scytale

SECURITY COMPLIANCE FOR CISOs:

SOC 2 and ISO 27001 Deep Dive

Contents

INTRODUCTION

Coffee, compliance, and CISOs: the three things keeping organizations safe from cybercriminals. However, without the needed support and guidance to navigate a changing security landscape, one of the three is about to run dry - spoiler alert: it's not coffee.

Security compliance often feels like the ever-present task that looms over every angle of your role as Chief Information Security Officer. Yet, regardless of the hours spent managing it, something can always slip through the cracks.

In this eBook, we're deep diving into security compliance for CISOs and how to best manage InfoSec frameworks. We're looking at key tips and details to keep in mind when undergoing two leading security standards, freeing up critical time without compromising security.

But first, let's cover the basics.

01

What is security compliance?

If you're a CISO, you're far too familiar with the concept of **security compliance.** However, in a fast-paced security environment that's quick to change, it's crucial to ensure you're always on the right track..

In a nutshell, security compliance refers to successfully implementing and following a security standard or framework. These frameworks, like **ISO 27001** and **SOC 2**, have set controls, requirements, and guidelines for protecting enterprises against cyberattacks and data breaches. If organizations comply with these standards, they can rest assured that they have implemented due diligence regarding information security. Easier said than done, of course.

02

The role of CISOs in security compliance at their organizations

Although security frameworks outline the dos and don'ts of your security systems (using significantly more tech jargon), it is still each organization's responsibility to understand, implement and manage these standards. Each security standard comes jam-packed with its own set of requirements, controls and audit processes. Hence, the need for a Chief Information Security Officer.

Naturally, a CISO's role in security compliance highly depends on the industry, location, products and services, and specific framework they've implemented. More often than not, it includes managing multiple frameworks across various products and services. However, a few high-level responsibilities apply to security compliance for most leading security standards. These include:

Developing and implementing security policies and procedures

Managing the security and compliance team

Monitoring network activity and preparing and identifying potential threats

Incident response and disaster recovery plans

Communicating security posture with upper management such as the CIO, CEO, or board of directors.

The most important takeaway from the list of responsibilities is that they all have one thing in common - they demand consistent management through either manual tasks or **automation**. However, developing, implementing, and enforcing security policies to protect critical data has its share of challenges.

03

The top security challenges for CISOs

Compliance is fleeting if not constantly monitored, tracked, updated, and tested. Fortunately, all great CISOs are known for identifying and adapting to new and evolving security challenges. However, some of the most significant challenges within the cybersecurity scope are harder to shake than others.

Unconsolidated products and services

Modern-day compliance often requires many digital products and services. This creates frequent back and forth when managing day-to-day tasks and overall compliance. Although digital tools can be beneficial in streamlining tasks, they also come with their share of data risks. It often means that CISOs work with various apps, platforms, and solutions that don't always work well together and further spread out critical data. Current industry trends are promoting a shift towards consolidated platforms. The administrative nightmare of running between apps, platforms, and solutions is an important contributing factor.

Growing attack surface

It's no secret that organizations across all industries need help to secure their public-facing applications, with threats evolving quicker than information security systems can keep up with. A significant contributor to the escalating threats can largely be attributed to the growing attack surface. CISOs must defend their data on multiple fronts, including web, mobile, social, physical, and cloud networks. Moreover, with increasing organizations settling into a hybrid work setup, protecting sensitive data becomes even more challenging (and essential).

Accurately measuring security posture

One of the most challenging aspects of robust cybersecurity is accurately gauging its effectiveness over time. In the security compliance world, we often speak of the difficulty of staying compliant instead of getting compliant. CISOs are responsible for continuously monitoring and measuring an organization's security posture to better identify and mitigate any vulnerabilities, weaknesses, or new threats. To do this, CISOs seek tools and solutions that prioritize security progress over time and allow CISOs to gauge their current security posture accurately.

04

Compliance frameworks and overcoming common challenges

Organizations can no longer afford to settle for subpar standards regarding information security. That's where leading security compliance comes into the picture. Security standards like ISO 27001 and SOC 2 act as a blueprint for creating and managing the highest level of cybersecurity.

The proper compliance framework allows CISOs to map out their controls and risks in one fell swoop, and ensure that they are implemented and operating effectively with an official audit. However, staying compliant with these frameworks is just as crucial and no small task. The first step? Coming to terms with which security compliance framework/s is right for your organization based on location, industry, business operations and more.

05

SOC 2 and ISO 27001: What's the difference?

In the infosec world, putting **two leading compliance frameworks** against each other is a familiar narrative to determine which one will reign supreme. But that's not what we're going to do.

There is no favorite when comparing SOC 2 and ISO 27001. Now although this can easily sound like the stereotypical cop-out when avoiding picking a side, i,e (you're both special in your own unique way) - hear us out because staying objective is key here.

Compared to ISO 27001, SOC 2 follows a more flexible and customizable approach. SOC 2 is based on the **five Trust Service Principles**, and (apart from the mandatory security TSP) organizations can choose the criteria that apply to their specific business. This differs from ISO 27001, which requires companies to establish an Information Security Management System (ISMS) according to specific requirements.

Another important differentiator is that SOC 2 is not considered a certification, as with ISO 27001. Instead, a SOC 2 report is an attestation given by an independent auditor assessing the effectiveness of your controls. The result of a SOC 2 audit is an attestation report confirming an organization meets SOC 2 standards. In contrast, an ISO 27001 certification reviews the whole design and operating effectiveness of an organization's ISMS at a point in time.

Regardless of which framework your organization needs to implement, the overall success hinges on an organization's ability to implement and manage it effectively. Here's what you need to know to best implement and manage consistent compliance for SOC 2 and ISO 27001.

06

SOC 2 compliance for CISOs

SOC 2 (Service Organization Controls 2) is based on the five "Trust Service Principles"; **Security, Availability, Processing Integrity, Confidentiality,** and **Privacy**. This specific framework includes a set of compliance requirements primarily geared toward technology-based companies that need to secure and manage a cloud-based security landscape.

In terms of compliance, as it's an **attestation**, organizations must undergo a strict audit process to specify how exactly the organization manages internal controls and protects customer data.

Here are a few tips on preparing for the audit process and managing consistent compliance.

07

Managing SOC 2

Firstly, it's important to understand how exactly the audit process works. A SOC 2 compliance audit can only be conducted by a licensed CPA firm or agency accredited by the **American Institute of Certified Public Accountants (AICPA).**

The audit will be divided into two types of reports, a **Type I** and a **Type II** report. A SOC 2 Type I reports on the suitability of the design of an organization's relevant Trust Service Criteria controls. A SOC Type II will examine the design and the operating effectiveness of an organization's relevant Trust Service Criteria controls. Type I will be done at a set date, whereas Type II will stretch over a set period, to accurately manage effectiveness. Once you've established the type of SOC 2 report that you need to prioritize, you're ready to start focusing on the following steps:

Identify a clear TSP scope

Before prepping for your audit, you need to define your TSP scope. As a CISO, you have a clear and precise understanding of what your SOC 2 attestation needs to achieve and what the scope should include. So take time to fine-comb through the five trust service principles and build your unique scope. Although the Security principle is mandatory, other principles may be necessary and more valuable to your organization than others. You can move toward additional compliance goals only once you've achieved this strategic clarity.

Undergo a readiness assessment

When undergoing an audit, no organization wants to deal with pitfalls that could have easily been avoided. To mitigate any missed steps in the preparation process, CISOs utilize **readiness assessments.** Readiness assessments are paramount in confirming whether your company's relevant controls meet the standards required by SOC 2. A readiness assessment is also critical to gauge whether you have all the needed documentation and requirements before the audit. Any shortcomings can then be dealt with effectively during the remediation process.

Prepare documents and policies

Most preparation revolves around documentation and policies required for SOC 2 compliance. Throughout the audit, the auditor will examine the following documents that must be prepared, gathered, and aligned with SOC 2 standards.

- **Policies:** Create and retain the complete set of policies that outline all necessary controls and how you've implemented them to align with the SOC 2 framework.
- **Procedures:** All information security activities must be identified, recorded and collected as evidence for the auditor to assess. Auditors are seeking a clear outline of your security posture based on your relevant business operations. For example, organizations must disclose all third-party vendors and the relevant risk management procedures.

08

ISO 27001 certification for CISOs

We can't start the deep-diving process without a proper introduction, especially for one of the leading global data security protocols. ISO 27001 is a comprehensive security standard that considers personnel, policies, systems, and technologies to gauge an organization's security posture. It follows a systematic approach and is a highly effective way to assess and correct data security risks across the organization. To become ISO 27001 certified (yes, this one's a certification), a company must develop an appropriate **Information Security Management System (ISMS)** and undergo an independent audit.

An Information Security Management System (ISMS) includes all your policies, procedures and controls for systematically managing sensitive data. After you've established a robust ISMS, an audit will compare it against the ISO 27001 standard and how you preserve ISO 27001's three core pillars of information security: Confidentiality, Integrity, and Availability.

09

Managing ISO 27001

Regarding ISO 27001, most organizations heavily rely on their CISO for most of the tasks and responsibilities needed to secure compliance. As compliance covers a significant scope across the organization, a CISOs role typically includes everything from compliance, relevant documentation, risk management, asset management, incident management, third parties, and relationships with top management. It's a multi-faceted role that not only hinges on a CISOs ability to understand compliance frameworks but also highly depends on their understanding of all internal structures and processes.

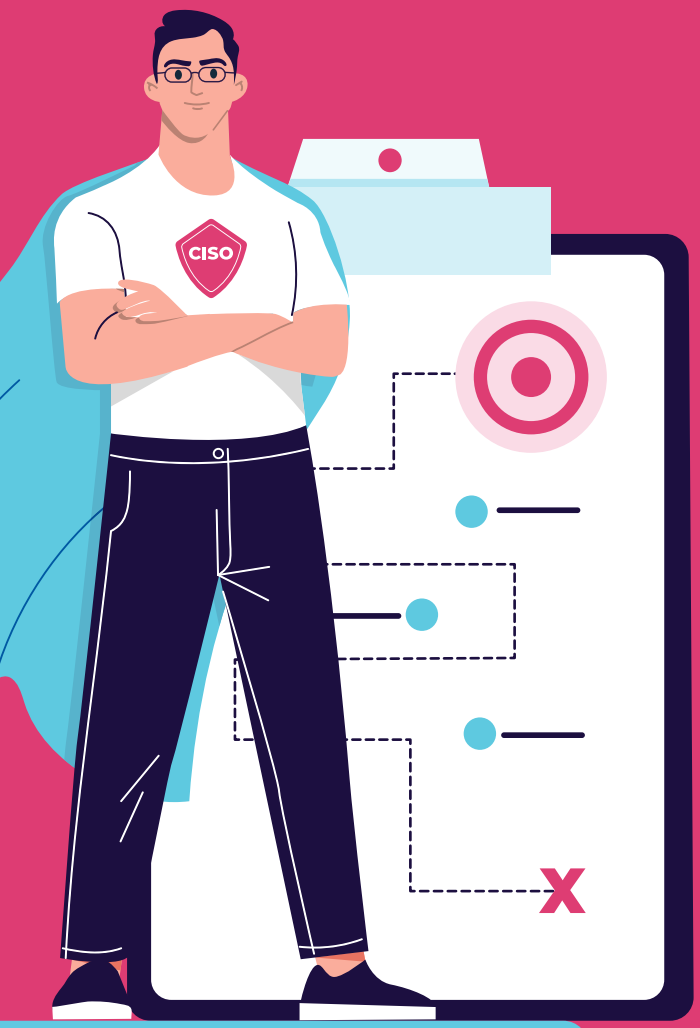
To help ease the burden, here's our deep dive into ISO 27001 for CISOs.

10

A step-by-step guide to ISO 27001 compliance

Since preparing for an ISO 27001 audit can be resource-intensive and costly, compliance managers and CISOs must ensure that their approach, controls, and standards are in place before the audit process.

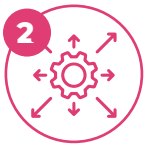
However, keeping track of all the requirements can take time and effort. In addition, the last thing anyone wants is to go through rigorous preparations to fail the audit or expose your organization to areas of non-compliance. So, if you're implementing ISO 27001 or preparing for your next audit, here's our step-by-step guide to ensure you haven't missed anything critical.



STEP ONE

Follow a systematic approach

Creating an effective ISO 27001 strategy is indispensable to the certification process. This means that you'll need to decide at a high level what you'd like to achieve with ISO 27001. This includes documenting clear timelines and assigning clear roles and responsibilities. In addition, transparency and accountability are vital in obtaining and managing your ISO 27001 certification. Be sure to consistently review responsibilities and tasks to ensure everyone (including leadership) is in the loop with what is required from them regarding security and compliance.



STEP TWO

Define the scope of your ISMS

Defining the scope of your Information Security Management System (ISMS) is one of the most critical aspects of your data security. You could miss critical gaps within your security protocols if your scope is too narrow. However, on the other hand, if your scope is too broad, you could be wasting valuable time and resources. Therefore, align your ISMS scope with industry-specific goals and relevant security concerns when finalizing it.

STEP THREE

Create ISMS policies

At this point, drawing up the ISO 27001 policies and documentation and sharing them with the relevant stakeholders is essential. These policies form the blueprint of your security posture and define your high-level data security needs and objectives.

STEP FOUR

Confirm risk management procedures

Each CISO within an organization is often responsible for deciding which **metric they prefer to score their risks.** ISO 27001 compliance does not specify **risk management procedures.** However, CISOs must decide upfront whether they will use qualitative or quantitative metrics to assess risks.

STEP FIVE

Risk assessments

Risk assessments are critical in helping organizations identify, analyze and evaluate any crucial gaps within their information security systems. Conducting risk assessments will, in turn, allow you to identify where some of the most significant vulnerabilities lie, which then helps you better gauge which controls to prioritize.

STEP SIX

Specify and implement relevant controls

You need to determine the relevant controls needed to safeguard your information security. In most cases however, at least 90% of the ISO 27001 controls are applicable. When specifying and determining controls, it's required that you draw up a **Statement of Applicability** detailing the relevant controls and how they are being implemented.

STEP SEVEN

Ongoing monitoring and training

To become ISO 27001 certified, a top-down approach may work to pass the initial audit. However, it will only last for a while. To maintain consistent compliance, CISOs must prioritize constantly monitoring controls, gaps, security structure and awareness within the organization. Security awareness training plays an important role in monitoring and maintaining said consistency and shouldn't be overlooked when managing security compliance.

11 Security awareness training for ISO 27001 and SOC 2 compliance

In the grand scheme of compliance, **Security Awareness Training** has often been regarded as a box to tick off rather than an intentional and transformative tool. However, nowadays, it has become more apparent that, if done properly, security awareness training can drive consistent compliance and mitigate data breaches and security threats. However, the true impact of security awareness training can only be seen if implemented correctly.

Who's responsible for quality assurance? The CISO, of course.

A part of a CISOs scope will be to ensure proper security awareness training across the organization. Not only because it's considered best practice but also because it's a strict requirement for both SOC 2 and ISO 27001 compliance. Security awareness training is among the many overlapping criteria within SOC 2 and ISO 27001. Both security benchmarks insist that security awareness training be implemented into the long-term security policies of your organization.

So, how do you choose the right security awareness program? You're looking for an SAT that provides behavioral change within your organization and creates a security-conscious culture - not just a quick workshop, monkey-puzzle, and badge of completion. Building this behavioral change starts with including the following core elements in your SAT.

How to measure security awareness training

As both security frameworks consider security awareness training mandatory requirements, accurately measuring it and sourcing evidence regarding its implementation can be tricky. Therefore, when rolling out an SAT, CISOs must prioritize the traceability of the program and whether it allows for accessible evidence collection.

If you're responsible for collecting the evidence without the help of an automated compliance solution, keep the relevant documentation or records that prove the successful completion of each employee's training. This could include an attendee list, test results, and registration reports.

Speaking of automated compliance solutions.

Simulated exercises

Responding to cybersecurity may seem straightforward on paper (although rarely even on paper), but putting it to practice is an entirely different story. To ensure that everyone has contextualized their training, frequent simulated exercises are a great way to keep the team sharp, prepared, and up to date with the most recent systems and response protocols.

Relevance

Some concepts may seem relatively straightforward to you, but for employees unfamiliar with infosec best practices, an overload of information can be overwhelming. Keep the material relevant and concise to maximize knowledge retention and information consumption. This can also be done by segmenting content towards specific teams within the security scope, so they can prioritize training that they can apply to their day-to-day tasks. It's also critical to ensure that the learning material is aligned with your organization's security policies and the scope of an employee's job description.

Learning methodologies

Ultimately, the goal is to create a workforce that eases the burden of security compliance and works together to mitigate cybersecurity threats. To do so, you need to ensure that your employees are interacting with the training material in a way that encourages them to consume and retain the information. That being said, people process and internalize information in different styles. Therefore, your SAT program needs to be mindful of this and incorporate tools and techniques that support different learning styles, such as a mixture of explanatory videos, tutorials, quizzes, and exercises.

But, as with all things compliance, when it comes to security standards, even your best attempts at creating a robust security culture are null and void if it's not measurable. To correctly measure your security awareness programs for SOC 2 or ISO 27001 compliance, CISOs need to consider the following.

12 Automation and security compliance: Is it worth it?

As the scope of cyber threats snowballs, day-to-day tasks, and responsibilities start piling up, and security framework requirements are constantly updating - compliance can feel like a constant race against time. Feeling anxious? Well, **94% of CISOs** said they are equally stressed at work. In fact, 65% admitted that work-related stress issues directly compromise their ability to protect their organization.

This is why many CISOs have gravitated towards implementing automated compliance solutions to help them track and manage their security posture and compliance. At the very crux of compliance automation, technology replaces tasks that previously required strenuous manual labor. Moreso, through efficiency and effectiveness, all these previously manual processes and systems are precise, consistent, and up to date with the most recent changes regarding security standards.

However, if you're handing over some of your priority tasks to a platform, you will want to be sure of how (and why) it works and how it impacts your specific role in compliance. Overcoming this trust barrier is one of the key reasons some CISOs have yet to implement automation.

Will it replace some of the core responsibilities that CISOs are frequently tasked with? On the other hand, could it perhaps add more to your plate? Here's what you need to know about how automation is transforming compliance management for CISOs.

Automation consolidates compliance management

Compliance isn't a one-time task (whether attestation or certification), so constant tracking and monitoring are quintessential in assuring consistent compliance. However, no CISO can be the all-seeing eagle eye of an organization 24/7. Sooner or later, something will go unnoticed or slip through the cracks. However, this is not for lack of trying, leading to even more stress and employee churn. According to a **recent survey**, 57% of CISOs surveyed believed that one consolidated platform would significantly reduce their workload and stress.

The right automated platform consolidates all the necessary variables that impact compliance and manages it on one platform, giving CISOs an overview of all their obligations, including workflows, risk assessments, control evaluations, testing, staff security awareness training, and corrective actions.

Automation bolsters productivity

Without automated compliance management, successful compliance hinges on your team's ability to spend hours compiling reports, collecting evidence, deciphering controls and security frameworks, and testing their effectiveness. It also leaves little room for in-depth monitoring as the compliance catch-up game is time-consuming and resource intensive.

Automation platforms give CISOs that need a break in the storm to gather their bearings and get ahead of the curve. It monitors and assesses internal controls in real-time, allowing you to take a proactive approach instead of relying on damage control. More so, it creates the much-needed gap for CISOs to take a more hands-on approach to processes that require their attention while automating other tasks such as control processes, risk assessments, evidence collection, and alerts - maximizing productivity and accuracy.

Automation provides access to expertise

Automation isn't just about freeing up your schedule and streamlining processes. Truly automated platforms prioritize the importance of giving access to industry experts in the field. As a CISO, you know what you're doing and what your vital objectives are; however, in the intricate and complex world of security compliance, it's critical to enhance your understanding of specific controls and framework requirements, especially considering that standards are prone to change, easily misinterpreted and challenging to apply to particular niche industries. The right automated compliance platform puts experts in your corner to ensure that you're up to date and that nothing slips through the cracks.

Automation improves third-party vendor management

Third-party risks are a growing threat when it comes to cybersecurity and can quickly become a resource-intensive and time-consuming process to track and monitor. Ultimately, CISOs are responsible for overall supply chain management; however, even if vetted, landscapes change, and threats exist and submerge. With automation, CISOs can easily manage vendor security assessments and track compliance, gauging the risks of internal and external stakeholders.

Manage security compliance with confidence

Ultimately, the best way to ensure consistent compliance is to know you don't have to take on the mammoth task alone. But unfortunately, the world of compliance is complex, isolating, and sets even the top CISOs up for failure without the needed guidance and support.

Rather than relying on trial and error, get (and stay) compliant up to 90% faster with Scytale. We offer a fully automated compliance solution consolidating everything you need to manage your **SOC 2** and/or **ISO 27001** compliance in one centralized platform. Zero errors, zero risk, zero stress.

Keen to see how Scytale can revolutionize your compliance management?

Experience Scytale here