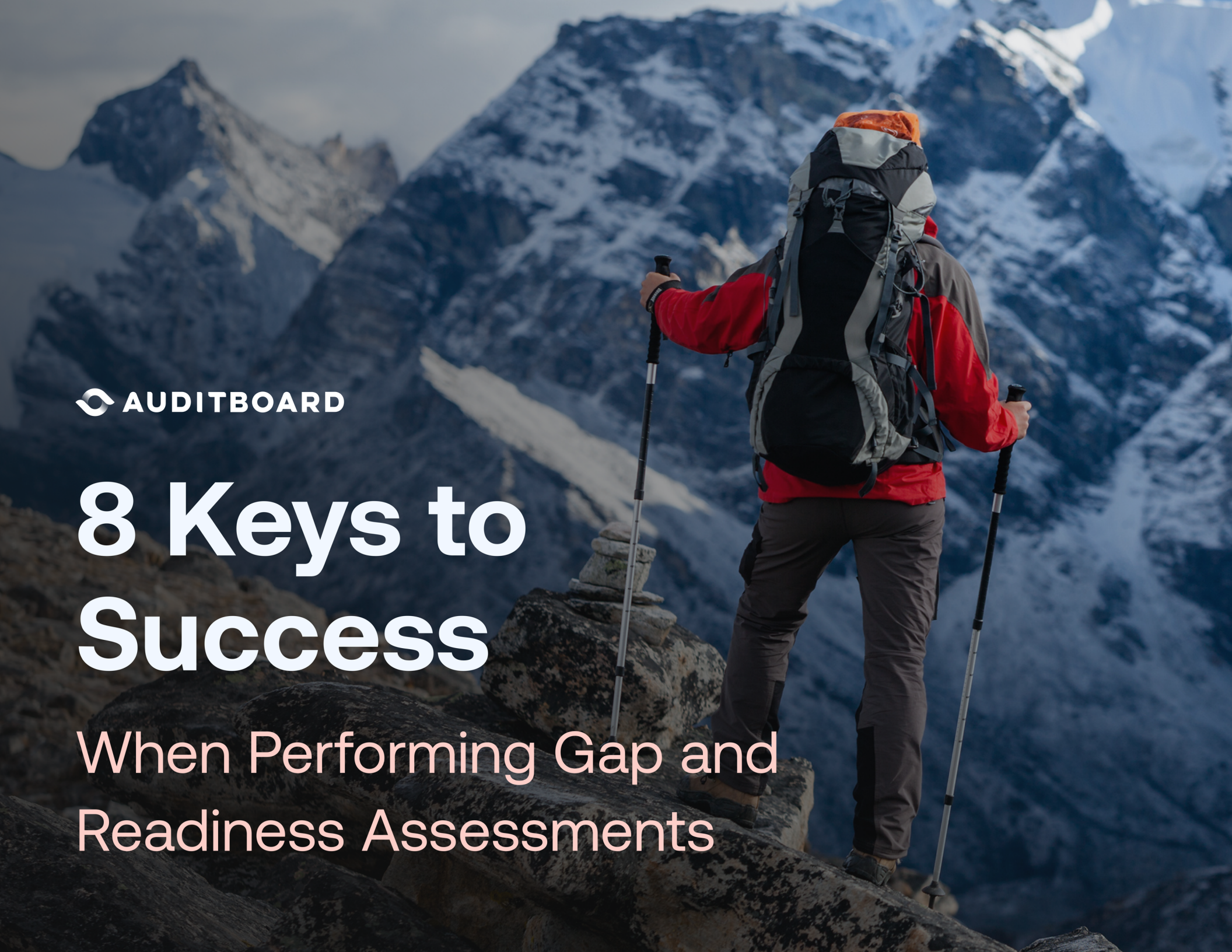


AUDITBOARD

8 Keys to Success

When Performing Gap and Readiness Assessments

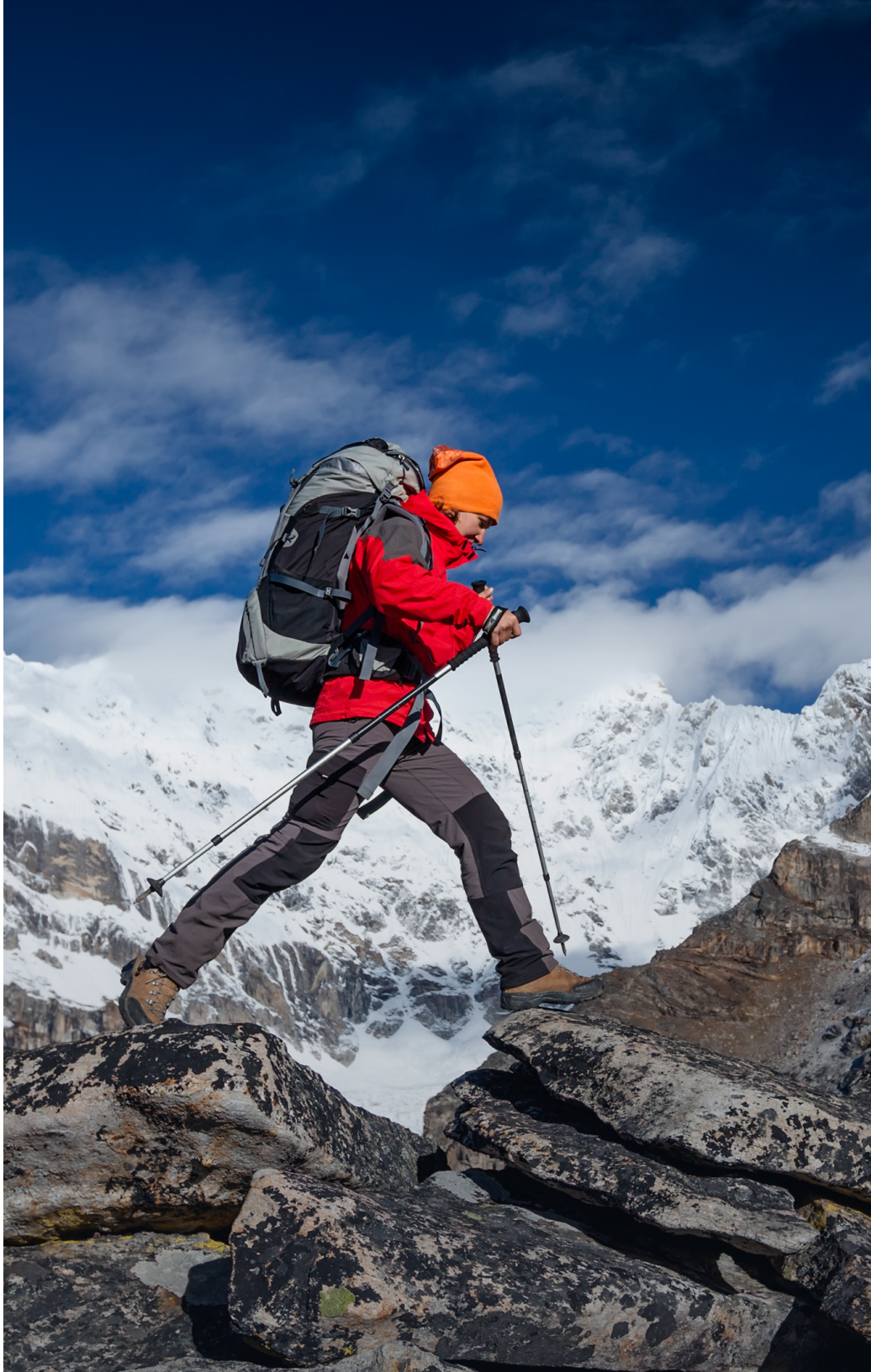
8 Keys to Success

When 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:

1. **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.
2. **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.
3. **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.
4. **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.
5. **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.
6. **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

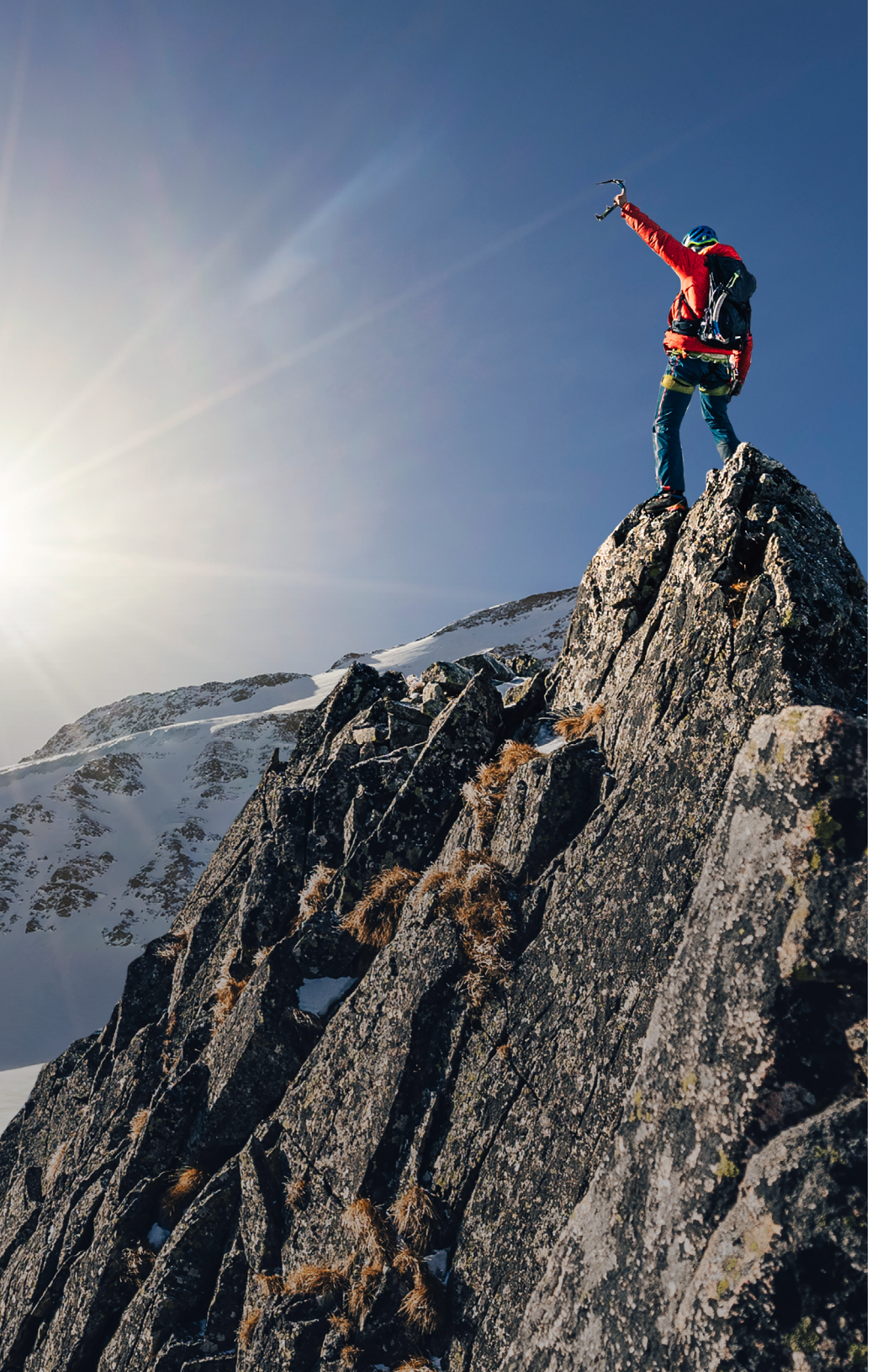
Choosing an appropriate baseline framework is foundational to developing continuous monitoring. Taking a risk-based approach, rather than a compliance-based approach, is especially relevant because it will set your compliance program on the path to accommodating new changes efficiently. This is essential for the evolution of your compliance program and is key to maturing compliance in the business over time. So, instead of viewing compliance as a short-term goal — consider it a long-term investment.

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?



Common baseline frameworks include:

- NIST Cybersecurity Framework*
- NIST 800-53*
- ISO 27001*
- 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 NIST and ISO frameworks are commonly regarded by the IT security industry as "best practice" baseline frameworks.

**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. Risk-rate 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.

7. 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.

8. Consider 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.

To achieve a state of continuous monitoring, a compliance program must programmatically reassess risk and adjust its practices to ensure they are up-to-date and on track to achieving your compliance goals. By following the best practices outlined above when performing reassessments, you can set your compliance program up to successfully monitor risks throughout the year. Learn how CrossComply by AuditBoard can help you automate your assessments.