Carbide

Security and Compliance Solutions for Startups and High-Growth Companies

A BUYER'S GUIDE TO ENSURING INFORMATION SECURITY IS YOUR COMPETITIVE ADVANTAGE

Carbide

A BUYER'S GUIDE TO ENSURING INFORMATION SECURITY IS YOUR COMPETITIVE ADVANTAGE

Why Security Matters for SMBs

In the past two years, security rose to the top of technology priorities for small and medium businesses (SMBs)[1] and many have doubled their security budgets.[2] But despite the bigger investments, security remains the biggest challenge for IT admins.[3] However, security is not just an IT problem — it's a mission-critical aspect for any company because it can hinder business growth and even create barriers for successful business deals.

Many startups and high-growth companies have fragmented IT, which ultimately exposes them to a growing number of threat vectors. One of the biggest mistakes for SMBs is focusing on the wrong objectives — compliance rather than effective security.

For many organizations, risk reduction is the major driver for security programs. While reducing risk is important, security has much bigger ramifications. In fact, for many organizations it has become clear that security is a business enabler and competitive differentiator.

In an interconnected digital ecosystem, cyber attackers see SMBs as an easier entry point into larger enterprises. Consequently, 88% of enterprise leaders express concern about the resilience of SMBs within their supply chain, and 40% have experienced an attack within that ecosystem, impacting their business negatively.[4]

These enterprises are your customers and prospects — and they have elevated expectations of their vendors' security. You can't afford to overlook security from the outset and then try to meet those expectations quickly when it's time to sign a contract.

Many SMBs implement piecemeal security to support specific initiatives tactically. This approach may solve the immediate need but fails as a long-term strategy. In this ebook, we offer insights into how to create a holistic security program that continuously improves security and privacy, helping you achieve compliance and enabling the growth and success of your company.

> **Data privacy is another competitive differentiator to consider. 83% of surveyed consumers prefer to patronize businesses that prioritize data protection.[5]**

[1] *Cisco/IDG, "2020 Small Business Digital Transformation"*
[2] *Hiscox, "Cyber Readiness Report 2022"*
[3] *Jumpcloud, "IT Evolution: How IT Is Securing the Next Stage of SME Workplace Models"*
[4] *World Economic Forum, "Global Cybersecurity Outlook 2022"*
[5] *Shred-it, "Data Protection Report 2020"*

Common Misconceptions about Security and Compliance

A variety of vendor solutions promise to help you put security on autopilot. The idea sounds great in theory. In reality, these types of solutions provide a bare-minimum checklist of steps for achieving regulatory compliance. However, it's a common misconception that compliance equals security and privacy. Far from it.

Compliance plays an important role in mitigating your company's risks, but meeting compliance doesn't mean you're prepared to defend against threat actors. Regulations are simply the lowest benchmarks or basic standards that you must meet, and compliance steps don't go far enough to provide robust security in the constantly evolving threat environment.

Holistic security, on the other hand, helps you implement best practices and robust controls that support your business goals and growth. A holistic security program ensures your organization is prepared for cyberattacks and protects data privacy.

When security is done right, simplified compliance is a byproduct, even with multiple sets of requirements. By integrating a strong security and privacy program into your business from the start, you're in a much better position to comply with both current and future frameworks and regulations.

AVOIDING SECURITY DEBT

When your fast-growing company adopts a compliance-focused mindset, it creates "security debt" as the business scales. Guided by ad hoc policies and practices, security programs that cut corners eventually fall further behind, resulting in lost business opportunities. Not to mention the accumulated complexity from piecemeal efforts makes it harder to catch up.

Security debt is the implied cost of additional work, time, and finances that are a direct result of choosing the fast and easy security and privacy solutions rather than the solutions that get it done right the first time.

20% OF STARTUPS FAIL BECAUSE THEY GET OUTCOMPETED.

Let's say your SaaS solution gains high interest from potential customers. If you can't prove that your platform is secure, you will lose business from security-conscious prospects. To avoid security debt, build a solid security foundation that integrates security and privacy by design.

Six Other Common Security and Compliance Fallacies

Expect fast outcomes

You cannot gain SOC 2 or other framework compliance in a few weeks. Fast outcomes are the result of implementing bare minimum to mark off compliance checkboxes rather than creating a robust program through a thoughtful process.

Set it and forget it

You can't achieve security by putting it on autopilot. Automating certain security tasks improves efficiency, but automation doesn't mean setting up security controls and forgetting all about them. You need to be realistic about what it takes to truly boost security.

Think "one and done."

Achieving compliance once is not the end of the road. Making security and privacy part of your company's DNA prepares you to meet current and future compliance requirements. This means constantly evaluating and evolving your security methodology in response to the ever changing and growing threat landscape.

Think of security as a technology problem

Cybersecurity requires people, processes, and technology. Every person on your team — from the founders and leaders to frontline employees — shares the responsibility for maintaining security with the right tools and processes.

Grow now, secure later

Security may not feel like a priority at the beginning, but the longer you put it off, the more vulnerable your business becomes and the more difficult it will be to meet client security requirements. Your security debt will pile on and eventually you'll look for quick fixes. As the business grows, the lack of a security foundation creates bigger hurdles.

Rely on cloud vendor's security

Popular cloud platforms like Azure or AWS don't ensure your data privacy and security is taken care of. The shared responsibility model leaves all your policies up to you. While the vendor secures the infrastructure running the platform, it's your company's responsibility to use that platform securely.

Going beyond 'Checkbox' Security

Oftentimes, startups and fast-growing companies use a specific compliance framework as a starting point for their security program. Some of these frameworks are required by national or industry regulators, while others are a voluntary set of standards that businesses typically use to demonstrate their security and privacy practices to their customers.

These frameworks play an important role in ensuring you're meeting specific requirements and reducing risk. You need to understand and meet those requirements because noncompliance can result in costs such as fines and penalties.

However, falling into a framework-centric mindset is dangerous. This mindset typically translates into following the letter of the law but not the spirit. When security and privacy controls are limited to the legally required checkboxes, security debt magnifies — and business growth suffers.

Additionally, many organizations must comply with several frameworks, which generates overlapping policies and controls. If you're addressing each framework separately, the overlap is inefficient and may also create confusion for your team.

Focus on implementing robust security and data protection and privacy controls rather than the high-level framework requirements. Look for security and privacy solutions for designing a custom-tailored program that integrates all the compliance requirements into your core business processes and daily operations. A comprehensive solution will help you implement your policies, controls, and procedures; assess and manage your risks; and maintain and improve your security posture continuously.

When security and privacy controls are limited to the legally required checkboxes, security debt magnifies — and business growth suffers.

Common Regulatory and Compliance Frameworks

Factors such as industry and location impact which of the following compliance frameworks apply to your company, but building a solid foundation for security and privacy practices prepares you to meet the requirements of multiple frameworks.

FRAMEWORK	REQUIREMENTS
CCPA (California Consumer Protection Act)	State regulation requiring specific data privacy safeguards for certain businesses that collect and use California consumers' private information
CIS (Center for Internet Security) Critical Security Controls	A voluntary, prescriptive framework for best practices to help organizations prioritize and implement defenses
HIPAA (Health Insurance Portability and Accountability Act)	U.S. federal regulation requiring U.S. healthcare providers and their associates to safeguard protected health information (PHI)
ISO/EIC 27001	An internationally recognized, voluntary framework for protecting information and improving information security management systems in any industry, with compliance certified by an independent third party
GDPR (General Data Protection Regulation)	European Union's regulation requiring entities that collect and process EU subjects' personal data to apply certain privacy safeguards, regardless of the entity's geographic location
NIST 800-171 (National Institute of Standards and Technology Special Publication 800-171)	Standards for sensitive federal data protection required for suppliers and vendors of the U.S. Department of Defense and other federal agencies
PCI-DSS (Payment Card Industry Data Security Standard)	Information security standards required for organizations that handle payment card transactions
PIPEDA (Personal Information Protection and Electronic Documents Acts)	Canada's national privacy law mandating private sector entities to safeguard personal information collected, used, and disclosed in the course of commercial activities
SOC 2 (Service Organization Control 2)	A voluntary data protection and privacy standard from the American Institute of CPAs (AICPA) for SaaS and other companies, with compliance certified by an independent third-party auditor

Organizational Controls for Achieving Security, Privacy, and Compliance

Embedding security, privacy, and compliance controls into your day-to-day operations is the best way to avoid security debt and implement consistent best practices. Several industry-leading frameworks, such as NIST, CIS, and ISO 27001, provide controls that are excellent starting points. A big challenge in implementing these controls, however, is the redundancy you create when you have to meet multiple compliance requirements.

Using security and privacy best practices — rather than a specific framework — to develop controls eliminates the redundancy and streamlines multi-compliance. Based on our analysis of thousands of requirements in various regulations, industry-leading frameworks, evolving best practices, and common contractual obligations, we recommend the following 12 domains and associated controls for establishing a solid security, privacy, and compliance foundation.

1. GOVERNANCE

Enforce your governance, risk, and compliance (GRC) policies and create a process for executing action plans that address GRC issues.

2. SYSTEM AND DATA GOVERNANCE

Create a process for systems and data inventory so you can ensure security and privacy safeguards are applied. The inventory should also include third-party applications and processes that handle personal data.

3. RISK MANAGEMENT

Establish controls for managing risk, including identifying, assessing, escalating, and mitigating risks based on your determined risk tolerance.

4. INFORMATION SECURITY

Deploy critical controls to secure data:

- Network and device security (such as anomaly detection and data loss prevention) to detect and contain threats in your network and endpoints
- Vulnerability management to identify and address vulnerabilities
- Cloud security to detect and contain threats in your cloud environment
- Access management to ensure only authorized users can access sensitive data
- Encryption, both for data at rest and in transit

5. PHYSICAL SECURITY

Create controls for maintaining the physical security of your systems and data, such as access.

6. PRIVACY

Ensure data protection and privacy through practices such as limiting data collection, restricting access to sensitive data, and complying with the appropriate privacy regulations.

7. SOFTWARE SECURITY

Establish the procedures and controls for your software development operations to mitigate risks throughout the development lifecycle and ensure your systems and applications are secure by design.

8. HUMAN RESOURCES

Include security and privacy practices, as well as programs like training and awareness, across personnel-related activities such as employee screening, onboarding, performance evaluation, and offboarding.

9. LEGAL AND COMPLIANCE

Develop processes for protecting intellectual property as well as monitoring, auditing, and maintaining compliance with statutory, regulatory, and contractual requirements.

10. THIRD-PARTY MANAGEMENT

Develop processes and controls for managing risks created by vendors, business partners, suppliers, independent contractors, and other third parties.

11. INCIDENT RESPONSE

Create a plan and process for identifying, isolating, investigating, responding to, and reporting incidents, taking into consideration regulatory, contractual, and statutory requirements.

12. BUSINESS OPPORTUNITY AND DISASTER RECOVERY

Ensure you can quickly recover after a major event, restore operations, and minimize disruption.

Keep in mind that many of the individual controls address multiple privacy and security requirements across different frameworks. These recommended domains apply to any company size and maturity level and provide a universal blueprint to help you simplify controls while adopting best practices across your business. Use the domains as your roadmap for building a security and privacy program strategically, as well as for operationalizing best practices for tactical implementation.

What to Look for in a Security and Compliance Solution

Many marketplace solutions offer the ability to achieve compliance quickly. These solutions may fill your immediate need, but they don't go beyond helping you pass an audit.

Making security and privacy a part of your company's DNA takes much more than compliance software. You need to adopt a security-first mindset — and that means avoiding a patchwork of controls and practices that leave gaps in your defenses and privacy protections. If you had to start out with a simple compliance solution by necessity, now is the time to think strategically, before your security debt catches up with you.

Building out a sustainable, resilient security and privacy program relies on having the right tools. A holistic solution can help you not only pass audits but also build and maintain robust policies, procedures, and controls. A comprehensive solution will also help you continuously boost your security posture, manage risks and create a culture of security within your organization.

Knowing where to start their security journey is a big challenge for startups and high-growth businesses that are committed to it. The first step is to set realistic expectations about the process. Think about what it took to create a vision for your startup and bring that vision to reality. Just like creating great products, embedding security into your business DNA won't happen in two weeks, but there are solutions that can accelerate the process while doing it the right way.

Moving from a tactical to a more programmatic approach takes work, especially when your resources are limited. An accessible solution will eliminate much of the frustration along that journey.

Just like creating great products, embedding security into your business DNA won't happen in two weeks, but there are solutions that can accelerate the process while doing it the right way.

Top 5 Criteria for Evaluating Your Options

COMPREHENSIVE PLATFORM

A strong security program has three pillars: people, processes, and technology, and these components intertwine and rely on each other. A comprehensive security platform that allows you to manage all three aspects in tandem greatly improves your program's effectiveness. Look for features such as policy management, asset tracking, and employee awareness training along with a platform that easily integrates with your existing software and programs. Integration will optimize processes like evidence collection and multi-framework compliance.

ABILITY TO OPERATIONALIZE SECURITY

To embed security into your company's DNA, you need a consistent way of integrating security and privacy best practices into your daily operations across all your teams through policies, controls, and procedures. Consider a platform that enables you to easily create policies, helps you design an implementation plan, and tracks progress such as policy sign-off and awareness training.

STREAMLINED AUDITING AND REPORTING

With robust security practices ingrained into your business, proving compliance to regulators, prospects, customers, and other stakeholders should not be a time-consuming and complicated process. Look for features such as evidence collection and custom reporting.

SECURITY POSTURE MANAGEMENT

Your attack surface constantly grows, threats evolve, and your team changes. Maintaining good security posture in such a dynamic environment requires continuous monitoring. A platform with features such as a security dashboard and insights provides the tools you need for sustaining and improving posture.

EXPERT SUPPORT

Limited in-house security expertise is a barrier for startups, and outside experts are an invaluable resource. Look for an experienced vendor that can be your expert partner, offering guidance and support in addition to tools that help define your program and fast-track your compliance initiatives.

Carbide

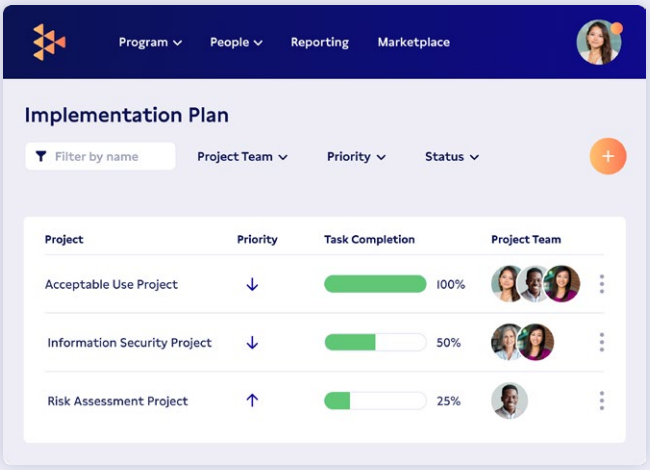
Scale your business without incurring security debt

At Carbide, we understand from first-hand experience how security drives growth for startups. Founders Darren Gallop and Laird Wilton had a successful SaaS startup that was quickly gaining customers around the world. Demonstrating security and data compliance to potential customers, however, was a hurdle — resulting in delayed deal closings and the loss of a six-figure opportunity to land a Fortune 500 customer.

Carbide was born to fill a market gap for a comprehensive, affordable tool that helps other fast-moving startups design and execute a complete information security program.

Built to streamline multi-compliance, Carbide delivers the tools, resources, and expertise for designing, reviewing, implementing, validating, and evolving your security program over time.

Strong security, data privacy, and compliance are critical components for startup success in a hypercompetitive business world. Carbide helps you operationalize security from the ground up, turning security into a business enabler rather than an obstacle.

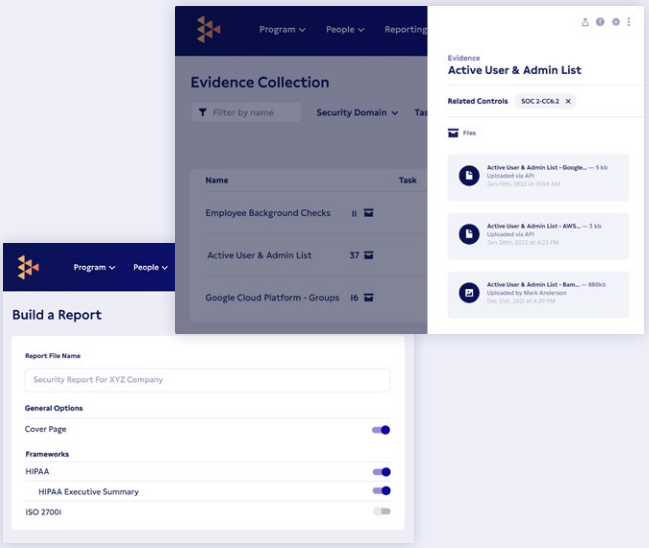


THE CARBIDE ENTERPRISE-CLASS INFORMATION SECURITY PLATFORM CAN HELP YOU:

- Accelerate the development and validation of their security and privacy program
- Extend their team's capacity through automation and in-platform guidance
- Minimize their security debt with a program built for agility and sustainability

Carbide

Top features of the Carbide platform include:



CUSTOM POLICY BUILDER

Generate 20+ policies customized to your business environment on day one.

ORGANIZATIONAL CONTROLS

Map your security and privacy requirements and implementation tasks to your specific needs using our 12 Security and Data Protection Domains.

ASSET MANAGER

Track and manage assets and their associated risks.

SECURITY AWARENESS TRAINING

Assign, manage, and track employee training progress.

BUSINESS CONTINUITY PLAN BUILDER

Create a robust business continuity plan to boost your resilience.

TECHNICAL INTEGRATIONS

Connect your critical business systems to the platform for automatic evidence collection.

RISK ASSESSMENT MATRIX

Understand and manage your company's security risk.

Carbide

Make cybersecurity your competitive differentiator

Connect with Carbide to learn how our platform and team of security and privacy advisors can help you create a holistic security program that supports your business growth.

Frameworks & Regulations We Support

"Just 6 months after implementing Carbide, we closed deals with multiple Fortune 500 companies. Without Carbide, we could never have accomplished what we have in such a short amount of time."

Boris Lipchin, CEO @ BRIO

"Carbide keeps track of all of the details, so I don't have to."

Stephen F, COO @ TeneraCare

"Carbide allows you to become compliant in multiple frameworks at once and it maps out common controls among different frameworks so you do not need to repeat efforts anywhere. It makes getting multiple certifications easy."

Marie J, Security Solutions Engineer @ Trava

Read More Carbide Reviews