WHITE PAPER

Regulatory Compliance: Bridging Compliance and Cybersecurity

A Comprehensive Approach to Third-Party Risk Management

SecurityScorecard

Table of Contents

Navigating Cybersecurity in a Complex Regulatory Landscape

Organizations are under mounting pressure to improve their cybersecurity posture and keep pace with evolving regulations and an ever-expanding network of third-party suppliers in 2025. Government and oversight bodies continue to expand the scope and specificity of regulations aimed at safeguarding sensitive information and critical infrastructure. Yet despite significant focus and investment, many enterprises struggle to keep pace.

The challenge is not simply the volume of regulations, but the fragmentation, overlap, and dynamic nature of these regulations which often span across multiple jurisdictions and industries. As organizations expand from on-premises systems to the cloud and onboard new vendors, their attack surface continues to expand, making compliance a moving target. Security and risk leaders must align internal controls to regulatory requirements while staying ahead of an evolving threat landscape.

In order to meet this challenge, organizations need to move beyond static compliance checklists toward a more dynamic, risk-informed approach. Organizations increasingly need the ability to generate meaningful, quantifiable metrics that demonstrate both cybersecurity maturity and regulatory alignment—not just within the organization, but also across the third-party ecosystem. These metrics must not only reflect current posture but also provide clear evidence of how organizations are proactively identifying, prioritizing, and mitigating risk.

The Strategic Imperative: Real-Time Risk Intelligence for Compliance and Security

Several converging trends are reshaping how forward-looking organizations approach regulatory compliance, including vulnerability prioritization and context-aware risk ranking. At the same time, regulatory bodies are building increasingly contextualized and robust frameworks for ensuring security controls are in place. Chief Information Security Officers (CISOs), governance, risk, and compliance professionals, and third-party risk managers must juggle a series of crucial considerations in order to align with compliance frameworks:

Vulnerability Prioritization

- Regulatory bodies are increasingly moving away from point-in-time audits and are calling for continuous assessment of vulnerabilities.
- Simply identifying vulnerabilities is no longer sufficient. Organizations must prioritize them based on context, such as exploitability, business criticality, and threat actor intent. This shift reflects a broader recognition that not all vulnerabilities are created equal, and that risk must be addressed based on potential impact.

Risk-Based Ranking and Reporting

- Regulations now include evidence-based frameworks for ranking vulnerabilities based on business risk. Will inadequate Identity and Access management (IAM) controls lead to credential theft? Are current Network Access Control (NAC) provisions still allowing hackers to steal key intellectual property (IP)?
- Risk-based ranking can include maintaining visibility over legacy systems, understanding how bad actors can exploit these systems if left unpatched and taking action to prevent such exploitation.
- Auditors want to know what controls are in place and why security teams decided on those particular controls. Security teams should be prepared to define and demonstrate how they measure effectiveness.

Expanding Digital Footprints

- An organization's digital footprint is no longer limited to internal assets. Organizations must also monitor and understand assets that are exposed to the open internet and those that partners, suppliers, and vendors own or maintain. Both internal and external assets play critical roles in shaping an organization's overall risk profile.
- Regulatory reviews increasingly consider third-party access to sensitive data, including intellectual property, customer information, Personally Identifiable Information (PII), and Protected Health Information (PHI). Understanding and managing this extended footprint is now a core element of an effective compliance strategy.

Continuous Monitoring

- Regulatory frameworks are beginning to reflect what cybersecurity practitioners have long known: Static controls and point-in-time assessments are insufficient in the face of constantly evolving threats and growing attack surfaces.
- Continuous monitoring, attack path validation, and real-time threat intelligence are essential for ensuring internal, third-party, and nth party environments are equipped to protect, detect, and remediate expeditiously.

Regulatory compliance can no longer be treated as a check-the-box exercise. Organizations should approach compliance and cybersecurity in a continuous, collaborative manner, focusing on real-time data, risk prioritization, and cross-business and third-party collaboration. It must be embedded into broader cyber risk governance frameworks. This means adopting a continuous, integrated approach—where compliance, security, and third-party risk management operate in tandem.

Understanding the Landscape: Regulations vs. Mandates

Before we dive deeper into details on the regulations themselves, a nuanced understanding of regulatory constructs is essential.

Regulations are often industry-specific laws or standards that mandate protection of digital assets—such as the Health Insurance Portability and Accountability Act (HIPAA) or Payment Card Industry Data Security Standard (PCI DSS). Non-compliance can lead to substantial penalties, reputational demand, and legal liability.

Mandates such as General Data Protection Regulation (GDPR) in the European Union (EU) or the United States Securities and Exchange Commission (SEC) cybersecurity disclosure rule are typically broader in scope and jurisdiction. They have legally-enforceable requirements that transcend industries.

Focused on North America, the European Union (EU) and Great Britain, we will cover several industry-specific regulations and mandates that organizations must incorporate into their security workflows and touch on what they encompass, relevant penalties, and how they tie into Third-Party Risk Management (TPRM).

Navigating Regulatory Compliance in Financial Services: A Catalyst for Better Risk Management

The financial services industry sits at the crossroads of trust, technology, and regulation. As digital interdependence grows, regulators on both sides of the Atlantic are intensifying their scrutiny—not just of how firms manage internal cybersecurity, but how they govern risk in their entire cybersecurity ecosystem, including third-parties' security postures.

New and evolving mandates like the SEC's cybersecurity disclosure rules, New York's 23 NYCRR 500 (also known as Part 500), the EU's Digital Operational Resilience Act (DORA), and the United Kingdom's PS21/3 all share a common theme: Cyber resilience is not optional and third-party risk is central to compliance.

For financial institutions, these regulations do more than create new requirements. They also signal a shift in accountability. Boards and executive leadership are now expected to demonstrate that they have assessed cyber risk and that they can monitor, prioritize, and mitigate it across their supply chains quickly and transparently.

Keeping pace with these regulatory changes presents both a challenge and an opportunity. Organizations that pay meticulous attention to these have the chance to operationalize compliance through smarter third-party cyber risk practices; reducing exposure, building institutional trust, and preventing reputational damage along the way.

SEC Rules	Securities and Exchange Commission (SEC) Rules Rules on Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure by Public Companies
WHAT IS IT?	On July 26, 2023 the Securities and Exchange Commission (SEC) announced that it adopted rules requiring registrants to disclose material cybersecurity incidents. The change requires annual disclosures of material information regarding cybersecurity risk management, strategy, and governance. The SEC also adopted rules requiring foreign private issuers to make comparable disclosures. Foreign private issuers are those with less than 50% of their outstanding voting securities directly or indirectly held by US residents, among a few other requirements. The new rules also add Regulation S-K Item 106, which will require registrants to describe their processes for assessing, identifying, and managing material risks from cybersecurity threats. The rule also requires organizations to describe the material effects or reasonably likely material effects of risks from cybersecurity threats and previous cybersecurity incidents. **Three Key Tenets of SEC Rules:** • One of the SEC's primary missions is to protect investors • The SEC has specifically called out vendor breaches as a risk. Healthcare, financial services, and fintech companies are highly targeted, and cybercriminals are targeting their supply chains • Severe civil penalties apply to companies that minimize impacts in disclosures
COVERED ENTITIES	Public companies must disclose how they manage, govern, and protect their company against cyber risk.
RELEVANCE TO TPRM	Healthcare, financial services, and fintech firms have become prime targets for hackers given that their supply chain and third-party vendors are numerous, diverse, and maintain or have access to highly sensitive information
PENALTIES	The SEC is applying civil penalties to companies for allegedly misleading disclosures. For instance, on October 22, 2024, the SEC charged four companies for allegedly disseminating materially misleading disclosures regarding cybersecurity incidents. The SEC charged that these companies learned between 2020 and 2021 that the likely perpetrator of the SolarWinds supply chain attack had also attacked and infiltrated their systems, but in their respective public disclosures at the time, each company "negligently minimized" the impacts. **Example:** • One of the companies agreed to a $4 million civil penalty. • The SEC also charged that company with disclosure controls and procedure violations. • The other companies paid between $990,000 and $1 million in civil penalties each.

NYDFS	NYDFS Department of Financial Services 23 NYCRR Part 500 Amended Part 500
WHAT IS IT?	The NYDFS (New York State Department of Financial Services) Cybersecurity Regulation (23 NYCRR Part 500), originally enacted in 2017, is designed for financial services companies to better protect customer information as well as information technology systems. New York amended Part 500 of the regulation in 2020 and 2023. The updates are intended to address the fact that bad actors increasingly have tools that allow them to launch attacks easily and the fact that companies can more easily implement measures to improve their security posture. Senior management must take this issue seriously, take responsibility for the organization's cybersecurity program, and file an annual certification confirming compliance with these regulations by April 15 each year. **Three Key Tenets of DFS** • The rule notes that "each covered entity shall implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers" • Organizations can be fined for improper / inadequate implementation of security policies and procedures • Examples of covered entities include mortgage companies, other lenders, state-chartered banks, and more.
COVERED ENTITIES	Covered entities include, but are not limited to, partnerships, corporations, branches, agencies, and associations operating under, or required to operate under, a license, registration, charter, certificate, permit, accreditation, or similar authorization under the Banking Law, the Insurance Law, or the Financial Services Law. The Banking law pertains to banks, trust companies, savings banks, credit unions, and other financial institutions. The Insurance Law addresses the insurance industry, including insurers, brokers, and agents. The Financial Services Law provides the framework for the DFS to continually update the regulation and include a broader range of financial services.
RELEVANCE TO TPRM	Each covered entity shall implement written policies and procedures designed to ensure the security of information systems and nonpublic information that are accessible to, or held by, third-party service providers. It covers entities that provide services to the covered entity and those that maintain, process or otherwise are permitted access to nonpublic information through its provision of services to the covered entity.
PENALTIES	The regulation mandates penalties for non-compliance, with fines ranging from $1,000 per violation to potentially millions for egregious violations. There may be daily penalties of up to $250,000 for ongoing non-compliance. **Example:** The NYDFS fined a popular online payment system $2 million in 2025 for failing to ensure the proper implementation of its cybersecurity policies and procedures in violation of the regulation in 2022. The organization failed to utilize qualified cybersecurity personnel to perform and oversee the performance of core cybersecurity functions and failed to use Multi-Factor Authentication (MFA).

DORA	DORA The European Union's Digital Operational Resilience Act
WHAT IS IT?	The DORA regulation is intended to help financial institutions across the EU guard against and mitigate threats. It applies to covered entities as of January 17, 2025. The EU's intention is to institute a consistent approach to cyber resilience across all EU countries. The regulation encompasses five "pillars" related to security controls including: • Information and Communication Technology (ICT) Risk Management • ICT-related Incident Management, Classification and Reporting • Digital Operational Resilience Testing • Managing of ICT Third-Party Risk • Information-Sharing Arrangements The regulation states that "financial entities shall manage ICT third-party risk as an integral component of ICT risk within their ICT risk management framework." DORA mandates that organizations report supply chain breaches within as little as four hours and proactively address at-risk suppliers. **Three Key Tenets of DORA** • Pillar 4 specifically calls out the management of third-party risk • Penalties can be severe. European Supervisory Authorities (ESAs) can impose fines of up to two percent of total annual worldwide turnover (revenue) for firms that don't comply with DORA. • The EU's intention is to institute a consistent approach to cyber resilience across all EU countries.
COVERED ENTITIES	Financial sector entities including banks, investment firms, and insurance companies. DORA also covers: • Cloud service providers • Data reporting services • Insurance and reinsurance entities • Cryptocurrency-asset service providers • Centralized securities depositories • Crowdfunding service providers
RELEVANCE TO TPRM	Managing third-party risk is specifically called out in the regulation within its five "pillars."
PENALTIES	European Supervisory Authorities (ESAs) can impose fines of up to two percent of total annual worldwide turnover (revenue) for firms that don't comply with DORA. **Example:** As the regulation went into effect on January 17, 2025, there are no known examples yet available.

Healthcare's Expanding Risk Landscape: Compliance in the Age of Digital Care

As healthcare delivery becomes increasingly digitized, the sector faces growing scrutiny over how it protects PHI across complex, often opaque, digital ecosystems. Regulations such as HIPAA in the United States and the GDPR in the EU are no longer just about internal cybersecurity best practices. They now demand that healthcare organizations take responsibility for the security maturity of their vendors, service providers, and digital partners.

The stakes are uniquely high in health services. Unlike other sectors, healthcare organizations hold highly sensitive, personal data that, if compromised, can have direct consequences for patient safety, privacy, and public trust. At the same time, these organizations often rely on a wide network of third parties—from cloud platforms and billing processors to specialized telehealth providers—each of which represents a point of vulnerability.

HIPAA	**Health Insurance Portability and Accountability Act of 1996 (HIPAA)** Security Rule, as amended by the Health Information Technology for Economic and Clinical Health (HITECH) Act Compliance Enforcement section Security Law section
WHAT IS IT?	HIPAA governs the protection of patients' sensitive health data. The Security Rule establishes measures to protect electronic PHI (ePHI). The Security Rule works in concert with the Breach Notification Rule and the privacy standards established in HIPAA's Standards for Privacy of Individually Identifiable Health Information. HIPAA's privacy standards are commonly referred to as the Privacy Rule. The Breach Notification Rule, which operates as part of the HITECH Act, directs entities to notify the Department of Health and Human Services (HHS), and in some cases, the public in the case of a data breach incident. **Three Key Tenets of HIPAA** • The security rule specifically protects patients' sensitive health data. • Any organization that has access to ePHI is a covered entity. • Penalties can be severe. The highest recorded fine was issued to a large health insurer for $16 million.
COVERED ENTITIES	There is a vast array of people and entities must maintain HIPAA compliance: • **Providers** such as doctors, clinics, psychologists, dentists, chiropractors, nursing homes, and pharmacies that transmit information in an electronic form in connection with a transaction for which HHS has adopted a standard. • **Health plans** are also covered entities. This includes health insurance companies, Health Maintenance Organizations (HMOs), company health plans, and government programs that pay for health care, such as Medicare, Medicaid, and military and veterans' health care programs. • **Healthcare clearinghouses** including entities that process nonstandard health information they receive from another entity into a standard format (such as a standard electronic format or data), or vice versa also must comply. • **Business associates** must also comply with administrative, physical, and technical safeguards of the Security Rule, as well as its policies, procedures, and documentation requirements.
RELEVANCE TO TPRM	Third parties, including business associates, must comply with HIPAA. Any organization that has access to ePHI is a covered entity. Knowing vendors' security postures and their likelihood of HIPAA compliance is critical to protecting PHI and maintaining compliance.
PENALTIES	HHS' Office for Civil Rights (OCR) is responsible for enforcing the Privacy and Security Rules. HIPAA penalties can be substantial. **Example:** The highest recorded fine was issued to a large health insurer, for $16 million. HHS updates a list of settlement agreements here.

GDPR	General Data Protection Act https://gdpr-info.eu
WHAT IS IT?	The EU's General Data Protection Regulation (GDPR) lays down rules regarding the processing of personal data and rules relating to the free movement of personal data. It protects fundamental rights and freedoms of "natural persons" and, in particular, their right to the protection of their personal data. GDPR requires that personal information be collected for specific and legitimate purposes and not further processed in a manner that is incompatible with those purposes. It requires that organizations implement technology and processes to continually protect personal information. It impacts persons and organizations in the United States and around the world. While it is intended to protect the personal data of people within the EU, if data is being processed by an organization in the United States, then the GDPR applies. **Three Key Tenets of GDPR** • It requires that organizations implement technology and processes to continually protect personal information. • It protects the personal data of people who reside in the EU. • Any organization that allows third parties to access or maintain personal data must determine those vendors' cybersecurity practices and risk profiles.
COVERED ENTITIES	The regulation applies to organizations in and outside of the EU that engage in "any transfer of personal data which are undergoing processing or are intended for processing." A stipulation is that the personal data is of a person who resides in the EU.
RELEVANCE TO TPRM	Businesses around the globe often rely on third parties to process customers' personal data. Any organization that allows third parties to access or maintain this kind of data must determine those vendors' cybersecurity practices and risk profiles on a continuous basis to draw down on risk and make better decisions about which vendors to use.
PENALTIES	Each member state provides for one or more independent public authorities to be responsible for monitoring the application of this Regulation. Each member state determines penalties as well. For especially severe violations, fines can be up to €20 million, or up to four percent of their total global turnover of the preceding fiscal year, whichever is higher. For less severe violations, fines of up to €10 million or up to two percent of its entire global turnover of the preceding fiscal year, whichever is higher, can be assessed. **Examples:** • In 2023, Ireland fined a large technology company €1.2 billion for transferring data from EU users to the United States. The Irish Data Protection Commission also fined the same organization €390 million in 2023 for issues related to subsidiaries. • Ireland also fined a different technology company €345 million in 2023.

Retail Under Pressure: Securing Payment Data in an Expanding Threat Landscape

Retailers remain a top target for cybercriminals and must remain constantly vigilant against hacking incidents. A single breach can erode consumer trust, damage brand equity, and trigger steep financial penalties. With widespread adoption of e-commerce, point-of-sale systems, and third-party vendors, safeguarding payment data in retail has become an expanding and complex operation.

The Payment Card Industry Data Security Standard (PCI DSS) 4.0 raises the bar for protecting cardholder data across today's modern retail ecosystem. The updated standard, which took effect in March 2025, emphasizes continuous risk management, greater transparency, and enhanced third-party oversight—not just technical controls. This means retailers must move beyond annual compliance checklists and embrace real-time, continuous validation, especially when it comes to the vendors and platforms that touch the cardholder data environment (CDE).

For retailers, compliance is no longer just about avoiding fines, it's about protecting brand reputation, sustaining customer loyalty, and proving to partners and regulators that cyber risk is being actively managed across the full supply chain. Third-party risk management isn't a side requirement under PCI DSS 4.0, it's now central to a retailer's overall security and compliance strategy.

PCI DSS	Payment Card Industry Data Security Standard 4.0 https://www.pcisecuritystandards.org/
WHAT IS IT?	PCI-DSS is a global standard for technical and operational requirements designated to protect payment data. **Key Tenets of the Current Version, 4.0** • Organizations must meet standards of payment industry to protect customer cardholder data from illegitimate access and misuse by implementing several security controls. • It promotes the use of a continuous process to maintain and enhance security profile. • New, enhanced validation methods must be employed.
COVERED ENTITIES	The Cardholder Data Environment (CDE), which is comprised of: • System components, people, and processes that store, process, and transmit cardholder data (CHD) and/or sensitive authentication data (SAD) • System components that may not store, process, or transmit CHD/SAD but have unrestricted connectivity to system components that store, process, or transmit CHD/SAD • System components, people, and processes that could impact the security of the cardholder data and/ or sensitive authentication data. • System components include network devices, servers, computing devices, virtual components, cloud components, and software.
RELEVANCE TO TPRM	PCI DSS Requirement 12.8 applies to third-party service providers (TPSPs). Businesses or merchants must monitor the PCI DSS compliance status of all their TPSPs in accordance with Requirement 12.8, including TPSPs that have access to the business' CDE (cardholder data environment), manage in-scope system components on their behalf, and/or can impact the security of their CDE. Organizations must apply due diligence, have appropriate agreements in place, identify which requirements apply to the customer (the merchant) and which apply to the TPSP, and monitor the compliance status of TPSPs at least annually.
PENALTIES	Fines are tiered based on the number of card transactions. Fines of $100,000 per month are common for companies that process over 6 million card transactions per year and that have been non-compliant for several months. Smaller organizations that process fewer than 20,000 card transactions per year will pay fines closer to $5,000 per month. Fines can increase or decrease based on the number of transactions and time spent out of compliance. **Examples:** • The U.K.'s Information Commissioner's Officer fined a UK-based airline $229 million in 2017 for a breach affecting 500,000 customers. • A US-based retailer agreed to pay $18.5 million in a multi-state settlement after a 2013 data breach exposed over 41 million customers' payment information. • A US-based department store company agreed to a $40.9 million settlement with banks after exposing more than 94 million customer accounts between 2005 and 2006.

Frameworks, Standards, and Questionnaires

Frameworks and Standards

Regulations and mandates can provide both incentives and consequences—enhanced security for compliance, penalties for non-compliance—while cybersecurity frameworks and standards provide the structure organizations need to turn strategy into action.

Frameworks help enterprises translate complex risk landscapes into clear and repeatable processes. They enable teams to identify, assess, and mitigate threats to critical digital assets with consistency and confidence. Widely adopted frameworks such as the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0 and International Organization for Standardization and the International Electrotechnical Commission's ISO/IEC 27001 help align internal controls with industry best practices and regulatory expectations.

SecurityScorecard maps to these and other leading frameworks, helping organizations embed cyber risk management into day-to-day operations and demonstrate resilience in a measurable, scalable way.

Cybersecurity standards can establish clear, measurable expectations for performance, security, and compliance. They serve as fixed reference points that ensure organizations and their third parties consistently align with industry-recognized benchmarks. Adhering to standards such as Service Organization Controls (SOC) 2 and ISO/IEC 27002 enable organizations to demonstrate due diligence, reduce risk exposure, and build trust with regulators, partners, and customers.

SecurityScorecard supports alignment with these standards by continuously monitoring controls across ecosystems and providing mapped evidence to simplify audits and strengthen accountability.

NIST Cybersecurity Framework (CSF) 2.0

The NIST Cybersecurity Framework (CSF) 2.0 provides guidance to industry, government agencies, and other organizations to manage cybersecurity.

Before the CSF's introduction in 2014, the cybersecurity community lacked a common language or framework for critical infrastructure cybersecurity. After NIST introduced the framework, there was a default, unified mechanism in place for the audit and governance, risk, and compliance communities to reference. NIST announced CSF 2.0, an update to the framework, in 2024.

Organizations should use CSF and supplementary NIST updates and documents to help understand, assess, prioritize, and communicate cybersecurity risks.

It outlines guidance on managing cybersecurity risks for industry, government agencies, and other organizations. It provides a taxonomy of cybersecurity outcomes that organizations of any size or cybersecurity posture can use to assess their security practices.

The framework provides a roadmap based on measuring risk and security posture that gives shared nomenclature for cybersecurity professionals, auditors, assessors, and CISOs to work from common ground to develop better security outcomes.

CSF 2.0 places special emphasis on the importance of governance and supply chains. It gives CISOs a way to further justify the return on investment (ROI) of cybersecurity budgets if they can map solutions and tools to an industry standard.

The framework has several implications for businesses and cybersecurity professionals that manage supply chain risk:

- The governance of cybersecurity supply chain management section 3 (GV.SC-03) notes that cybersecurity supply chain management should be integrated into cybersecurity and enterprise risk management risk assessments and improved processes.
- The governance of cybersecurity supply chain management section 7 (GV.SC-07) notes the risks posed by a supplier, their products and services, and other third parties should be understood, recorded, prioritized, and monitored. It notes that businesses should also respond to these risks.

ISO 27001 Framework

ISO 27001, which was formally adopted in 2005, establishes a framework for all organizations to establish, implement, operate, monitor, review, and maintain an Information Security Management System (ISMS).

Organizations that follow the framework should have an easier time complying with GDPR, the Network and Information Systems Directive (NIS), and other key frameworks or mandates. ISO 27001 describes specific activities and controls to secure information and information systems, manage risks, and meet legal and contractual security requirements. It also provides organizations of all sizes guidance on how to continually improve an ISMS.

Three principles of information security enshrined in ISO 27001 are confidentiality, integrity, and availability. Applying these principles is essential for organizations of any size; Ensuring that only the right people have access to certain information, that data is protected against manipulation or deletion, and that information is available when necessary is a crucial step for most cybersecurity professionals.

SOC2

Service Organization Controls (SOC) 2 compliance is a voluntary standard that ensures organizations protect client data. It's based on the Trust Services Criteria, a set of principles developed by the American Institute of Certified Public Accountants (AICPA).

Compliance with SOC 2 can:

- Ensure organizations have the right processes to protect client data
- Demonstrate to customers an organization prioritizes data security
- Help organizations gain a competitive edge

Cloud providers, Software-as-a-Service (SaaS) vendors, IT managed services firms, and other organizations that provide web-based service are all considered covered entities and need to comply with the standard. Service organizations and Information Systems-as-a-Service (ISaaS) providers rely on SOC2.

SOC2's five categories of Trust Services Criteria with accompanying security practices or considerations are:

1. **Security**
   Information and systems are protected against unauthorized access, disclosure, and damage that could compromise availability, confidentiality, integrity and privacy of the system. Organizations that address this can use:
   - Firewalls
   - Intrusion detection
   - Multi-Factor Authentication (MFA)

2. **Availability**
   Information and systems are available for operational use. Organizations that address this can use:
   - Performance monitoring
   - Disaster recovery
   - Incident handling to manage breaches, cyber attacks, and other adverse events

3. **Confidentiality**
   Information is protected and available on a legitimate need to know basis. Applies to various types of sensitive information. Organizations that address this can use:
   - Encryption
   - Access controls
   - Firewalls

4. **Processing Integrity**
   System processing is complete, valid, accurate, timely and authorized. Organizations that address this can use:
   - Quality assurance
   - Process monitoring
   - Adherence to principles as a way to document system processing

5. **Privacy**
   Personal information is collected, used, retained, disclosed and disposed according to policy. Privacy applies only to personal information. Organizations that address this can use:
   - Access control
   - MFA
   - Encryption

ISO 27002 Standard

ISO 27002 is an international standard for security control implementation for organizations across industries to improve their cybersecurity posture within their ISMS

It provides best practices and security control objectives centered on access control, cryptography, human resource security, and incident response. By following ISO 27002 guidelines, companies can take a proactive approach to protecting critical information from unauthorized access and loss.

\Organizations across multiple industries use ISO 27002, as it is an international standard. There is no certification to ISO 27002 itself, rather it supports compliance with ISO 27001.

ISO/IEC 27002 is a versatile standard that can help organizations both improve security practices and provide helpful signals to other entities, customers, and business stakeholders. It can:

- Provide businesses with best practices to protect sensitive data and to encourage trust among stakeholders, clients, and partners.
- Signify a proactive approach to minimizing the risks of unauthorized access, data breaches and financial and brand damages.
- Assist organizations in complying with regulatory data protection mandates.

Questionnaire Support: How SecurityScorecard Supports Cybersecurity Compliance

Security questionnaires are essential for validating vendor compliance, but the traditional process can be fragmented, manual, and difficult to scale. Managing hundreds of responses across frameworks and regulations can slow down risk assessments and place an incredible strain on internal teams. Security questionnaires empower users to cut through the “questionnaire noise,” and reduce the time and effort it takes to assess third and fourth-party vendors so your team can focus on high-risk findings, not paperwork.

SecurityScorecard makes it easier to stay on top of compliance by mapping your organization’s performance against key cybersecurity regulations and frameworks, including SOC2, ISO 27001, and NIST CSF 2.0. Our platform highlights gaps and tracks alignment, giving teams a clear, structured view of where they stand and what needs attention to ensure regulatory compliance. At the core of all these standards is a consistent requirement: Robust third-party risk management, supported by continuous monitoring and regular vulnerability assessments.

To further reduce compliance burdens, SecurityScorecard streamlines the questionnaire process. Whether you’re working with NIST CSF 2.0, the Standardized Information Gathering (SIG) Lite, or other frameworks, we correlate responses across multiple standards.This makes it easier to reuse validated answers and ensure consistency. Combined with trusted, data-backed insights, our approach helps you meet regulatory expectations with greater ease.

Some of the questionnaires that SecurityScorecard has integrated include:

- Standardized Information Gathering Questionnaire (SIG) Lite 2025
- Standardized Information Gathering Questionnaire (SIG) Core 2025
- NIST CSF 2.0
- CIS (Critical Security Controls) - V8
- CMMC Level 2 - v2
- HIPAA Compliance Checklist
- HiTrust CSF

Reduce Risk and Meet Compliance Requirements with SecurityScorecard

SecurityScorecard's MAX significantly lowers the overall cost of managing vendors and business partners. MAX, a managed service, allows customers to dramatically expand the number of vendors they monitor, reduce risk, **and improve compliance**. When SecurityScorecard resolves a critical cybersecurity issue, it is resolved for the entire ecosystem, demonstrating the power of collective defense.

SecurityScorecard helps organizations in four key areas as it relates to compliance and third-party risk management.

- Risk Management
- Legal and Financial Protection
- Operational Efficiency
- Enforceable Due Diligence

Risk Management

Proof of control efficacy helps identify and mitigate security risks, reducing the likelihood of data breaches and cyberattacks. Implementing proactive security measures that protect critical assets is a best practice towards meeting compliance requirements. Leveraging SecurityScorecard, you can demonstrate compliance, provide evidence of a risk assessment program with insights into the cybersecurity risk profile of your organization and its third parties.

Cybersecurity ratings are generated by objectively monitoring an organization's security hygiene and tracking whether its security posture is improving or deteriorating over time. Ratings are invaluable for vendor risk management programs, meeting third-party risk management regulatory requirements, determining risk premiums for cyber insurance, credit underwriting, financial trading decisions, M&A due diligence, executive-level reporting, and for self-monitoring.

Legal and Financial Protection

Meeting regulatory compliance requirements can help your organization avoid hefty regulatory fines and reinforce proof of security posture that can help shield your organization from legal and financial penalties.

Enforceable due diligence

You can integrate Data Forensics and Incident Response (DFIR) capabilities to augment your security team's capabilities with SecurityScorecard on demand.

Operational Efficiency

Implementing standardized frameworks such as NIST CSF 2.0 can enhance operational efficiency by streamlining security practices and ensuring consistent application across the organization, which is crucial for maintaining a robust security posture. Implementing well-regarded frameworks requires accurate, real-time assessment and identification of material risks from cybersecurity threats, including those from third parties.

Adopting a framework, backed up with timely, structured data derived from standards-driven guidelines, can ensure that risk management is up-to-date, well-documented, and capable of addressing the dynamic nature of cybersecurity threats. It also can help feed overall compliance and security efforts. SecurityScorecard aids operational efficiency by providing:

- **Executive reporting:** Demonstrate the value of your security program to boards and business leaders with SecurityScorecard's actionable data and reporting capabilities
- **Cyber risk reporting:** SecurityScorecard's Cyber Risk Reporting Center interprets and shares findings by providing business context appropriate for various stakeholders.
- **Cyber risk quantification:** By using SecurityScorecard's cyber risk quantification you can drive risk management strategies and mitigation efficiency.

Demonstrating Compliance, Enhancing Security, and Protecting Trust

Meeting regulatory requirements is no longer a standalone objective, it's part of a broader mandate to build trusted, cyber-resilient organizations. As regulatory expectations become more sophisticated, they increasingly reward continuous monitoring, evidence-based risk prioritization, and proactive third-party oversight.

Forward-looking organizations are evolving their compliance strategies to align with these expectations. They are operationalizing frameworks, automating assessments, and integrating real-time risk intelligence into how they manage both internal and third-party cyber risk. By doing so, they not only meet audit requirements, they also drive meaningful improvements in security posture and resilience.

This shift calls for tools and practices that enable organizations to map regulations to controls, monitor risk across the digital ecosystem, and prioritize threats based on context and business impact. Those with visibility across their vendor landscape—combined with the ability to respond to risks in real time—are better positioned to demonstrate compliance, reduce exposure, and build trust with customers, regulators, and partners.

Ultimately, the path forward lies in aligning compliance and cybersecurity efforts—not through complexity, but through connected insights, continuous assessment, and collaboration across the supply chain. In doing so, organizations can transform compliance from a burden into a real strategic advantage.

To learn more and create your free account, visit SecurityScorecard.com

ABOUT SECURITYSCORECARD

Funded by world-class investors, including Evolution Equity Partners, Silver Lake Partners, Sequoia Capital, GV, Riverwood Capital, and others, SecurityScorecard is the global leader in cybersecurity ratings, response, and resilience, with more than 12 million companies continuously rated.

Founded in 2013 by security and risk experts Dr. Aleksandr Yampolskiy and Sam Kassoumeh, SecurityScorecard's patented rating technology is used by over 25,000 organizations for enterprise risk management, third-party risk management, board reporting, due diligence, cyber insurance underwriting, and regulatory oversight.

SecurityScorecard makes the world safer by transforming how companies understand, improve, and communicate cybersecurity risk to their boards, employees, and vendors. SecurityScorecard achieved the Federal Risk and Authorization Management Program (FedRAMP) Ready designation, highlighting the company's robust security standards to protect customer information, and is listed as a free cyber tool and service by the U.S. Cybersecurity & Infrastructure Security Agency (CISA). Every organization has the universal right to its trusted and transparent Instant SecurityScorecard rating. For more information, visit securityscorecard.com or connect with us on LinkedIn.

SecurityScorecard

SecurityScorecard.com
info@securityscorecard.io