360ADVANCED

COMPLIANCE THAT PAYS:

How the Right Audit Firm Protects and Propels Your Business

Table of Contents

SECTION 01

Compliance as a Business Growth Driver

"Working with 360 Advanced to build out our compliance program has put us in a position to take advantage of – and win – much bigger opportunities. It's also allowed us to keep business, because we're able to continue supporting our clients as their compliance requirements grow."

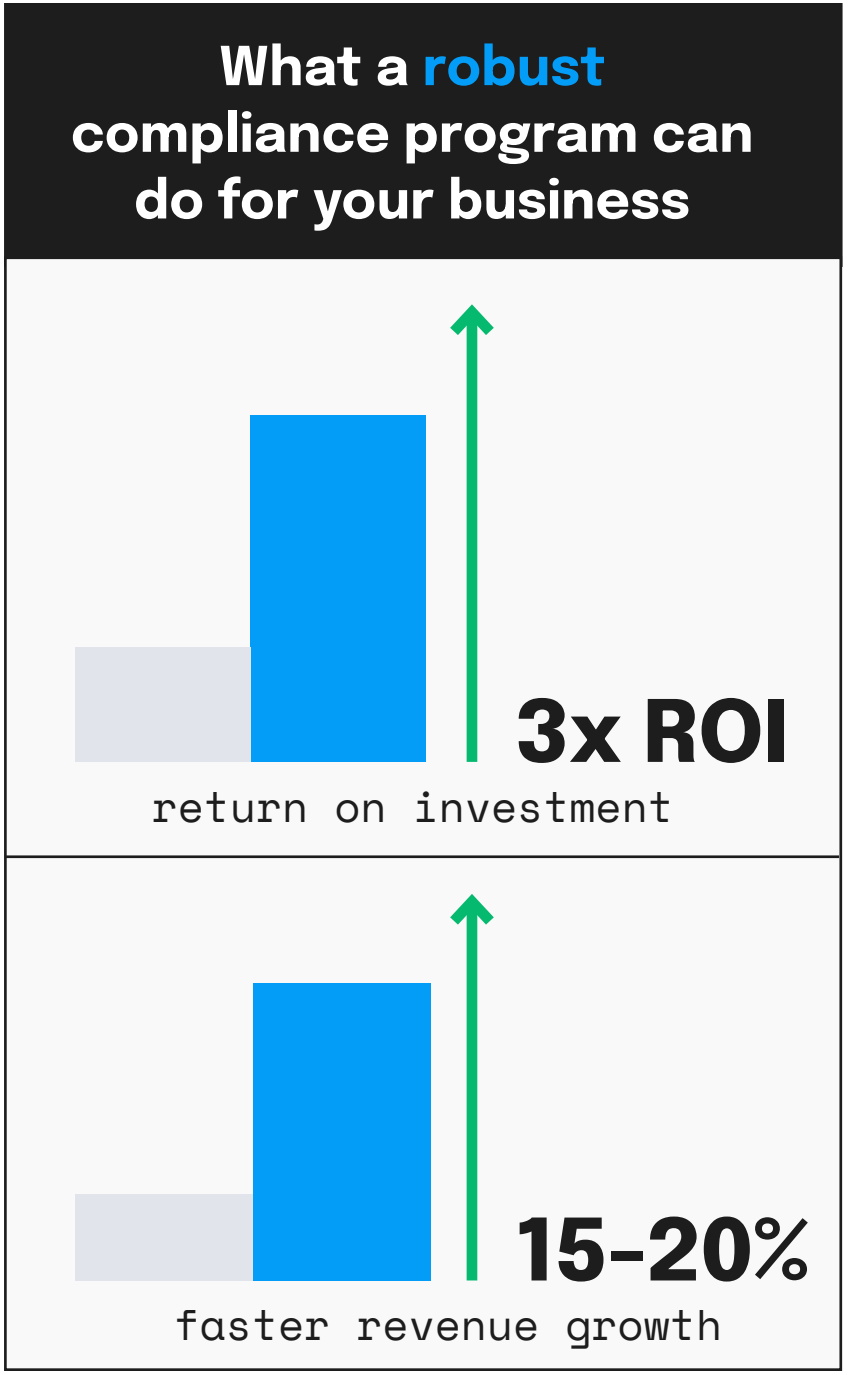
Sam Scott | CEO | Xfernet

CYBERSECURITY COMPLIANCE IS AN UNTAPPED GROWTH LEVER

Cybersecurity compliance is too often simply a box to check for regulators, clients, or auditors. However, approached strategically, compliance is a powerful business enabler. Certifications confirm your internal controls but they also demonstrate operational maturity and a commitment to protecting your customers' data. Federal frameworks like FedRAMP® or CMMC unlock multimillion-dollar opportunities in the federal and defense sectors. Similarly, HIPAA and HITRUST® are essential for doing business in healthcare, while SOC 2 is effectively a prerequisite for enterprise SaaS vendors. ISO, NIST and others are applicable across a multitude of industries. For growth-focused companies, achieving compliance with these frameworks is often essential to tapping new verticals, landing larger deals, and competing at a higher level.

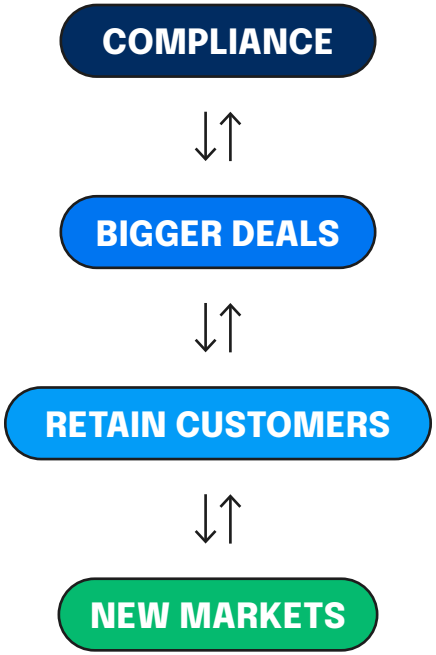
When executed well, compliance doesn't just protect–it propels.

This guide can help security and compliance leaders make informed, strategic decisions about selecting a compliance audit provider. Whether you're navigating complex frameworks, under pressure to reduce audit costs, or looking to turn certifications into a competitive edge, this resource arms you to maximize the return on your compliance investments, while reducing risk and building trust.



HOW COMPLIANCE HELPS YOU GROW, RETAIN, AND COMPETE

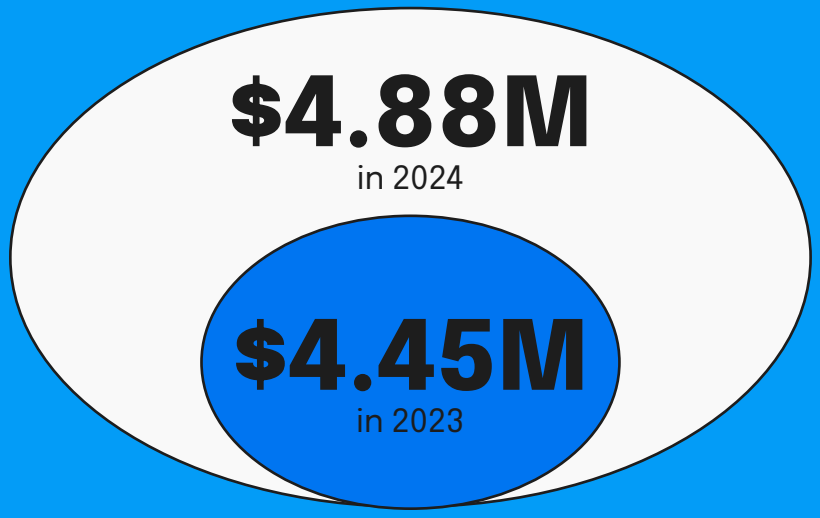
Cybersecurity and compliance are often seen as operational checkboxes, but for high-performing organizations, they represent something much more powerful: a **strategic growth lever.** Companies that embrace compliance not as a sunk cost, but as a signal of operational maturity and trust, are able to win bigger deals, enter new markets, and retain customers more effectively. By reframing compliance as a value multiplier instead of a regulatory burden, leaders can unlock compounding returns across revenue, retention, and resilience.



Certifications Open New Markets

Attaining security attestations or certifications like SOC 2, HITRUST®, or FedRAMP® satisfies buyer requirements and opens doors to new revenue streams. These credentials validate that your company meets the high standards demanded by enterprise and government buyers, accelerating procurement processes and giving your sales and marketing teams a competitive advantage. Compliance also enables geographic and vertical expansion, allowing businesses to serve regulated industries like healthcare, finance, and the public sector.

> "Compliance has never been just a checkbox. It's a growth lever.The companies that take compliance seriously win bigger deals,keep customers longer, and expand into new markets faster. Strategic compliance isn't optional, it's the foundation for trust and growth."
>
> - AJ Yawn, author of GRC Engineering for AWS



Cost of a Breach

The average cost of a data breach jumped 10% from 2023 to 2024

Costs will continue to increase, reinforcing how strategic compliance like faster identification via internal audits and GRC tools reduce breach impact.

The Retention Power of Compliance

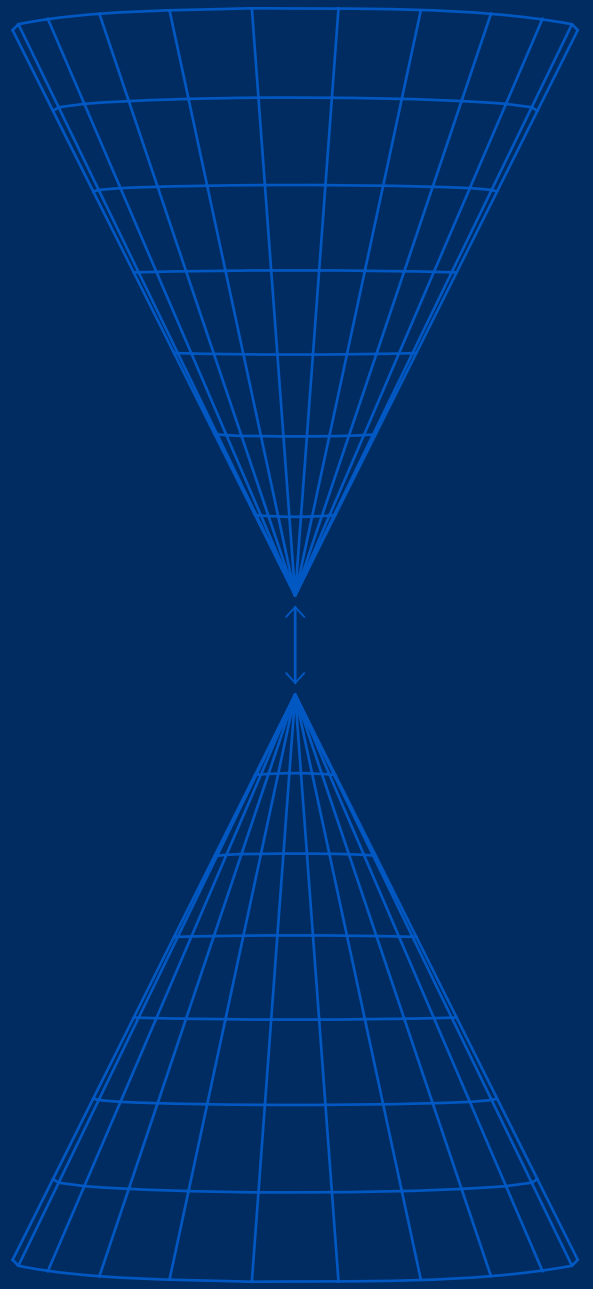
Clients carefully scrutinize their vendors' security posture, so a robust compliance program offers reassurance that you take their data seriously. When executed thoughtfully, compliance audits can also surface opportunities to enhance processes, improve service delivery, and differentiate your organization. This "trust premium" fosters customer loyalty and creates advocates who recognize and reward your commitment to security and transparency.

Mitigating Risk While Meeting Mandates

While the business case for compliance continues to grow, the regulatory requirements are evolving just as quickly. From new state privacy laws to federal mandates for critical infrastructure, organizations face increasing scrutiny. Proactive compliance management protects you from costly fines, reputational damage, and business disruption. More importantly, it empowers you to anticipate changes to the regulatory landscape.

Sharing the Benefits of Compliance Across the Business

Compliance isn't just the domain of your CISO or legal team–it's a brand asset that can be leveraged across departments. Sales and marketing teams can highlight certifications in proposals and campaigns. Procurement and customer success can point to audit reports as proof of partnership quality. Even HR and recruiting benefit by showcasing your company's commitment to security and ethics. When shared across the business, compliance becomes a tool to build credibility, influence, and growth.



Leveraging framework compliance to reduce the likelihood of a breach - by even 20% - **saves almost $900,000** (average breach cost $4.45 million).

WHAT OTHER INDUSTRY LEADERS SAY

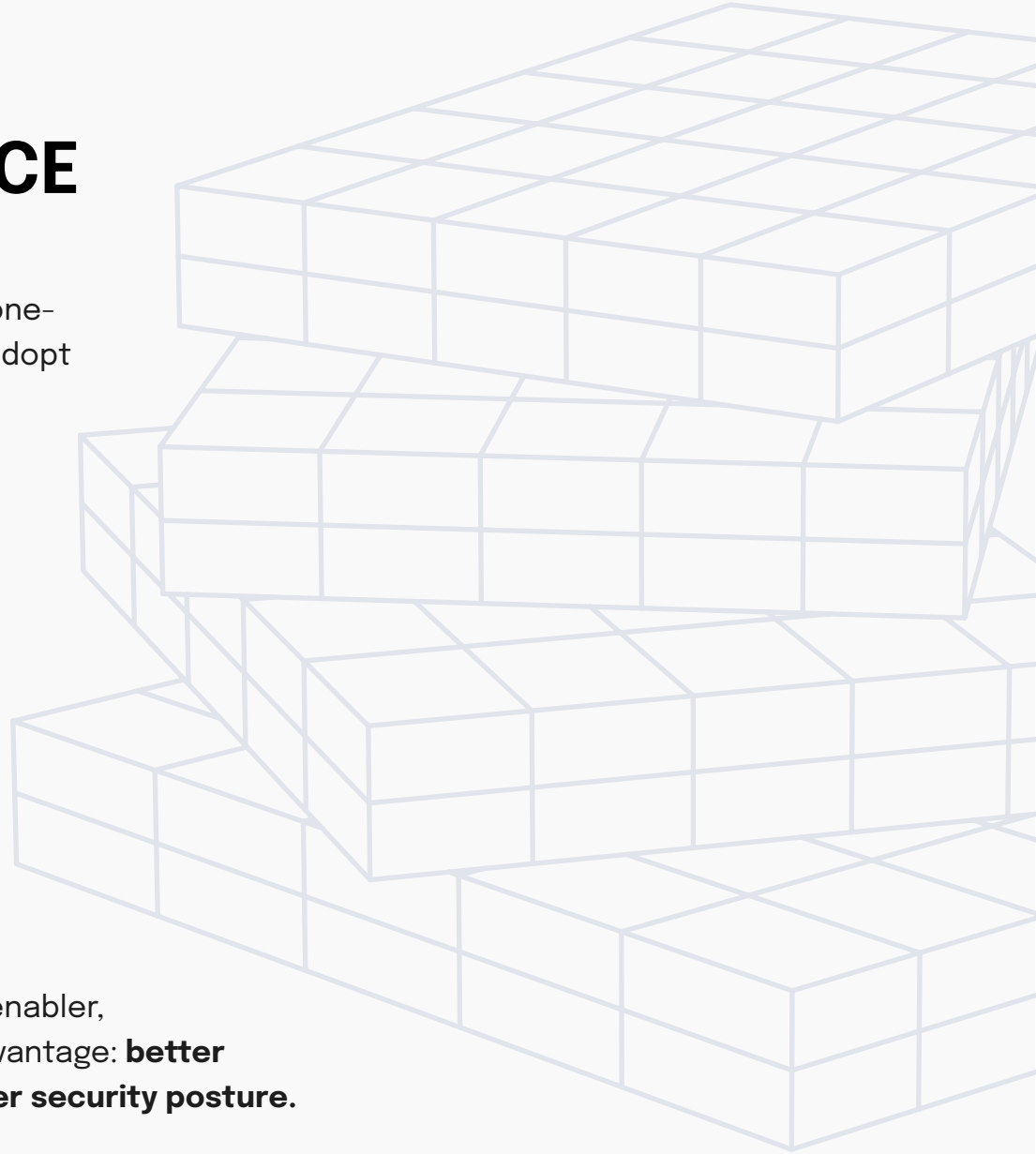
"A strong cybersecurity program should never be off-the-shelf. It should be bespoke, intentional, and built to protect your organization and your customers while meeting the regulatory and cost benefit realities of your business. Rather than chasing checkboxes, leading practice organizations build foundational security practices that are technically sound, aligned with their real-world threats. This tailored approach not only strengthens your organization's security posture but also positions cybersecurity as a business enabler to protect what matters most while building confidence with stakeholders.

Once that foundation is in place, the next step is creating a trust program that helps you clearly and credibly articulate the strengths of your cybersecurity approach to customers, partners, and regulators. Frameworks like SOC 2, ISO/IEC 27001, and HITRUST are all compliance vehicles, but they are also opportunities to demonstrate how your security program is not just present, but purposefully designed to add value and protect your customers. A good quality auditor brings your differentiated program to life through a well-articulated, high-integrity report that reflects your unique approach to trust, transparency, and protection. It's not a coincidence that companies with some of the strongest security posture partner with auditors who understand nuance and are willing to go beyond the standard to engage with the substance of your program."

Jake Nix, CEO, Riscpoint

RISCPoint

MAKING THE SHIFT TO STRATEGIC COMPLIANCE



At earlier stages, many teams operate in a reactive posture, juggling spreadsheets and responding to one-off compliance requests. Over time, organizations adopt GRC platforms or audit portals to streamline evidence collection and introduce repeatable processes. As maturity grows, so does the need for a strategic compliance ally that not only audits but provides guidance tailored to your business goals. Many companies who reach this point in their compliance maturity also bring in or lean more heavily on a CISO (fractional or full-time) to coordinate security and compliance priorities across departments.

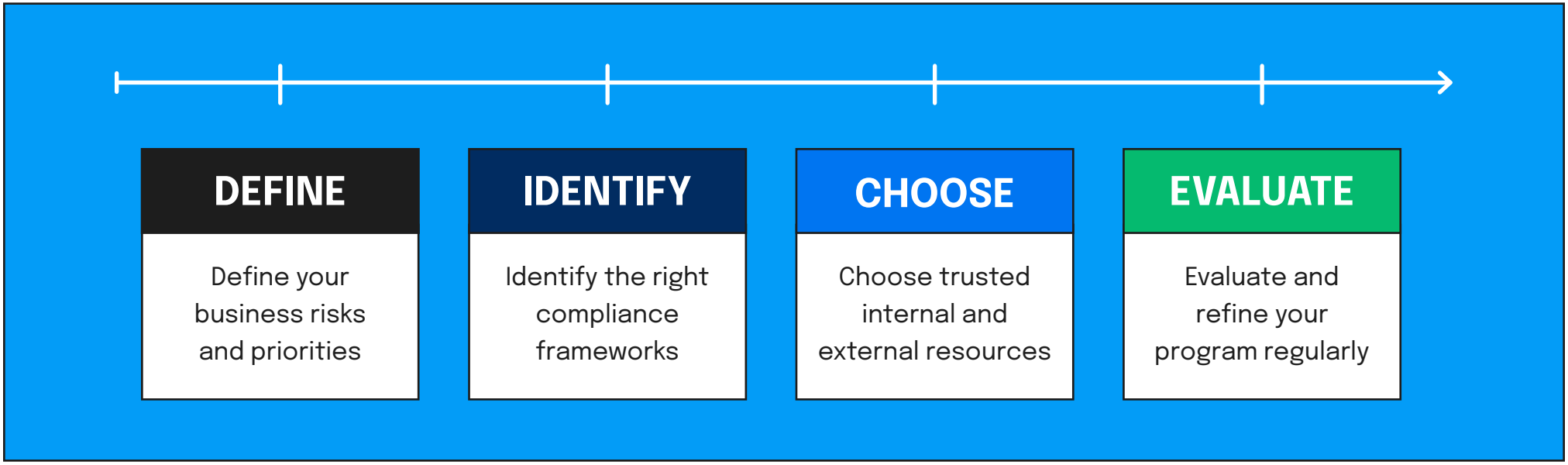
Understanding this roadmap helps other corporate leaders including CISOs, CROs, CEOs, General Counsel, and compliance leads to plan ahead. Those who treat compliance as a business enabler, rather than a defensive necessity, gain a lasting advantage: **better customer trust, faster sales cycles, and a stronger security posture.**

SECTION 02

Assessing and Advancing your Compliance Readiness

MAPPING YOUR COMPLIANCE MATURITY PATH

Every organization's path to cybersecurity and compliance maturity is different, shaped by industry demands, growth stage, and internal capabilities. Regardless of the path, the foundational elements tend to remain consistent:



Whether you're a growing SaaS company responding to your first enterprise RFP, a healthcare provider navigating HIPAA requirements, or a cloud vendor pursuing FedRAMP authorization, it's essential to recognize where you are on the journey, and where you want to go next. Understanding your maturity level helps you make smarter investments, reduce risk, and stay ahead of evolving requirements.

BENCHMARKING YOUR SECURITY AND COMPLIANCE PROGRESS

STAGE 01

Reactive & Constrained

Limited or ad hoc compliance efforts

Basic tools like spreadsheets for tracking

Responding to requirements only when prompted

STAGE 02

Operationalizing & Scaling

Implementing GRC platforms or compliance audit portals

Achieved 1–2 key attestations or certifications (e.g., SOC 2, HIPAA, ISO 27001)

Appointed a dedicated compliance lead or established a security team

STAGE 03

Strategic & Differentiated

Multiple audit cycles aligned under one program

Compliance integrated into go-to-market and growth strategy

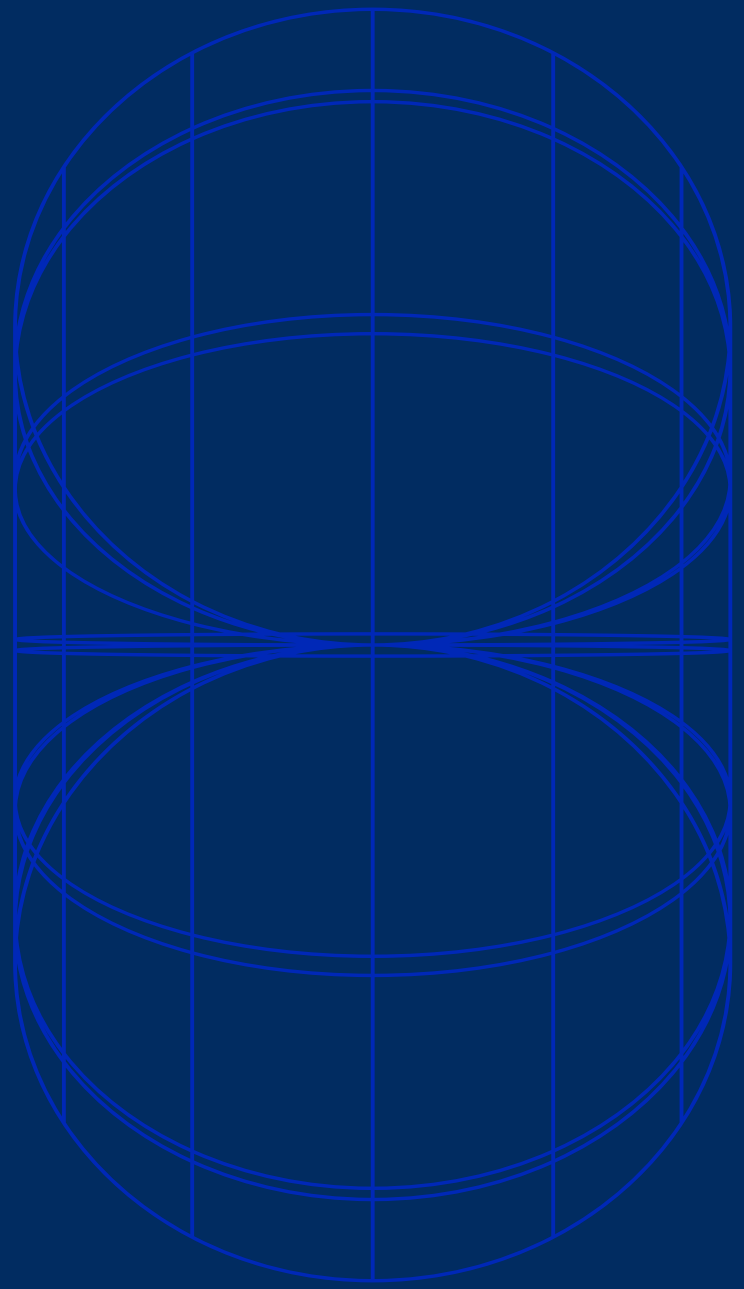
Used proactively to accelerate sales and build trust

Expanding into regulated markets (FedRAMP, HITRUST, etc.)

Leveraging certifications as a competitive advantage across the business

Internal Factors and Resources for Success

Achieving long-term compliance maturity definitely requires a capable audit firm, but it also depends on the structure, buy-in, and bandwidth of your internal team. Organizations that succeed in compliance allocate dedicated time and resources, engage cross-functional stakeholders early, and secure executive sponsorship from the outset. Whether you're working with a fractional CISO or a full in-house team, it's crucial to define roles, maintain consistent communication, and treat compliance as a strategic function, not an ad hoc project. Internal and external teams that are aligned deliver faster audits, fewer surprises, and a stronger return on the compliance investment.



If annual security incident response costs are $1 million, proper compliance could save **$200,000 to $300,000** in annual operating costs.

CYBERSECURITY COMPLIANCE GLOSSARY: FRAMEWORKS EVERY LEADER SHOULD KNOW

Below is a listing of major compliance and cybersecurity frameworks, their purpose, audit authority, frequency, and value to organizations.

TYPE	AUTHORITY	FREQUENCY	PURPOSE	IDEAL FOR
SOC 1 - Builds trust with financial auditors and clients	AICPA (American Institute of CPAs) aicpa-cima.com/home	Annual examination	Evaluates internal controls over financial reporting (ICFR)	SaaS providers that support customer financial operations
SOC 2 - Essential for enterprise deals and vendor risk assessments	AICPA aicpa-cima.com/home	Annual examination	Assesses security, availability, processing integrity, confidentiality, and privacy	SaaS, cloud, and IT service companies
ISO 27001 - Internationally recognized benchmark for security governance	International Organization for Standardization (via accredited bodies like ANAB) iso.org	Annual surveillance audit; recertification every 3 years	Establishes and maintains an Information Security Management System (ISMS)	Global organizations, particularly in tech and manufacturing
FedRAMP™ - Mandatory for government contracts; high assurance to all buyers	FedRAMP Program Management Office (PMO) / Joint Authorization Board (JAB) / Third-Party Assessment Organizations (3PAO) fedramp.gov	Continuous monitoring; initial and periodic assessments	Validates cloud service provider security for federal use	Cloud vendors selling to U.S. federal government
CMMC 2.0 - Required for contract eligibility in the defense sector	U.S. Department of Defense (via C3PAOs) dodcio.defense.gov/cmmc/About	3-year cycle with possible interim reviews	Protects Controlled Unclassified Information (CUI) in defense supply chains	DOD contractors and subcontractors

TYPE	AUTHORITY	FREQUENCY	PURPOSE	IDEAL FOR
FISMA - Demonstrates compliance with federal mandates and supports national cybersecurity objectives	U.S. Office of Management and Budget (OMB) and NIST whitehouse.gov/omb/	Annual assessments and continuous monitoring	Mandates federal agencies and contractors follow standardized cybersecurity practices	Federal agencies and organizations that handle federal information systems
GovRAMP™ (formerly StateRAMP™) - Builds trust with public sector clients and accelerates procurement in state markets	StateRAMP Governing Body (based on NIST framework) govramp.org	Annual assessments with continuous monitoring	Provides a standardized approach to cloud security for state and local government vendors	Cloud service providers seeking to serve state and municipal agencies
HITRUST® e1 / i1 / r2 - Demonstrates rigorous security and privacy controls in regulated sectors	HITRUST Alliance hitrustalliance.net	1–2 year cadence depending on assurance level	Standardized framework combining HIPAA law, NIST standards, ISO, and others	Healthcare, fintech, and service providers handling sensitive data
PCI DSS - Prevents data breaches and meets card brand requirements	PCI Security Standards Council pcisecuritystandards.org	Annual assessment for Level 1; SAQs for others	Ensures secure handling of payment card data	Retailers, payment processors, SaaS with credit card transactions
NIST 800-53 / CSF / 800-171 / AI - Recognized structure for implementing secure systems and policies	National Institute of Standards and Technology (NIST) nist.gov/cyberframework	Varies by agency or program requirement	Sets cybersecurity and risk management controls for federal and commercial use	Public sector contractors and commercial firms seeking robust security

SECTION 03

Choosing the Right Partner for the Journey

HOW TRUSTED AUDITORS STRENGTHEN YOUR SECURITY PROGRAM

In today's risk-conscious and regulation-heavy business world, compliance firms deliver audit reports, but more importantly, they guide strategic outcomes. From ensuring regulatory alignment to unlocking market opportunities, the right firm acts as both validator and advisor, helping businesses turn compliance into a lever for growth, trust, and operational resilience.

Expertise: What the Right Auditor Brings to the Table

More than issuing reports, a trusted auditor uses regulatory fluency and practical guidance to deliver strategic value. Professionals with the right deep expertise interpret complex rules, uncover operational or security blind spots and lead organizations to long term security resilience.

Watch our recent webinar to learn more about the importance of auditor-consultant relationships.

Technology and Tools Amplify Outcomes with Intelligent Integration

Integrations with client systems, especially leading GRC tools and audit portals, enable audit teams to work more efficiently with your data. When implemented properly, these tools reduce redundancy, speed up assessments, and improve confidence across stakeholders. The result is a smoother audit process and more value from your compliance investment.

THE COMPLIANCE LANDSCAPE: SOFTWARE, AUDIT FIRMS, AND LEADERSHIP

Navigating the world of compliance requires a balance of various elements. GRC software platforms, automation tools, internal or fractional CISO expertise, and dedicated compliance audit firms all play a vital role in achieving sustainable compliance excellence and driving the business forward.

Bringing Together Automation & Expertise

A strong compliance plan effectively leverages automation tools with expert audit firms. A smart tool helps streamline and centralize data collection, simplify workflows, and deliver key insights. But that's only surface-level value without the guidance of a specialized auditor. The right firm not only validates your compliance to one or more frameworks, but enhances tool implementation and delivers strategic insights.

> "Enterprise buyers scrutinize audits and policies rigorously. Quality compliance reporting is crucial – it demonstrates our ability to exceed buyer expectations and manage risks effectively."
>
> Taylor Hersom | CEO
> Eden Data

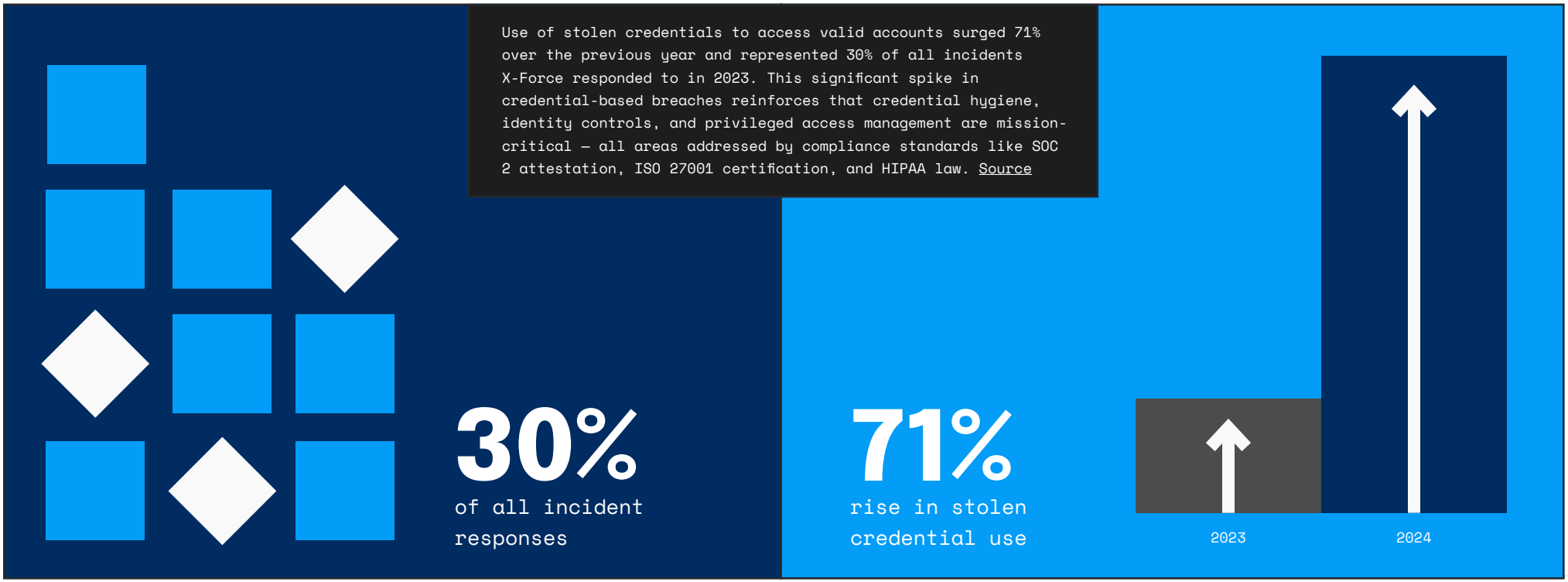
Certifications that Signal Credibility

Choosing a compliance auditor with robust certifications and accreditations is critical. A seasoned firm demonstrates credibility, firsthand understanding of the compliance process, and battle-tested expertise. Audit firms bring superior quality assurance, trusted insights, and validated methodologies, all of which are essential attributes for reliable compliance guidance.

Explore 360 Advanced's extensive list of credentials.

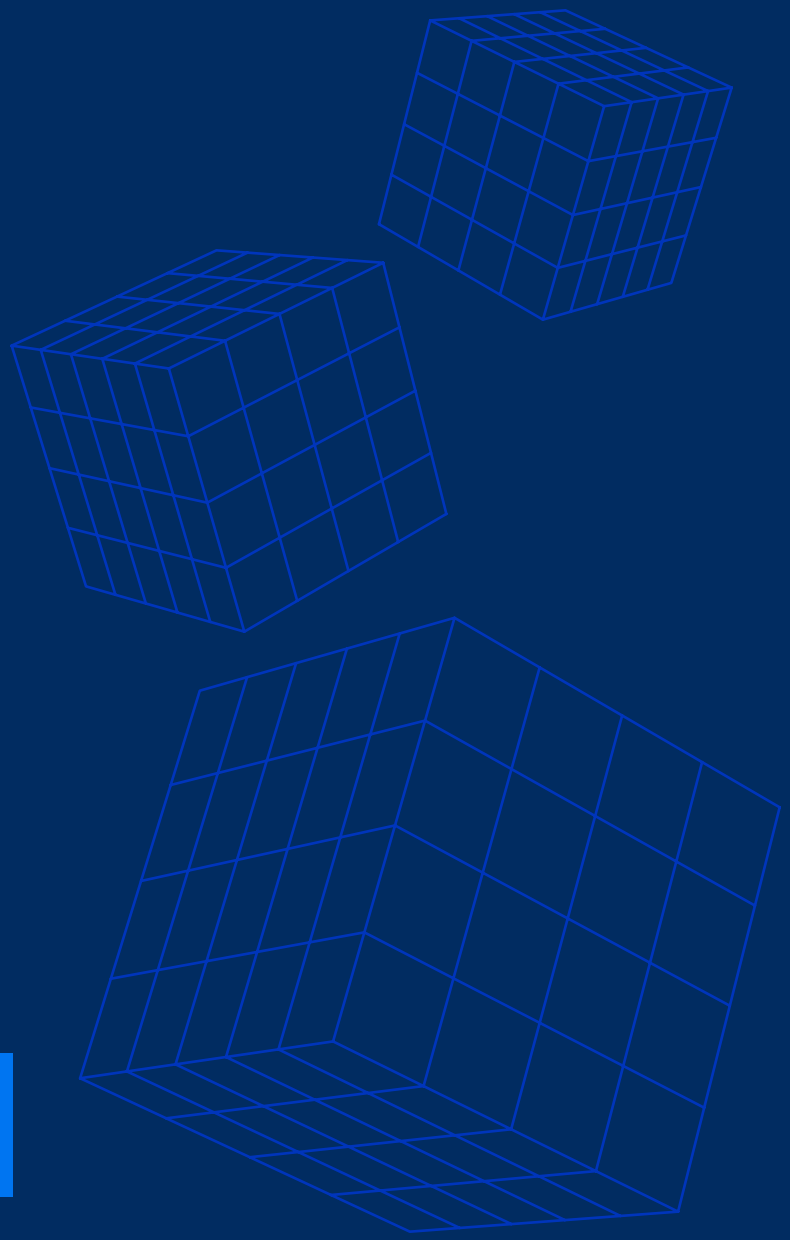
Matching Compliance Standards to Growth Goals

A quality audit firm should offer a broad range of frameworks such as SOC 2, ISO 27001, FedRAMP, PCI DSS, and HITRUST. Each framework not only supports risk management but also plays a direct role in business growth, opening doors to regulated markets, enabling faster sales cycles, and signaling trust to buyers. The right partner will help you choose and implement the standards that best support your growth strategy while minimizing compliance roadblocks.



When Does Industry Expertise Really Matter?

In highly regulated industries such as healthcare and finance, specialized compliance expertise is non-negotiable. Healthcare organizations must meticulously navigate HIPAA and HITRUST standards to protect patient data. Financial institutions face stringent requirements, so expert compliance support ensures accurate interpretation of regulatory nuances, risk mitigation, and seamless integration into industry-specific processes.



Companies with strong cybersecurity programs could see **20-30% lower premiums** on their cyber insurance policies.

Assessing Your Audit Team for Fit and Flexibility

Selecting a compliance firm involves evaluating beyond technical skills. Selection teams must also consider communication, responsiveness, and proactive advisory capabilities.

High-quality compliance reporting directly impacts insurance premiums, liability protection, and credibility during cybersecurity incidents.

Key questions to ask an audit firm you are considering:

How proactive is your guidance in regulatory changes?

What level of executive involvement can we expect?

How do you ensure quality in deliverables?

Evaluation and Selection Criteria to Choose the Right Audit Firm

CRITERIA	LOW-MARKET FIRMS	MID-MARKET FIRMS	BIG NAME FIRMS
	Budget-friendly but may lack full methodology or documentation depth to support credibility in work and reports	Often more nimble, may offer excellent value and tailored services - creditable name and work	Enterprise-focused, often bundled with broader risk consulting - creditable household name
Audit Types Offered	Limited selection, basic audits	Comprehensive SOC, HIPAA, ISO audits	Extensive audit types, global reach
Expertise & Focus	Generalist, less specialized	Specialized in key standards	Broad expertise, less personalized
Additional Services	Few or none	Advisory, readiness assessments	Extensive consulting services
Technology	Minimal tech integration	Advanced GRC integrations	Proprietary platforms and solutions
Cost	Lower cost, limited scope	Balanced cost and value	Premium pricing, higher budgets

There are dozens of firms ranging in size from a few staff to tens of thousands of employees. The options can seem endless and qualifications may blend together, making it difficult to parse what's really needed for your particular organization. The above table outlines some of the relevant information organizations learn when doing their research and hearing proposals.

Want to learn more about the Compliance and Audit Landscape? Read more here

About 360 Advanced

360 Advanced is a relationship-focused cybersecurity and compliance firm offering integrated compliance solutions customized to meet your business needs. We work with organizations that are seeking to assure data security, privacy, compliance, and processing integrity. Our open communication policy helps to facilitate a more thorough assessment of an organization's IT security.

Our clients can face challenges such as: reducing the number of audits completed each year, expanding into regulated markets or industries, and, especially, obtaining valuable feedback throughout the assessment process. Our clients are not just looking for a report, but a relationship with a trusted business advisor that can provide actionable recommendations and strategic insights.

Learn more about how 360 Advanced can streamline and increase your organization's security and compliance

info@360advanced.com

+1 (866) 479-5684