GUIDE

Cybersecurity Compliance for Highly Regulated Industries

Strategies to simplify and accelerate your compliance journey and avoid the pitfalls along the way.

November 2024

How prepared is your organization for the wave of new cyber regulations?

Compliance in highly regulated industries such as healthcare, finance, and defense is more than a checkbox; it's a journey.

Innovative firms know compliance isn't just essential for security—it's a source of competitive advantage.

This guide, tailored for companies operating in highly regulated industries, provides practical tips and key actions to help you prepare for, achieve, and maintain compliance in fast moving markets. We will cover key frameworks and regulations, including **ISO 27001, SOC 2, NIST 800-171, CMMC, HIPAA, PCI DSS, and GDPR**.

70% of leaders agree that cybersecurity compliance is getting harder and that a simpler, more strategic approach is needed. [1]

A few **big questions** should be considered as you prepare for compliance:

- Which standards do we need to comply with? Is it multiple standards?
- How prepared are we to meet them... and take advantage of them?
- Are we audit ready?
- Do we have the internal resources needed to do this?

Read on to get the answers to these questions. Learn how to simplify and accelerate your compliance journey, while avoiding the pitfalls along the way.

KEY CHALLENGES

Regulatory Changes
Staying informed and adapting to evolving regulations requires constant vigilance. Missing updates can result in non-compliance and costly business impacts.

Lack of Expertise and Time
Gaps in resources, time, and expertise will likely stall the development and implementation of robust security programs.

Financial Implications
Non-compliance leads to wasted spending, fines, and reputational damage, potentially impairing growth, and market trust.

Integration Across Departments
Ensuring a unified compliance approach across all departments is difficult. Silos lead to inconsistencies and vulnerabilities, weakening overall security posture.

Effective Risk Assessments
Thorough risk assessments require deep knowledge of threat landscapes and internal vulnerabilities. Translating assessments into prioritized, actionable strategies requires alignment on risk tolerance and appetite.

Incident Response and Recovery
Coordinating roles and regularly updating response plans to match evolving threats is complex. Without clear strategies, recovery efforts become disjointed, prolonging damage and increasing recovery times.

[1] 2023 Thomson Reuters Risk & Compliance Survey Report

Understanding and Managing Risk Tolerance

Business leaders and cybersecurity professionals often have different perspectives on risk.

Boards and senior executives expect a mature and defensible cybersecurity program, in accordance with organization-specific risk tolerance levels. Risk tolerances are set collaboratively across the business with guidance from technology leaders, in alignment with strategic objectives and the regulatory environment.

With a shared understanding of acceptable risk, your organization can navigate cybersecurity complexities with more confidence. This proactive approach ensures robust security that closely aligns to business priorities.

Aligning Compliance with Business Objectives

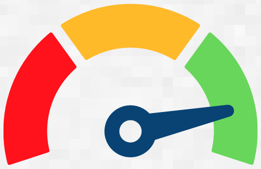
Business leaders may accept certain risks to drive business goals, while cybersecurity professionals aim to minimize those risks. This divergence can create challenges in aligning security efforts with business objectives. Security leaders must clearly link cybersecurity risks to specific business outcomes to drive home their strategic impact.

Integrate Compliance with Business Strategy: Spend time understanding the business strategies and explaining how technical issues relate to enterprise risk. Ensure that compliance initiatives are aligned with the organization's strategic goals.

Communicate Impact: Translate cybersecurity risks into business terms to highlight their impact on business outcomes.

Gain Stakeholder Buy-in: Ensure adequate resource allocation, and shared prioritization.

Using a Risk Register



A risk register helps overcome these challenges by providing a structured approach to identify, assess, and mitigate risks. It enhances visibility and ensures systematic resource allocation. Risk registers also play a key role in continuous compliance by providing a tool for ongoing risk assessment and adjustment.

To create an effective risk register:

- **Identify Risks Precisely**: Collaborate across the organization to pinpoint potential security threats.
- **Assess Severity Continually**: Evaluate the impact and likelihood of each risk and adjust over time.
- **Mitigate and Monitor:** Develop action plans for high-priority risks and regularly update the register.
- **Regular Updates:** Continuously review and update risk registers to ensure they accurately reflect the current risk landscape and evolving organizational context.

Choosing the Right Framework

Security compliance isn't just a checkbox; it's a strategic journey. Achieving and maintaining compliance with key frameworks starts with knowing which are most relevant to your business.

Which standards do we need to comply with? Is it multiple standards?

The plethora of different cybersecurity standards and frameworks can be overwhelming, leaving businesses unsure of where to begin or which to choose. Selecting the right framework depends on your industry, the type of data you handle, and your specific regulatory requirements. Often, companies need to comply with multiple standards, which can be complex and resource-intensive. Gaining certification of compliance demonstrates a commitment to managing cyber risks effectively and provides verifiable evidence of robust security practices and controls. However, certification is not the only measure of cybersecurity maturity.

NIST 800-171 (Framework)

This framework provides guidelines for protecting controlled unclassified information in non-federal systems and organizations. It is crucial for contractors working with the U.S. government.

CMMC (Framework)

The Cybersecurity Maturity Model Certification (CMMC) is a unifying standard for implementing cybersecurity across the defense industrial base, encompassing various maturity levels that reflect the extent of an organization's cybersecurity capabilities.

HIPAA (Regulation)

The Health Insurance Portability and Accountability Act (HIPAA) sets the standard for protecting sensitive patient data. Organizations dealing with protected health information (PHI) in healthcare must comply with HIPAA's stringent security measures.

ISO 27001 (Framework)

An international standard for managing information security, ISO 27001 provides a systematic approach to managing sensitive company information, including people, processes, and IT systems. It is relevant across multiple industries, especially those handling sensitive data.

SOC 2 (Framework)

A framework for managing data based on five "trust service principles"—security, availability, processing integrity, confidentiality, and privacy. It is particularly relevant for technology and SaaS companies.

PCI DSS (Contractual Obligation)

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment, applicable to the financial sector.

GDPR (Regulation)

The General Data Protection Regulation (GDPR) is a regulation in EU law on data protection and privacy, mandating strict data protection requirements and granting individuals more control over their personal data. It affects any company handling the data of EU citizens, regardless of the industry.

Assessing Risk and Maturity

Navigating the complexities of cybersecurity compliance requires careful preparation and coordinated action. By focusing on key areas such as risk assessments, skill gaps, and financial planning, your organization can build a solid foundation for achieving compliance.

Effective Risk Assessments

Thorough, human-led risk assessments, enhanced by automation, provide comprehensive clarity on the current threat landscape. This understanding is crucial for prioritizing mitigation efforts, allocating resources efficiently, and developing a clear action roadmap for continuous compliance. It also strengthens the business case for necessary resource allocation.

Key Steps

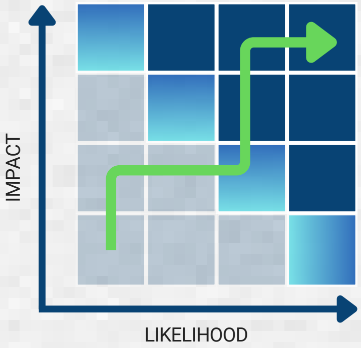
1. **Identify Assets and Risks:** Catalog all critical assets and potential risks associated with them.
2. **Analyze Threats and Vulnerabilities**: Assess the likelihood and impact of various threats exploiting identified vulnerabilities.
3. **Prioritize Risks**: Rank risks based on their potential impact and likelihood to allocate resources effectively.
4. **Develop Mitigation Strategies:** Create action plans to address prioritized risks, ensuring they are tailored to your organization's specific context.

Assessing Security Maturity

Seiso uses a methodology that scores an organization's security risk compliance and security program based on the following criteria:

- ✓ Performed with rigor and sophistication.
- ✓ Integrated into the organization's standard risk management process.
- ✓ Provides the appropriate level of cost effective reduction of cybersecurity risk.
- ✓ Consistent across organizational units, stabilized, predictable, and focused on continuous improvement.

Assessments inform adaptive compliance roadmaps tailored to business context.



Implementation Steps

Implementing effective cybersecurity measures involves a combination of administrative, technical, and physical controls. These steps ensure comprehensive protection and compliance with regulatory standards.

Implementation Step	Key Actions
Administrative Controls Implementing administrative controls is a foundational step in achieving compliance. These controls involve policies, procedures, and processes that govern security practices within your organization.	1. **Policy Development**: Create comprehensive security policies that align with industry standards and regulatory requirements. 2. **Training and Awareness**: Conduct regular training sessions to ensure all employees understand and adhere to security policies. 3. **Access Controls**: Establish and enforce strict access controls to ensure only authorized personnel can access sensitive information.
Technical and Physical Controls Technical and physical controls include software, hardware, and physical security measures designed to secure your systems and premises.	1. **Network Security**: Implement encryption for data at rest and in transit, deploy firewalls, and use intrusion detection systems to monitor and protect your network. 2. **Maintenance and Updates**: Regularly update and patch all software and hardware to protect against vulnerabilities. 3. **Access and Environmental Controls**: Install access control systems like key card entry and biometric scanners, use surveillance systems in sensitive areas, and equip facilities with fire suppression and climate control systems.
Documentation and Review Maintaining comprehensive documentation and conducting regular reviews are crucial for ensuring ongoing compliance and identifying areas for improvement.	1. **Policy and Procedure Documentation:** Keep detailed records of all security policies, procedures, and processes. 2. **Regular Audits:** Conduct regular internal and external audits to assess compliance and identify gaps. 3. **Continuous Improvement**: Use audit findings and other feedback to continuously improve your security program.

Incident Response and Recovery

Minimize the impact of cyber incidents like data breaches and service disruptions by defining roles, establishing response teams, implementing backup plans, and engaging experts for swift, organized responses and recovery, ensuring business continuity.

Implementation Step | **Key Actions**

Coordinating Roles and Responsibilities

Effective incident response requires clear role coordination. Each team member must understand their specific duties to ensure a swift, organized response.

1. **Define Roles**: Clearly document roles and responsibilities, ensuring everyone knows their specific tasks during an incident. This clarity helps avoid confusion and overlaps during critical moments.
2. **Communication Plan:** Establish a detailed communication plan that outlines how information will be shared during an incident. Effective internal and external communication ensures all stakeholders are informed and coordinated, minimizing response times and potential damage.

Establishing a Security Operations Centers (SOC)

A dedicated incident response team, or security operations center (SOC), is crucial for managing cyber incidents effectively. Equip this team with necessary tools, resources, and expertise to ensure comprehensive protection.

1. **Assemble a Team**: Form a dedicated SOC team with members from various departments. Ensure a mix of security analysts, threat hunters, and network engineers to cover all aspects of incident response.
2. **Equip the Team**: Provide the SOC with the latest tools and technologies, including Security Information and Event Management (SIEM) systems, intrusion detection systems, and threat intelligence platforms. These tools help in monitoring, detecting, and responding to cyber threats in real-time.
3. **Conduct Regular Drills and Training**: Conduct regular incident response drills and tabletop exercises to ensure the team is prepared for real-world scenarios. Continuous training is vital to maintain readiness as the threat landscape evolves.

Incident Response and Recovery (continued)

Minimize the impact of cyber incidents like data breaches and service disruptions by defining roles, establishing response teams, implementing backup plans, and engaging experts for swift, organized responses and recovery, ensuring business continuity.

Implementation Step	Key Actions
Implementing Alternative Support and Service Protocols During a cyberattack, implementing alternative support and service protocols is essential to minimize disruption and ensure continuity of critical operations.	1. **Backup Systems**: Implement robust backup systems for critical data and processes, with regular tests and updates. 2. **Redundant Communication**: Establish redundant communication channels, such as secure email systems and dedicated communication apps, to maintain uninterrupted communication during an incident. Regularly test to confirm reliability. 3. **Contingency Plans**: Develop comprehensive contingency plans for critical business functions, detailing alternative processes and resources. Include predefined roles and responsibilities. Regularly update to address new threats and operational changes.
Hire External Experts to Fill Gaps and Outsource Security Management External cybersecurity experts provide fresh insights and recommendations to enhance your incident response plans. They bring specialized track records to help you avoid costly mistakes. Experts can help conduct thorough risk assessments, and develop robust response strategies, ensuring compliance with evolving regulations.	1. **External Assessments:** Experts can conduct thorough evaluations of your incident response plans, including vulnerability assessments and penetration testing to identify and mitigate weaknesses effectively. 2. **Ongoing Support:** Engage experts for ongoing support and updates to your response strategies. Continuous monitoring and real-time threat intelligence can help adapt your defenses to evolving threats. 3. **Expert Training:** Utilize external experts to train your internal teams on the latest incident response techniques and best practices.

Continuous Compliance and Improvement

Continuous monitoring and regular assessments keep your defenses agile and responsive, enabling you to pre-empt threats, pivot swiftly, and maintain compliance. A proactive stance not only mitigates risks but also reinforces trust and reputation.

Implementation Step	Key Actions
Continuous Monitoring and Vulnerability Assessments Stay ahead of threats and regulatory changes with continuous monitoring and regular vulnerability assessments. This proactive approach ensures real-time tracking and pre-emptive threat prevention, keeping your defenses agile and responsive.	1. **Deploy Monitoring Tools and Automate Alerts**: Implement SIEM systems and other tools for continuous network activity tracking. Set up alerts for unusual activities to ensure swift, proactive responses. Customize alerts to reduce false positives and prioritize critical threats, integrating tools for comprehensive security. 2. **Routine Scans**: Regularly scan all critical systems to identify security gaps using automated tools and manual techniques. 3. **Prioritize and Remediate**: Rank vulnerabilities by impact and likelihood. Develop and implement remediation plans promptly, verifying fixes through follow-up scans.
Internal Audits and Feedback Mechanisms Implement Internal audits and feedback mechanisms that drive continuous improvement by identifying weaknesses, incorporating lessons learned, and adapting to new challenges.	1. **Schedule Audits**: Conduct regular audits, both scheduled and surprise, to review policies, procedures, and controls. This helps uncover hidden issues and ensures compliance. 2. **Audit Teams and Documentation**: Form cross-department audit teams. Document findings thoroughly and develop actionable plans. Track implementation and reassess to ensure improvements are sustained. 3. **Incident Reviews and Employee Feedback**: Perform post-incident reviews to identify lessons and improvement opportunities. Encourage anonymous employee feedback and regularly review suggestions to implement feasible enhancements.

Compliance as a Strategic Advantage

Leverage compliance as a strategic advantage to differentiate yourself, build trust, and ensure long-term success in an evolving regulatory landscape.

A strong record of meeting stringent vendor requirements can help you win new business by showing clients you prioritize security. Choosing a compliant vendor helps avoid regulatory gaps and maintain business continuity. This commitment across the supply chain builds trust and distinction in competitive markets, enhances your reputation, opens new markets, attracts investment, and drives growth.

Key Actions:

- **Transparency**: Clearly communicate compliance achievements and security measures to stakeholders through reports, website updates, and marketing materials.
- **Certifications**: Obtain and display certifications from recognized standards like ISO 27001, SOC 2, and HIPAA to reinforce your commitment to security.
- **Customer Communication**: Regularly update clients on your compliance status and new security measures.
- **Compliance Across Borders**: Ensure your security practices comply with international regulations to facilitate entry into new markets.
- **Marketing**: Incorporate compliance achievements into marketing campaigns and sales pitches to showcase your commitment to security.

Common Pitfalls to Avoid

Most companies struggle with cybersecurity compliance because they do it infrequently or for the first time.

Inexperience leads to common pitfalls that can result in data breaches, regulatory fines, loss of customer trust, delays, rework, and wasted resources.

Experts like Seiso specialize in compliance, avoiding pitfalls through best practices and a certified team. They bring expertise, early issue detection, and tailored solutions to keep your operations secure. This proactive approach ensures long-term security, compliance, and resource efficiency. Don't risk costly consequences—partner with Seiso to protect your organization.

Pitfalls	How to Avoid Them
Not Tailoring Frameworks to Business Context Frameworks provide a common language for managing cybersecurity risks but must be tailored to fit your organization's unique context.	**Adapt and Integrate Multiple Frameworks**: Adjust frameworks to align with your organization's specific requirements and risks, ensuring agility and continuous improvement.
Inadequate Documentation ncomplete or outdated records can lead to unclear security practices and failed audits.	**Maintain Comprehensive Records**: Document all security policies, procedures, and controls, keep thorough audit trails, and ensure easy accessibility for relevant personnel.
Failure to Implement Continuous Monitoring CPeriodic audits alone are not sufficient to identify and mitigate ongoing threats.	**Deploy and Review Monitoring Tools**: Implement SIEM systems for ongoing tracking, set up automated alerts, and regularly review outputs to refine detection.
Insufficient Resource Allocation Underfunding security efforts can undermine your organization's ability to maintain robust measures.	**Align Compliance to Business Objectives**: Gain buy-in from stakeholders by connecting compliance outcomes to business goals. Regularly review and adjust resource allocation and communicate successes.

THE SEISO WAY

The 10 Domains SM

Security Simplified.

Seiso's approach to risk assessment is driven by a desire to simplify security compliance. We follow a framework-agnostic method, the 10 Domains, that aims to swiftly evaluate and enhance a company's security program maturity, sidestepping the complexity and disruption often associated with traditional methodologies.

Business Imperatives

- Shareholder value and customer loyalty
- Contractual and regulatory commitments
- Brand protection, innovation, and agility

Security Capabilities

People

Skills support the information security program to successfully execute the requisite activities.

Process

Information security program operational processes to meet the anticipated expectations of stakeholders.

Technology

Controls to support the operational processes of the information security program.

10 Domains

- Governance
- Risk Management
- Asset Management
- Identity & Access Management
- Threat & Vulnerability Management
- Situational Awareness & Information Sharing
- Incident Response & Recovery
- Vendor Risk Management
- Workforce Management
- Data Protection

Benefits

Streamlines Compliance with Multiple Frameworks: Simplifies adherence to multiple standards (NIST CSF, ISO 27001, SOC 2, and others) with a unified, coherent methodology.

Consolidates Security into 10 Functional Areas: Organizes security measures into 10 key areas for streamlined development and ongoing management.

Simplifies Security Program Development: Streamlines the creation and review of security programs, making complex processes more manageable and efficient.

Prioritizes Alignment to Business Imperatives: Focuses on aligning security initiatives with business goals, considering the dynamics of the workforce.

Flexible, Non-Prescriptive Controls: Tailors controls to specific business needs, providing adaptability and relevance without being overly rigid.

Uses Clear Language: Employs straightforward, accessible language to ensure broad understanding across all organizational levels.

Security Simplified.

seisollc.com
(412) 206-6591
sales@seisollc.com

At Seiso, we believe that simplicity is the key to effective cybersecurity.

We are engineers, compliance experts and former CISOs that specialize in cybersecurity services for growing companies that need to quickly achieve audit compliance and maintain continuous security protection with small teams.

Our approach eliminates complexity, ensuring that your security measures are clear, manageable, and business aligned.

✓ **Be audit ready and maintain compliance with multiple standards and emerging regulations.**

✓ **Manage vendor risk and satisfy security questionnaires.**

✓ **Extend security capabilities fast and without disruption.**

✓ **Align security investments with business imperatives.**

Security Readiness

Where are you?

- Audit Readiness (ISO 27001, SOC 2, CMMC, NIST CSF, HIPAA)
- 10 Domains Blueprint
- Maturity & Technical Assessment
- Penetration Testing
- Cloud Security Assessment

Security Optimization

Where do you want to go?

- GRC - Policies, Standards, & Maintenance
- Risk Management & Register
- Cloud Security
- DevSecOps
- Threat & Vulnerability Management
- Incident Preparedness
- Crisis Planning, Business Continuity & Disaster Recovery
- Awareness & Training

Security Management

Keeping you audit ready

- GRC as a Service
- Security Operations Maintenance Support
- Compliance Automation
- Audit Day Support
- Table Top Exercises

Advisory

- Strategy & Roadmaps
- Fractional / vCISO
- Workshops
- Tooling Assessment & Rationalization

Tooling & Platforms

- Compliance Automation - Vanta, Drata
- IaC - Easy_Infra
- AWS / Azure / GCP

Industries

- Healthcare & Healthtech
- Financial Services & Fintech
- Advanced Manufacturing
- Energy & Utilities
- Retail & E-Commerce
- Defense & Aerospace

Snapshot Assessment

A fast, free assessment against benchmarks to uncover critical program risks. Get an actionable report in 48 hours.

10 Domains Blueprint

A detailed, risk-based plan for audit-readiness and program optimization.

Managed Security

Augment or completely outsource program management for better predictability and consistency.

Start Your Free Snapshot Assessment

Additional Resources

See additional resources from our online library, Seiso Notes.

Cybersecurity Compliance Checklist for Highly Regulated Industries

Our quick reference checklist to simplify your compliance journey, avoid pitfalls, and achieve continual compliance with confidence.

Get the Checklist

Threat Modeling AI Assistant

Simplify your threat modeling tasks with our custom GPT pre-trained with best practices and knowledge from our library of work across many industries and use cases.

Try Our AI Assistant

How Seiso Simplifies Cybersecurity

Cybersecurity doesn’t have to be complicated. In this guide, learn how to simplify your cybersecurity by focusing on reduction, clarity, and tailored solutions using the Seiso Way.

Simplify Your Cybersecurity the Seiso Way

Need Help with Your Security Compliance?

For expert guidance and support in your compliance journey, contact Seiso to help you navigate the complexities of cybersecurity compliance and strengthen your security posture.

Get in Touch.

seisollc.com
sales@seisollc.com
412.206.6591