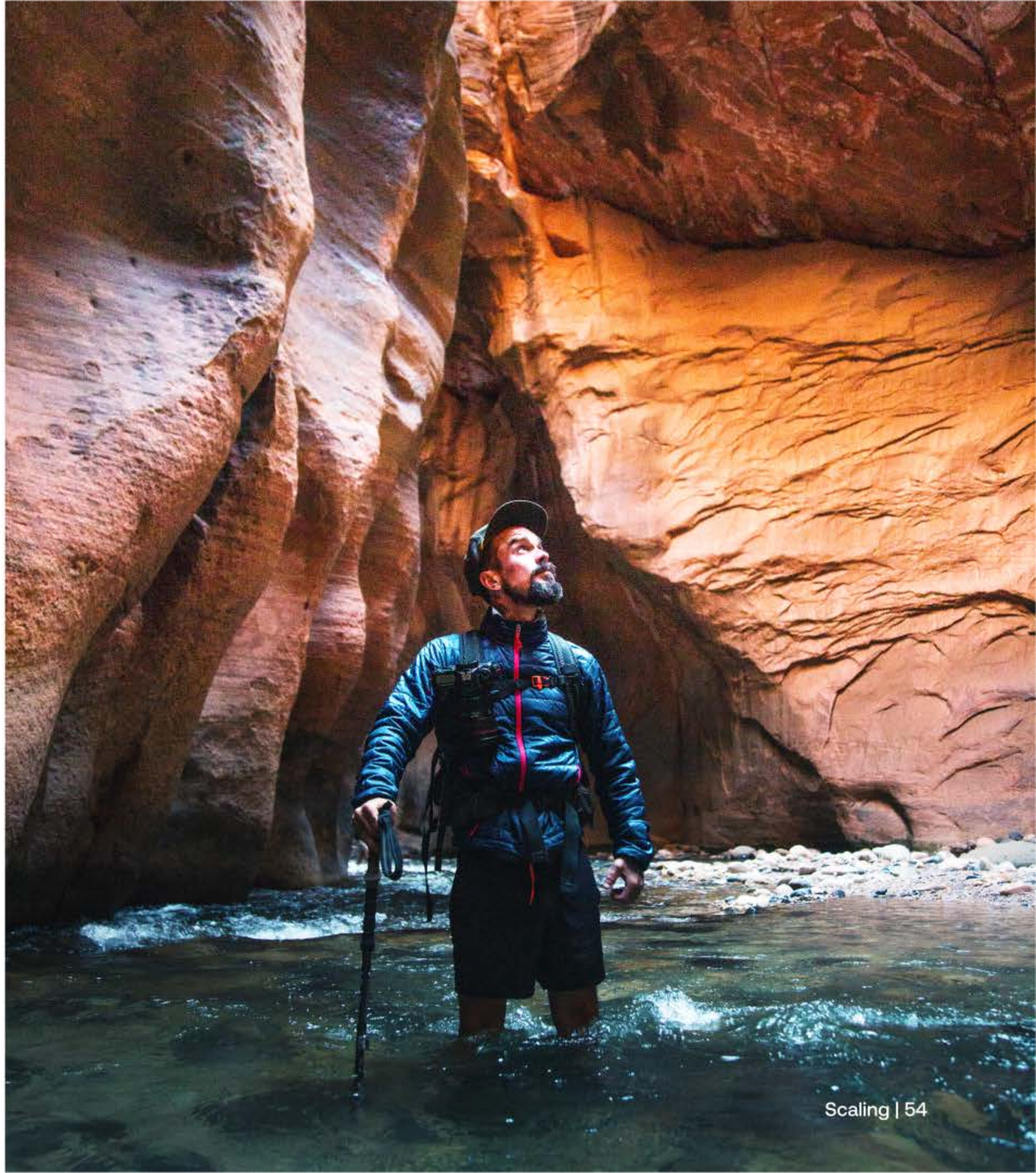
The Continuous Monitoring Cycle

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



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

Instead of viewing compliance in terms of that initial objective, consider what is needed to support that objective from the perspective of a long-term investment. Continuous monitoring is one mechanism to reduce compliance burden and allow programs to focus on emerging areas and improvements. The following seven steps will 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 every day and it is impossible to support a program without the use of technology. Simultaneously, compliance solutions have 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. See our Selecting a Security Compliance Technology Solution Checklist in the next chapter.

6

Track metrics to ensure continued success.

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

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

- ☐ Time 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.

7.2

What to Look for in a Security Compliance Technology Solution

If you find yourself drowning in a sea of compliance requirements, juggling multiple frameworks, and struggling to keep track of your compliance stakeholders and workflows, it may be time to bring order to the chaos. **The right technology solution can help streamline your InfoSec compliance program in a centralized platform that automates manual processes and enables real-time collaboration and reporting.**

Yet, finding a user-friendly, agile solution that enforces a standard issue management methodology and integrates with other analytics tools is no easy feat. The following checklist contains the most important features you should consider as you search for the right solution for your security compliance program.

Selecting a Security Compliance Technology Solution

The Checklist

☐ **Centralized, single source of truth.**
The risk and regulatory landscapes are constantly evolving and compliance requirements change. As your program matures, juggling multiple frameworks and requirements can become a complex and massive undertaking. A connected platform should facilitate this by serving as the centralized database and single source of truth for your risk, controls, and compliance data. This is foundational because without a proper structural database to support and link different data points to each other, analytics and automation are not possible.

☐ **Automated evidence collection.**
The benefit of a connected platform is that it provides a structured repository of evidence collected. Because your controls are linked to associated frameworks/requirements and risks, it allows your team to collect once, and use many. Having this foundation is essential to automating evidence collection in an efficient matter. Testing workflows should be easily created, scheduled, and repeated so you can integrate with your technology ecosystem and remove the manual effort in collecting evidence. Other features that can optimize the evidence collection process include:

- Automated timestamps when evidence is submitted in the platform.
- Automatic notifications to reviewers when it is time to validate the effectiveness of a control.
- Record of prior year's responses, allowing new team members to understand what was done the previous year.
- Consistent and standardized report formats.
- Real-time reporting, allowing for faster issue identification and longer remediation time.

The Checklist
cont'd

☐ **Real-time collaboration and follow-up.**
A robust InfoSec program requires cross-functional collaboration. Technology should facilitate this through cloud-based features like in-application commenting, tagging, role-based user permissions, automated workflows, and integrations with other collaboration applications, such as Slack and Jira. An example of how this works in action: The InfoSec team can create requests within Jira, directly from the compliance platform, so all questions control owners have can be asked and answered in the tools they already use, which is linked to the security platform itself — with a comments log showing the entire history of the communication.

☐ **Agile reporting capabilities.**
An ideal platform should have configurable reporting capabilities that enable compliance team members to easily create the reports they need — from day-to-day team reporting, quarterly issue reports for executive management, and reports for the CISO to leverage in board meetings. Issues should be automatically reportable anytime they are logged, and status will update in real time as issues move through the remediation process (validated, outstanding, overdue).

☐ **Intuitive and easy to use.**
An ideal technology solution should feel intuitive to its users — from day-to-day compliance team members to process and issue owners, management, and external auditors. An interface should not feel overwhelming to learn and there should not be a tremendous amount of time required to train users. It should feel instinctive in the way it facilitates compliance processes. A solution with these foremost qualities will enable it to scale easily with your InfoSec compliance program as it matures.

☐ **Issues dashboard that enforces the issues management methodology.**
As mentioned in Chapter 6, a solution should ideally enforce the issues management methodology agreed upon by the business departments that track and manage issues. Your organization-wide issues rating and identification framework should either be applied or formally standardized during implementation, which provides the basis for organization-wide compliance with the standard issues methodology.

The Checklist
cont'd

- [ ] **Standardizing the issues management workflow is essential in maintaining a security compliance program.**
A solution should enforce the issues management methodology agreed upon by key stakeholders throughout the issue management lifecycle. If no formal process is defined, then it is imperative a solution provides the baseline capabilities required to set up and formalize an issue management workflow.

- [ ] **Issue validation workflows that facilitate the issues methodology.**
In addition to enforcing a standardized issues methodology, a solution should also facilitate the issues validation process through automated issue remediation workflows. InfoSec team members can initiate an automated workflow that sends reminder notifications to issue owners with outstanding tasks due.

- [ ] **Ability to integrate with other analytics and workflow tools.**
Once an organization's risk, controls, and compliance data is in a connected platform, a compliance team can use complex queries to join and query the data from different data stores or sources to drive conclusions regarding control effectiveness. There are a number of different applications across an organization's cloud ecosystem that a compliance team might choose to integrate with to accomplish this, such as a data warehouse like Snowflake, or a data analytics tool such as Alteryx.

Section 8

Conclusion

Conclusion

Security Compliance for a New Risk Era

As the information security risk landscape evolves, new regulations and requirements will continue to come into scope. In this high-stakes compliance climate, it is essential to build a security compliance program with a strong foundation as well as the flexibility to accommodate new changes with ease. A traditional approach to compliance will inevitably come up short with point-in-time compliance results, overwhelmed resources, and process owner fatigue. **Adopting a continuous monitoring approach can help overcome these challenges by prioritizing higher-risk needs first, automating processes, and utilizing technology to assess and respond to risks on a more ongoing basis.**

Incorporating continuous monitoring into your InfoSec compliance program does not happen overnight; it is a process and can be accomplished iteratively. Remember: the goal of a risk-based approach to compliance is to recognize that compliance requirements always exist, not just during an audit, but as part of daily operations. Focusing on small and achievable goals, as outlined throughout the different chapters in this guide, means taking steps in the right direction. With every step — no matter how small — you will begin to build a continuous monitoring program that can serve your business for years to come.

To learn how AuditBoard can help automate your security compliance program and digitally transform your compliance department, visit auditboard.com to request a tailored demo.

Contributors

Elliott Bostelman CDPSE

Elliott is a former Senior Consultant, Cyber Risk Advisory Services at Deloitte; an Officer, Cyber and Information Technology in the US Army Reserves; and Manager of Solutions Advisory Services at AuditBoard.

Mike Condon CISA, CIA, Certified Blockchain Expert

Mike is a former consultant in the compliance and cybersecurity industry and a Manager of Compliance Solutions at AuditBoard.

Will Cryer CISA, CIPT

Will is a former Senior Manager, Technology Risk at EY, and Senior Manager of Solutions Advisory Services at AuditBoard.

Madison Dreshner CISA

Madison is a former Manager of Digital Assurance and Transparency at PwC and a Senior Manager of Compliance Solutions at AuditBoard.

Corey Landman CPA, CISA

Corey is a former Associate Audit Manager in the IT security and compliance industry and a Manager of Compliance Solutions at AuditBoard.

Tony Luciani CISA

Tony is a former PCI, QSA, and IT Risk and Compliance Sr. Manager at Sony Pictures and an IT Risk and Compliance Solutions Advisor for Enterprise Accounts at AuditBoard.

Richard Marcus CISA, CRISC, CISM, TPECS

Richard is a former Security Operations and IT GRC Leader in the technology industry and VP, Information Security at AuditBoard.

Kelley Spakowski

Kelley is a former creator and host of the GRC & Me Podcast; GRC software and services solutions professional; and IT Risk and Compliance Specialist at AuditBoard.

Mary Tarchinski-Krzoska CISA

Mary is a former Senior Manager at a security compliance company; EY alumna; and Market Advisor, Risk and Compliance at AuditBoard.

Kanaan Trotter

Kanaan is a former Enterprise Solutions Designer across InfoSec/GRC products, and a Senior Solutions Architect at AuditBoard.

John Volles CISA

John is a former Manager, Advisory Services at EY; PwC alumnus; and a Director of Information Security Compliance at AuditBoard.

The InfoSec Survival Guide

auditboard.com