# Cybersecurity Compliance Checklist

Quick Guide for Highly Regulated Industries

October 2024

# Cybersecurity Compliance for Highly Regulated Industries

Compliance isn't just about checking boxes—it's a strategic journey that transforms how your organization manages risk and demonstrates trustworthiness. For businesses in highly regulated industries, compliance is more than a necessity; it's an opportunity to differentiate, build trust, and accelerate growth.

That's why we created this quick reference guide—a compliance checklist to help you simplify your journey, address key challenges, and unlock competitive advantage with confidence.

Whether you're aiming for SOC 2, ISO 27001, HIPAA, or another standard, this checklist will streamline the process, ensuring that compliance enhances your security posture and aligns with your business goals.

## Key Challenges

**Regulatory Changes**
Staying informed and adapting to evolving regulations requires constant vigilance.

**Lack of Expertise and Time**
Resource gaps delay security programs.

**Financial Implications**
Non-compliance risks fines and reputation.

**Integration Across Departments**
Silos lead to inconsistencies and vulnerabilities.

**Effective Risk Assessments**
Thorough risk assessment requires deep knowledge of threat landscapes and internal vulnerabilities.

**Incident Response and Recovery**
Without a clear plan, response and recovery are disjointed and slow.

## 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.

# Simplify and Accelerate Your Compliance Journey and Avoid the Pitfalls Along the Way

## 1. Understand Your Compliance and Customer Requirements

- [ ] Identify the regulatory requirements (e.g., HIPAA, NYDFS, PCI, GDPR, CCPA) and customer expectations (e.g., ISO 27001, SOC 2) relevant to your industry.
- [ ] Conduct a thorough risk assessment to understand how these obligations impact your organization's operations and relationships.

## 2. Choose the Right Framework(s)

- [ ] Select and tailor frameworks or standards, such as ISO 27001, SOC 2, CIS, or the NIST 800-series, to address the identified regulatory and customer requirements.
- [ ] If multiple frameworks apply, consider implementing a unified control framework to streamline compliance across all of them.

## 3. Conduct a Security Program Maturity Assessment

- [ ] Evaluate your security program maturity (governance, risk management, data, cloud identity & access, etc.) using a comprehensive methodology such as the Seiso 10 Domains.[SM]
- [ ] Develop a detailed roadmap based on assessment results.

## 4. Implement Administrative, Technical, and Physical Controls

- [ ] Administrative: Develop policies, standards, processes, procedures, and regular training.
- [ ] Technical: Hardening, monitoring, identity management & access controls, vulnerability management, penetration testing, data protection, cloud infrastructure, etc.
- [ ] Physical: Secure facilities with surveillance and access controls.

## 5. Awareness & Training

- [ ] Conduct regular and tailored awareness training for all staff.
- [ ] Provide specialized, in-depth training for key roles.
- [ ] Simulate real-world cyberattacks and reinforce learning.
- [ ] Create a continuous, interactive learning program that fosters good behaviors.

# Navigate Cybersecurity Complexities With Confidence and Strengthen Your Security Posture

## 6. Monitor and Continuously Improve

- [ ] Use continuous monitoring tools (e.g., SIEM) and vulnerability assessments.
- [ ] Regularly update policies and procedures to reflect changing threats.

## 7. Prepare for Audits

- [ ] Conduct internal audits and maintain comprehensive documentation.
- [ ] Engage third-party assessors for independent evaluations.

## 8. Use Compliance as a Competitive Advantage

- [ ] Leverage certifications and attestations (ISO 27001, CMMC, SOC 2) to build trust with clients.
- [ ] Conduct business without worrying about how to stay compliant with laws and regulations.
- [ ] Align compliance with business strategy to attract investment and open new markets.

## 9. Avoid Common Pitfalls

- [ ] Maintain thorough and up-to-date documentation.
- [ ] Allocate sufficient resources for compliance efforts.
- [ ] Tailor industry standards to your unique situation.

**Cybersecurity Compliance Guide for Highly Regulated Industries**

Get the full guide for more resources to simplify your compliance journey.

Get the Compliance Guide

## 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**