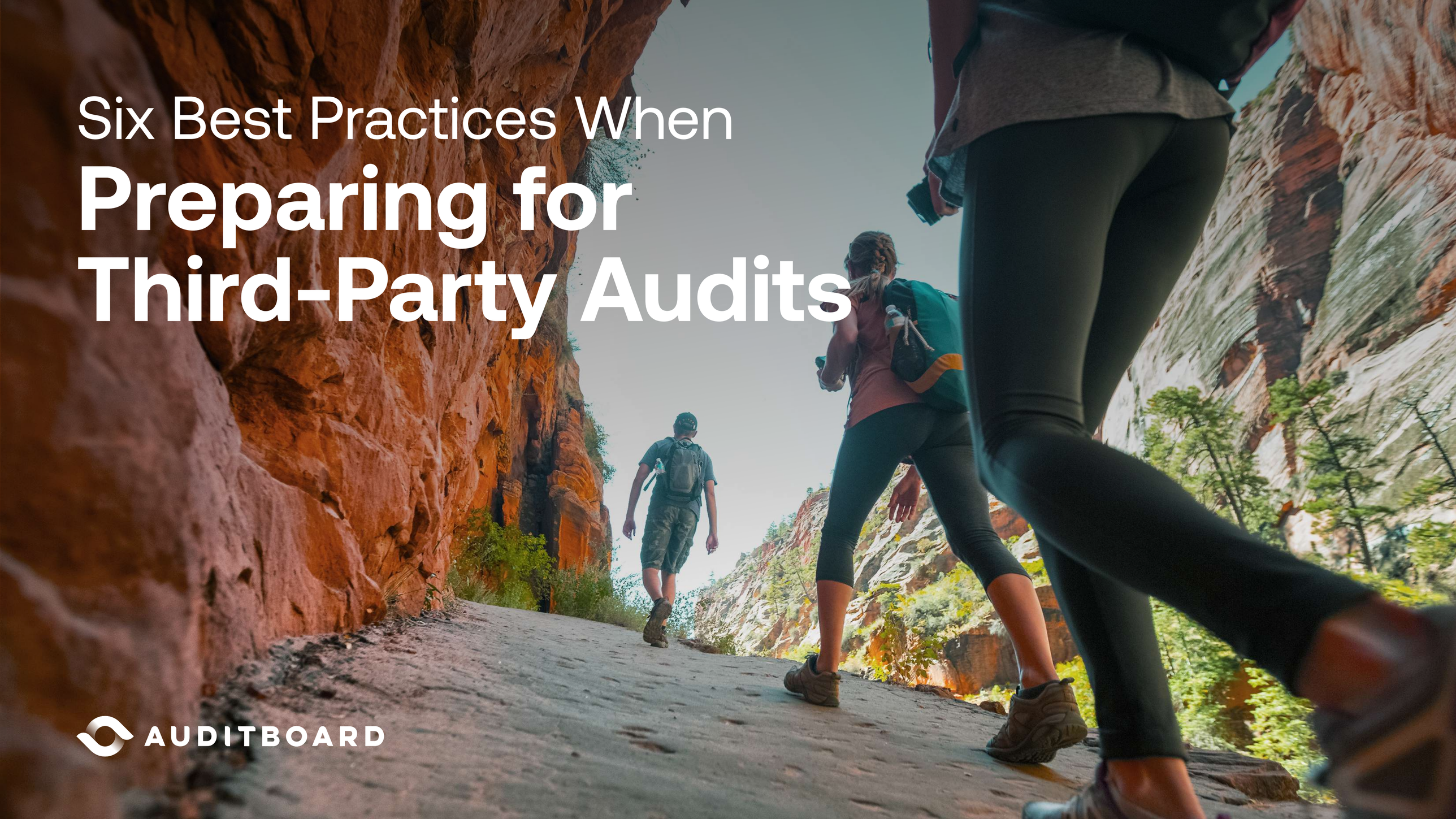


Six Best Practices When

Preparing for Third-Party Audits

AUDITBOARD

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.

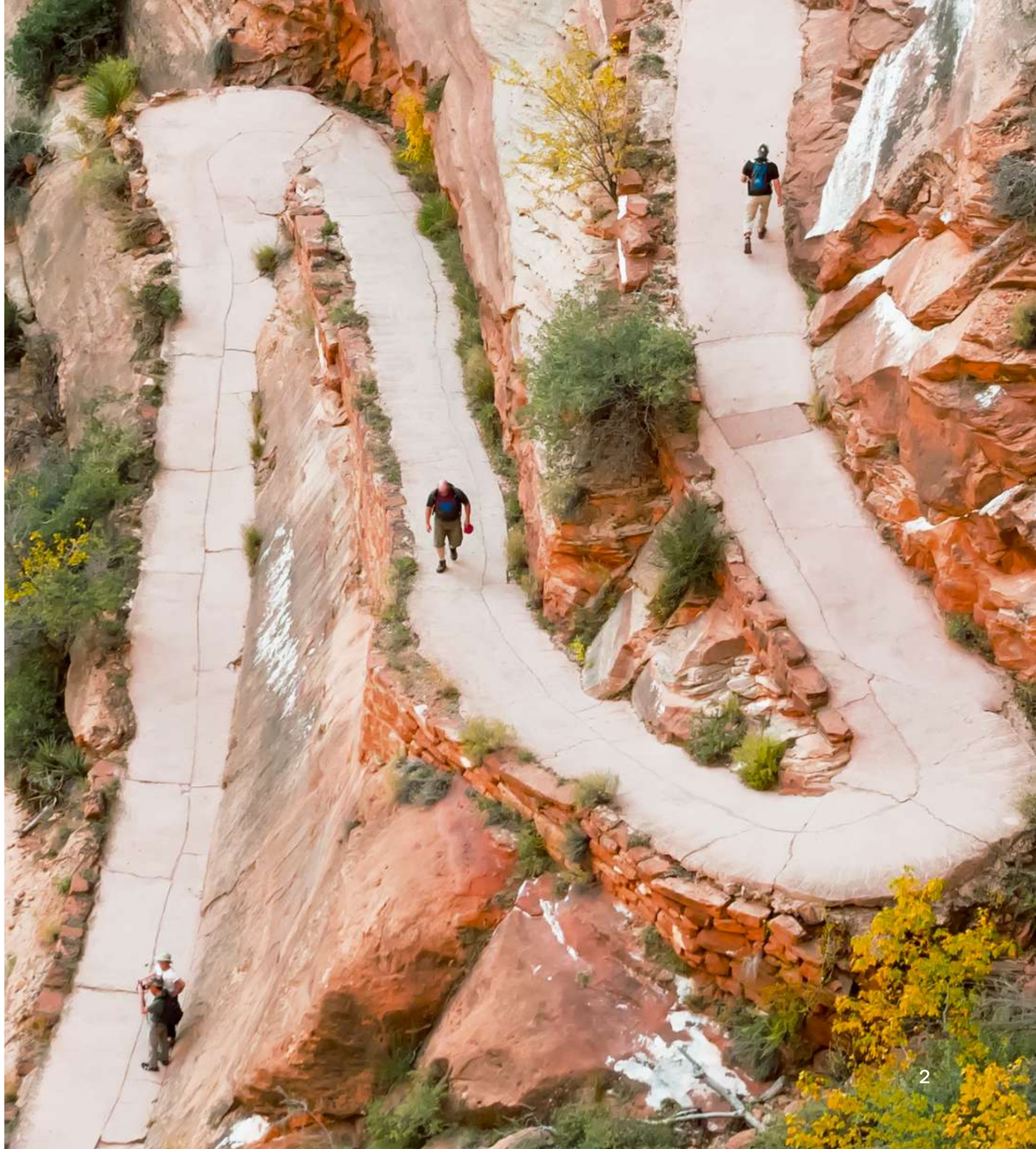
Audit Type	Time to Complete Audit	Period of Coverage
SOC 2 Type I	3-4 months	12 months
SOC 2 Type II[1]	2-3 months	12 months
PCI DSS	6 months	12 months
ISO 27001	3-6 months	3 years

[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

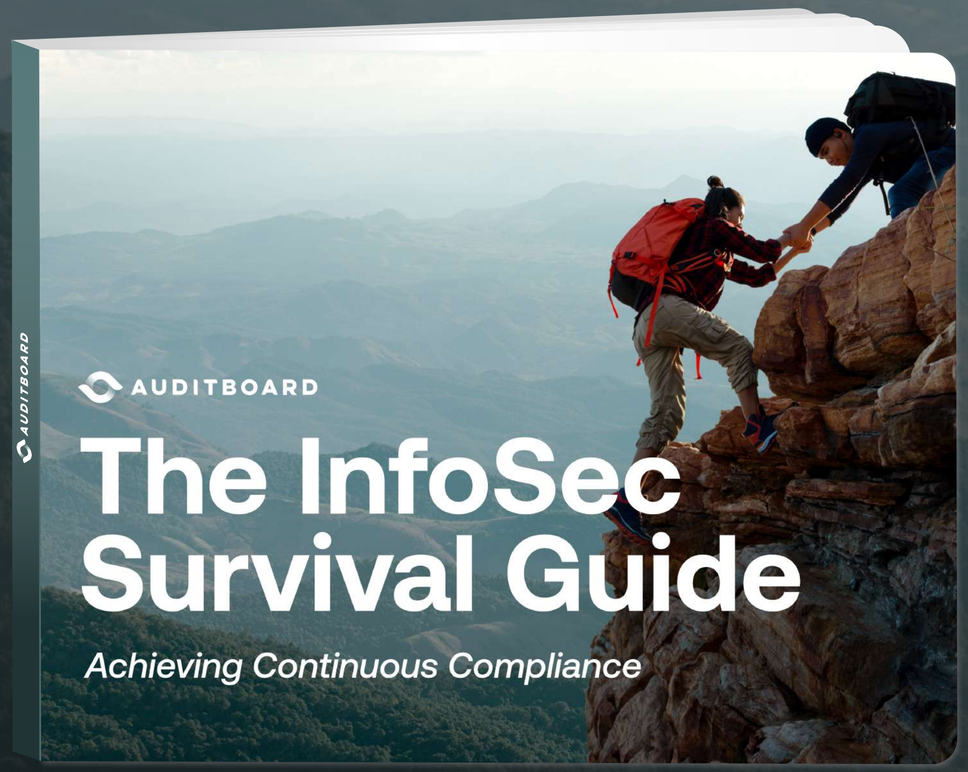
Be familiar with the scope of your certifications and reports.

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.



Get the Full Guide

auditboard.com